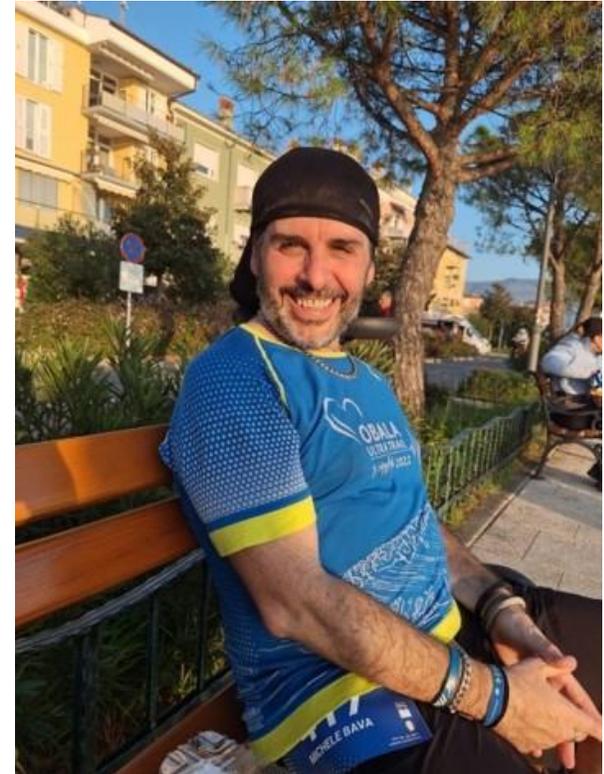


LA CYBER-SICUREZZA TRA COMPLESSITÀ E CRITICITÀ

Michele Bava

Direttore Area dei Servizi ICT e Privacy manager e RTD



SPERIMENTAZIONE IRCCS BURLO GAROFOLO



**Analisi e gestione del rischio per la sicurezza
informatica dell'IRCCS "Burlo Garofolo"**

Master INMED in Informatica Medica - 2006/2007



SPERIMENTAZIONE IRCCS BURLO GAROFOLO

Conclusioni

- Scenario sempre più complesso
- Necessità di proteggere la **conoscenza** aziendale
- Sensibilità e attenzione della dirigenza

- Professionisti esperti in sicurezza: un po' manager un po' hacker
- Formazione continua: leggi, norme ed underground

COSA MANCAVA ALLORA?

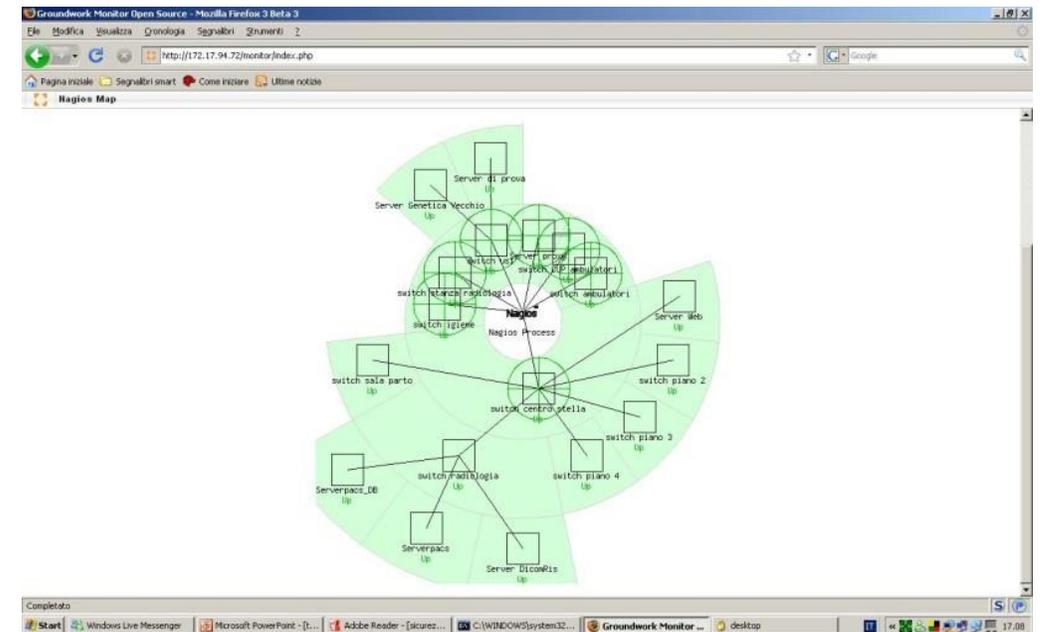
- ✘ Complessità/criticità?
- ✓ Visione di insieme?
- ✓ Strumenti?



COSA MANCAVA ALLORA? – VISIONE DI INSIEME

Regolamento informatico

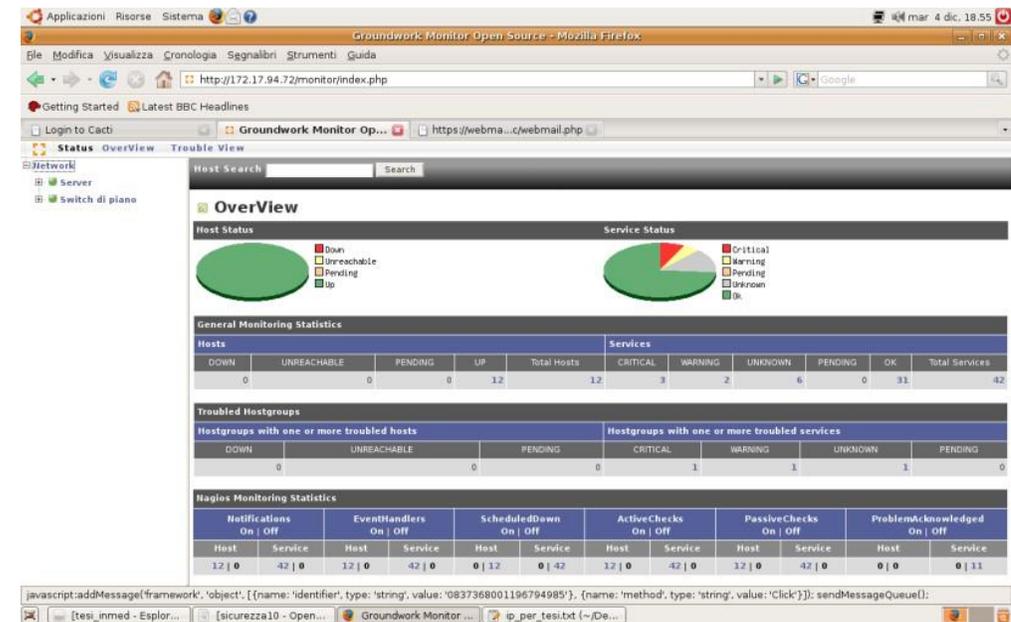
- Stesura basata su standard e normative
- Regole e controlli per utenze e sistemi
- Supporto per la gestione di sistemi, reti e programmi
- Revisioni continue programmate
- Capacità di gestione organizzativa della sicurezza informatica



