HEALTH TECHNOLOGY CHALLENGE AIIC 2019

GDPR, sicurezza informatica e dispositivi medici: come la valutazione di impatto sulla protezione dei dati (PIA) impatta sul calcolo dell'indice per la valutazione dei rischi dei DM connessi ad una rete ospedaliera

IRCCS materno-infantile «Burlo Garofolo»

Ospedale S.M. Misericordia - ASUIUD

Dott.ssa Magistrale Michela Stella
Dott.ssa Magistrale Chiara Corvasce
Ing. Michele Bava PhD

Descrizione - Introduzione

Calcolo di un Indice per la Valutazione dei Rischi dei DM collegati ad una rete IT-medicale che includa un Privacy Impact Assessment dei trattamenti dei dati sensibili utilizzati nei DM, nei DM SW e nei SW utilizzati con i DM

La connessione dei DM ad una rete IT-medicale rappresenta un vantaggio per la cura ma implica un'accurata valutazione del rischio, poiché le informazioni scambiate sono idonee a rivelare lo stato di salute dei pazienti.
Il GDPR introduce in un nuovo modello di gestione della privacy anche la valutazione d'impatto (PIA) dei trattamenti, con l'obiettivo di gestire e monitorare i rischi legati ai dati clinici e sanitari.
Lo scopo di questo studio è quello di dare un valore numerico alla PIA e integrarla con un Indice per la Valutazione dei Rischi (IVR) calcolato sui singoli DM, considerando l'uso sicuro ed efficace dei dispositivi, la privacy e la sicurezza di dati e sistemi.

Descrizione - Obiettivi e destinatari dello studio

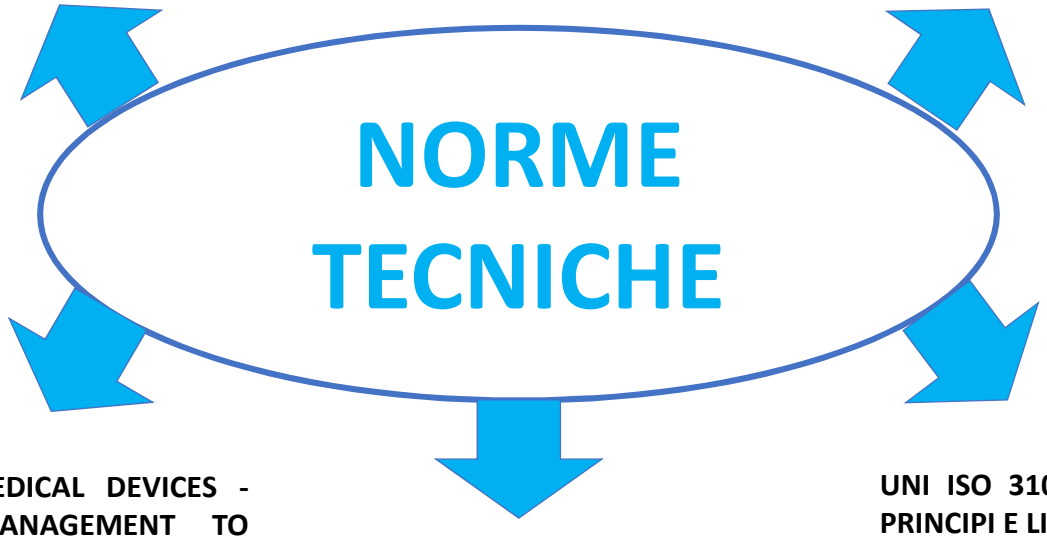
- Unificazione di procedure e metodi per la valutazione dei rischi dei DM che includano, oltre al quadro normativo proprio dei DM stessi, anche la sicurezza informatica (AgID) e la privacy secondo il GDPR

- Destinatari:
  - i titolari delle aziende che possono rispondere in modo efficace e documentato (accountability) ad eventuali minacce
  - i manager ospedalieri, dei servizi di ingegneria clinica e dei sistemi informativi che si occupano di rischio nella più ampia accezione del termine, che possono misurare il rischio e valutare nel tempo, in modo oggettivo, l'impatto delle misure che attuano per mitigarlo
  - Agenzie pubbliche e private, opinione pubblica, servizi di monitoraggio automatici che possono tener traccia nel tempo di analisi e azioni intraprese, grazie ad un approccio nella gestione del rischio integrata e che considera aspetti diversi e complementari

Descrizione – quadro tecnico e normativo

CEI 62-237: GUIDA ALLA GESTIONE DEL SOFTWARE E DELLE RETI IT-MEDICALI NEL CONTESTO SANITARIO

IEC 80001-1:2010: APPLICATION OF RISK MANAGEMENT FOR IT-NETWORKS INCORPORATING MEDICAL DEVICE



CEI UNI EN ISO 14971: MEDICAL DEVICES - APPLICATION OF RISK MANAGEMENT TO MEDICAL DEVICES

UNI ISO 31000: GESTIONE DEL RISCHIO - PRINCIPI E LINEE GUIDA

ISO IEC 27001: TECNICHE PER LA SICUREZZA - SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste
BURLO

Descrizione – quadro tecnico e normativo

Direttive 93/42/CEE, 2007/47/CE e Regolamento Europeo UE 2017/745 (dal 20 Maggio 2020) sui dispositivi medici

Linee Guida MEDDEV 2.X/Y con 1<X<12 e 1<Y<4 (con tutte le loro revisioni

D.Lgs 196/2003 novellato da D. Lgs. 101/2018

Misure Minime AgID – Piano Nazionale per la Sicurezza Informatica nella PA; ENISA Cybersecurity Act; NIS e Direttiva Europea 2016/1148

GDPR – Regolamento UE 2016/679

Descrizione – Misure minime di sicurezza ICT per le PA

•Fanno riferimento al modello CSC (Critical Security Controls) predisposto da Sans Institute nel 2015 che riporta 20 classi di controllo ordinate per efficacia, divise in 3 famiglie (System, Network, Application) e divisi in 2 sub controlli (Foundational e Advanced)

•AgID ha introdotto un terzo sub controllo (Minimo, Standard, Alto) e ha selezionato 8/20 classi chiamandole ABSC (AgIC Base Security Control).

•Top 5 dalla Sans 20 v6, le altre 3 dalla v5.

ABSC1: inventario dei dispositivi autorizzati e non autorizzati

ABSC2: inventario dei sw autorizzati e non autorizzati

ABSC3: protezione di configurazioni hw e sw sui dispositivi mobili, laptop, ws e server

ABSC4: valutazione e correzione continua della vulnerabilità

ABSC5: uso appropriato dei privilegi di amministratore

ABSC8: difese contro i malware

ABSC10: copie di sicurezza

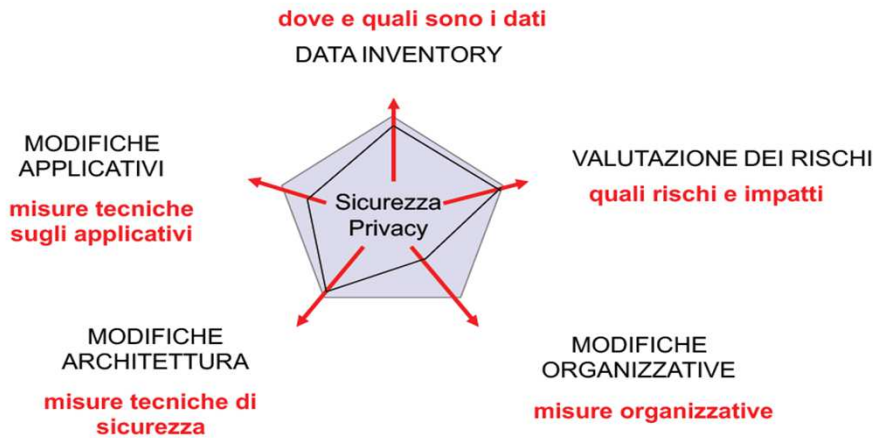
ABSC13: protezione dei dati

Descrizione – Regolamento UE 2016/679

Principi fondamentali:

- ❑ Tutela dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato
- ❑ Accountability (responsabilizzazione) (Art. 24)
- ❑ Valutazione di impatto privacy (PIA) e analisi (e gestione) dei rischi (Art. 35)
- ❑ Privacy by design
- ❑ Misure di sicurezza adeguate (Art. 32)
- ❑ Registro dei trattamenti e RPD/DPO (Artt. 30 e 37)

In sanità -> modello integrato di gestione del rischio (privacy + security)



Descrizione – Regolamento UE 2016/679

Valutazione dei rischi:

Il GDPR prevede in capo al Titolare del trattamento la costruzione di una mappa dei rischi che consenta di stimare, per ogni tipologia di trattamento, un indice di rischio generico.

- DPIA (Data Protection Impact Assessment)
- Analisi del rischio
- **Rischi possibili:**
  - **Danni materiali (danni fisici)**
  - **Danni immateriali (violazione dei diritti e delle libertà fondamentali dei soggetti)**

Descrizione – Regolamento UE 2016/679

Valutazione dei rischi:

Elementi di rischio che derivano dal trattamento dei dati:

- ❑ Distruzione o non diponibilità
- ❑ Perdita
- ❑ Modifica
- ❑ Divulgazione non autorizzata
- ❑ Accesso accidentale o illegale

(R) RISERVATEZZA
(I) INTEGRITA'
(D) DISPONIBILITA'

Obiettivo è quello di assicurare la massima protezione dei dati sanitari dei pazienti favorendo al contempo lo sviluppo di nuove tecnologie nella cura delle persone

- ❑ Finalità:
  - ❑ Identificare i rischi maggiori e adottare contromisure per mitigarli
  - ❑ Dare priorità agli interventi, in base alle risorse disponibili
  - ❑ Valutare e mantenere un rischio residuo

Materiali e metodi

Indice per la Valutazione dei Rischi dei DM & Privacy Impact Assessment

- Valutazione di Impatto Privacy (PIA) inclusa come categoria di rischio nell'IVR e sua rimodulazione
- IVR per i DM vuole essere indice predittivo che include quattro categorie di rischio (documentazione e manutenzione, rischio per il paziente, sicurezza informatica e la «new entry» privacy)
- PIA del Garante è strumento troppo generico per valutazione di impatto in Sanità e non correla in modo oggettivo i dati di uscita (matrice del rischio) con la valutazione che viene svolta in merito a perdita dei dati, modifica dei dati, accesso illegittimo
- Aspetti di privacy e IT security integrati e trattati assieme
- Sono stati selezionati 30 DM pilota connessi alle reti IT-medicali dei/delle due ospedali/Aziende del Friuli Venezia-Giulia (Burlo e Ospedale di Udine)

Materiali e metodi

I 30 DM pilota

DISPOSITIVO MEDICO	ETICHETTA
SPETTROMETRO DI MASSA	28427
MODULE PER HPLC (PC)	28423
SPETTROMETRO DI MASSA	27061
SPETTROMETRO DI MASSA	25552
ELETTROENCEFALOGRAFO (EEG)	28599
ELETTROMIOGRAFO (EMG)	26609
ELETTROCARDIOGRAFO (ECG)	28690
ECOTOMOGRAFO	28640
ECOTOMOGRAFO	26114
ECOTOMOGRAFO PORTATILE	27944
ENDOSCOPIO	
AMPLIFICATORE DI SEQUENZE NUCLEOTIDICHE	27519
TAC	27868
STAMPANTE DI LASTRE	25883
TELECOMANDATO (RAGGI X)	28281
ELETTROENCEFALOGRAFO (EEG)	28046
COAGULOMETRO (DATI RIL. SUL PC IN CUI C'è IL GESTIONALE)	20246
MONITOR ACQUISIZIONI IMMAGINI (sistema aida 27959)	27636
ECOGRAFO GE	28012
ECOGRAFO PROSOUND ALFA 7	27433
ECOTOMOGRAFO VOLUSON E8	27606
ECOGRAFO GE	27136
ECOTOMOGRAFO	28207
TOMOGRAFO A RISONANZA MAGNETICA	27679
WORKSTATION DI REFERTAZIONE RMN	
DIAGNOSI DELL'APPARATO DIGERENTE A CAPSULA DEGLUTTIBILE	27987
ELETTROENCEFALOGRAFO	27740
ELETTROCARDIOGRAFO	26045
ELETTROCARDIOGRAFO	26043
EMOGASANALIZZATORE	27347
EMOGASANALIZZATORE	20302

Materiali e metodi

Calcolo dell'IVR

$$IVR = aX + bY + cZ + \mathbf{dP}$$

X: DOCUMENTAZIONE E MANUTENZIONE
Y: RISCHIO PER IL PAZIENTE
Z: SICUREZZA INFORMATICA
P: PRIVACY-PIA

a,b,c,d: pesi da stimare

Materiali e metodi – categorie e fattori di rischio

DOCUMENTAZIONE E MANUTENZIONE			
(X1) **DOCUMENTAZIONE**	(X2) COSTO DI MANUTENZIONE	(X3) MANUTENZIONE PREVENTIVA	(X4) MANUTENZIONE CORRETTIVA 2018
COMPLETA (CON MAN. IN ITALIANO)=0	GLOBAL SERVICE/GARANZIA=0	MP EFFETTUATA DA MENO DI UN ANNO/ GARANZIA=0	NESSUNA=0
COMPLETA (CON MAN. D'USO IN INGLESE)= 0.5	CONTRATTO=0.5	MP EFFETTUATA DA Più DI UN ANNO / SERVICE/ DOC. INCOMPLETA O NON REPERIBILE=0.5	DA 1 A 3=0.33
NON COMPLETO/NON REPERIBILE=1	SENZA CONTRATTO=1	2 INTERVENTI DI MP NON EFFETTUATI=1	DA 4 A 8= 0.66
	DOCUMENTAZIONE ASSENTE=1	DOCUMENTAZIONE ASSENTE= 1	Più DI 8 (O DOCUMENTAZIONE ASSENTE) = 1

Materiali e metodi – categorie e fattori di rischio

RISCHIO PER IL PAZIENTE			
(Y1) **TIPOLOGIA APPARECCHIATURA**	(Y2) CONSEGUENZE PER IL PAZIENTE IN CASO DI GUASTO	(Y3) ETà (anni)	(Y4) FREQUENZA DI UTILIZZO
TERAPEUTICA=1	MORTE=1	MAGGIORE O UGUALE A 8=1	UTILIZZO GIORNALIERO=1
DIAGNOSTICA=0.66	DANNO=0.75	MINORE DI 8 =0	ALMENO UN UTILIZZO ALLA SETTIMANA=0.75
ANALISI=0.33	TERAPIA INAPPROPRIATA=0.5		ALMENO UN UTILIZZO AL MESE=0.5
ALTRO=0	NESSUN RISCHIO SIGNIFICATIVO=0.25		ALMENO UN UTILIZZO ALL'ANNO=0.25

Materiali e metodi – categorie e fattori di rischio

SICUREZZA INFORMATICA						
(Z1) CREDENZIALI DI ACCESSO AL SISTEMA	(Z2) ANTIVIRUS	(Z3) BACKUP	(Z4) TEST VULNERABILITà (CRITICITà)	(Z5) FIREWALL	(Z6) UPS	(Z7) SISTEMA OPERATIVO OBSOLETO
CREDENZIALI FORTI= 0	INSTALLATO E AGGIORNATO=0	GIORNALIERO=0	ASSENTE=0	ATTIVO=0	Sì= 0	NO=0
CREDENZIALI DEBOLI=0.5	INSTALLATO E NON AGGIORNATO=0.33	SETTIMANALE=0.25	BASSA=0.33	NON ATTIVO=1	NO= 1	Sì=1
NON PRESENTI=1	NON PRESENTE MA INSTALLABILE= 0.66	MENSILE=0.5	MEDIA=0.66			
	NON RESENTE NON INSTALLABILE=1	ANNUALE= 0.75	ELEVATA/NON EFFETTUATA=1			
		NON EFFETTUATO= 1				

Materiali e metodi – categorie e fattori di rischio

PRIVACY-PIA			
(P1) DATI	(P2) ACCESSO ILLEGITTIMO AI DATI	(P3) MODIFICHE INDESIDERATE DEI DATI	(P4) PERDITA DEI DATI
CODICE IDENTIFICATIVO=0	MASSIMA=1	MASSIMA=1	MASSIMA=1
DATI PERSONALI= 0.5	IMPORTANTE=0.66	IMPORTANTE=0.66	IMPORTANTE=0.66
DATI SENSIBILI= 1	LIMITATA=0.33	LIMITATA=0.33	LIMITATA=0.33
	TRASCURABILE=0	TRASCURABILE=0	TRASCURABILE=0

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste

Materiali e metodi – metodi statistici (per il calcolo dei pesi)

MODELLO/METODO DELLA REGRESSIONE LINEARE MULTIPLA:

risponde all'obiettivo di studiare la dipendenza di una variabile quantitativa *Y* da un insieme di n variabili esplicative quantitative *X1,…,Xn,* detti predittori, mediante un modello lineare

MODELLO/METODO LOGISTICO:

ci sono dei fattori *X1,…,Xn* misurabili, ed un output *Y* anch'esso misurabile, tutti relativamente ad un insieme di oggetti. Tuttavia, nella regressione logistica l'output Y è dicotomico: 0 o 1, mentre i predittori assumono valori reali generici, come nella regressione lineare multipla tradizionale.

Risultati

I risultati evidenziano l'attesa co-linearità tra le categorie di rischio privacy e sicurezza informatica e, utilizzando la sola privacy, si è ottenuta una equazione rappresentativa a un costo computazionale inferiore e a parità di risultati.

Risultati – regressione lineare multipla

IVR = *aX + bY + cZ + dP*

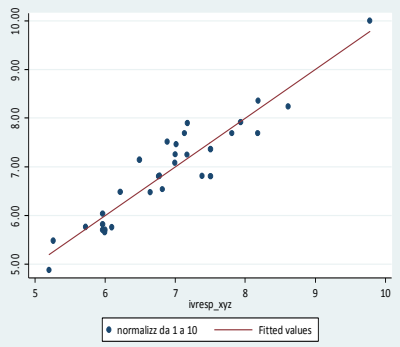
- X, vettore → «*Documentazione e Manutenzione*»
- Y, vettore → «*Rischio per il paziente*»
- Z, vettore → «*Sicurezza Informatica*»
- *P, vettore* → «Privacy»

a, b, c e d pesi da stimare per ciascuna categoria – modello regressione lineare multipla

Trovata multicollinearità tra Z e P → sono stati stimati e confrontati i due modelli con X.Y e Z e X,Y e P

IVR	0 BASSO-MEDIO	1 ALTO	TOTALE
5.197069	1	0	1
5.25547	1	0	1
5.72017	1	0	1
5.962609	3	0	3
5.993913	1	0	1
6.000978	1	0	1
6.09309	1	0	1
6.213079	1	0	1
6.486822	0	1	1
6.642969	1	0	1
6.759453	1	0	1
6.772733	1	0	1
6.816737	1	0	1
6.887031	0	1	1
6.994827	0	1	1
7.001647	0	1	1
7.009923	0	1	1
7.12947	0	1	1
7.167182	0	1	1
7.174247	0	1	1
7.37994	1	0	1
7.502832	1	1	2
7.80983	0	1	1
7.932722	0	1	1
8.176784	0	1	1
8.183192	0	1	1
8.613083	0	1	1
9.779943	0	1	1
TOTALE	16	15	31

Xi, Yi, Zi

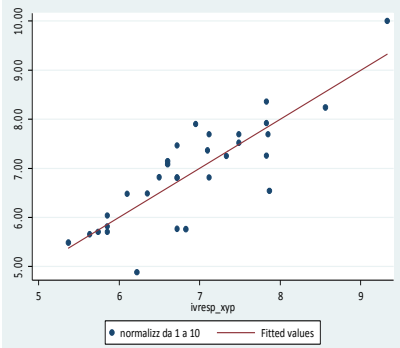


P<0.1

$$IVR_{RLM1} = 1.267733 + 1.289753 * z_3 + 1.360721 * x_2 - 0.7590005 * x_3 + 1.01601 * z_1 + 3.436427 * y_4 + 0.4929089 * z_6 + 1.166861 * y_3$$

IVR	0 BASSO-MEDIO	1 ALTO	TOTALE
5.370118	1	0	1
5.636159	1	0	1
5.739188	1	0	1
5.853402	3	0	3
6.099929	1	0	1
6.222472	1	0	1
6.35133	1	0	1
6.49787	1	0	1
6.602726	0	2	2
6.7204	3	1	4
6.829741	1	0	1
6.952283	0	1	1
7.100654	0	1	1
7.118341	1	1	2
7.332537	0	1	1
7.487411	0	2	2
7.830465	0	3	3
7.848152	0	1	1
7.867665	1	0	1
8.560276	0	1	1
9.327287	0	1	1
TOTALE	16	15	31

Xi, Yi, Pi



P<0.05

$$IVR_{RLM2} = 4.517765 + 0.7670108 * y_3 + 1.459622 * x_2 + 1.464495 * p_2 + 1.118394 * p_4$$

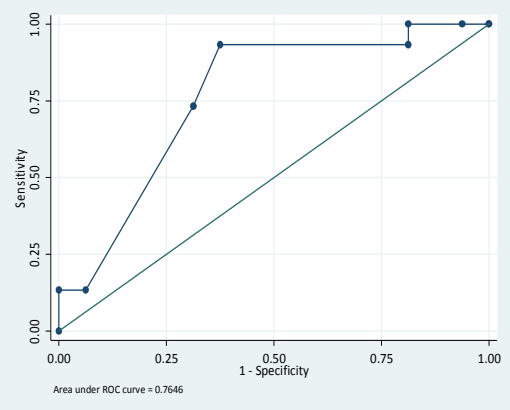
A parità di risultati (numero di DM correttamente classificati) e con un P inferiore (P<0.05), l'equazione con i Pi è computazionalmente più vantaggiosa

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste
BURLO

Risultati – modello logistico

Xi, Yi, Zi

Pr(ivresp)	0	1	Total
.0261295	1	0	1
.0538722	2	0	2
.1030915	0	1	1
.1179561	7	0	7
.5861655	1	3	4
.6894978	4	9	13
.7107756	1	0	1
.9592164	0	2	2
Total	16	15	31

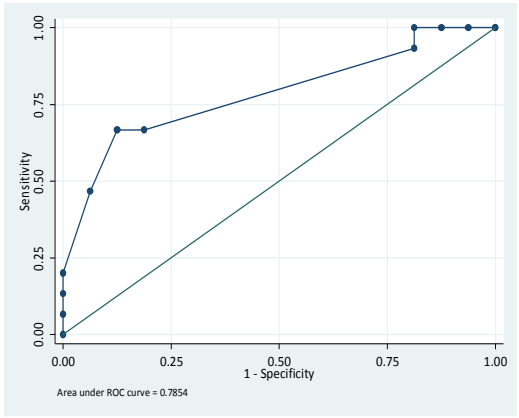


Sensitivity=93,33%
Specificity= 62,58%
Correctly classified=77,42%

P<0.15

Xi. Yi. Pi

Pr(ivresp)	0	1	Total
.0068564	1	0	1
.0332188	1	0	1
.1616833	1	0	1
.184903	0	1	1
.3181692	10	4	14
.5996258	1	0	1
.7237025	1	3	4
.7549489	1	4	5
.9453334	0	1	1
.9531385	0	1	1
.991317	0	1	1
Total	16	15	31



Sensitivity=66,67%
Specificity= 87,50%
Correctly classified=77,42%

P<0.15

$$IVR_{LOG1} = -11.04666 + 2.360065 * y_3 + 9.034736 * y_4 + 2.809702 * z_3$$

$$IVR_{LOG2} = -11.19683 + 3.774763 * x_2 + 1.7251 * y_3 + 10.43464 * y_4$$

Non ci sono significative differenze nell'utilizzo delle Zi o delle Pi

Conclusioni

Integrando il risultato del PIA nell'IVR è possibile attuare un'analisi predittiva sul parco macchine dell'azienda ospedaliera e tracciare la sicurezza dei dati sul singolo DM conformemente al GDPR.

Gli sviluppi sulla valutazione del rischio dei DM, oltre che con l'utilizzo di metodi statistici, di Machine learning e di intelligenza artificiale.

TROVARE UN METODO PREDITTIVO, RIPETIBILE E CONVALIDABILE PER VALUTARE L'IVR

Grazie per l'attenzione

Maria Chiara Corvasce
Dottoressa magistrale in ingegneria clinica
DIA – Dipartimento di Ingegneria e Architettura
Università degli Studi di Trieste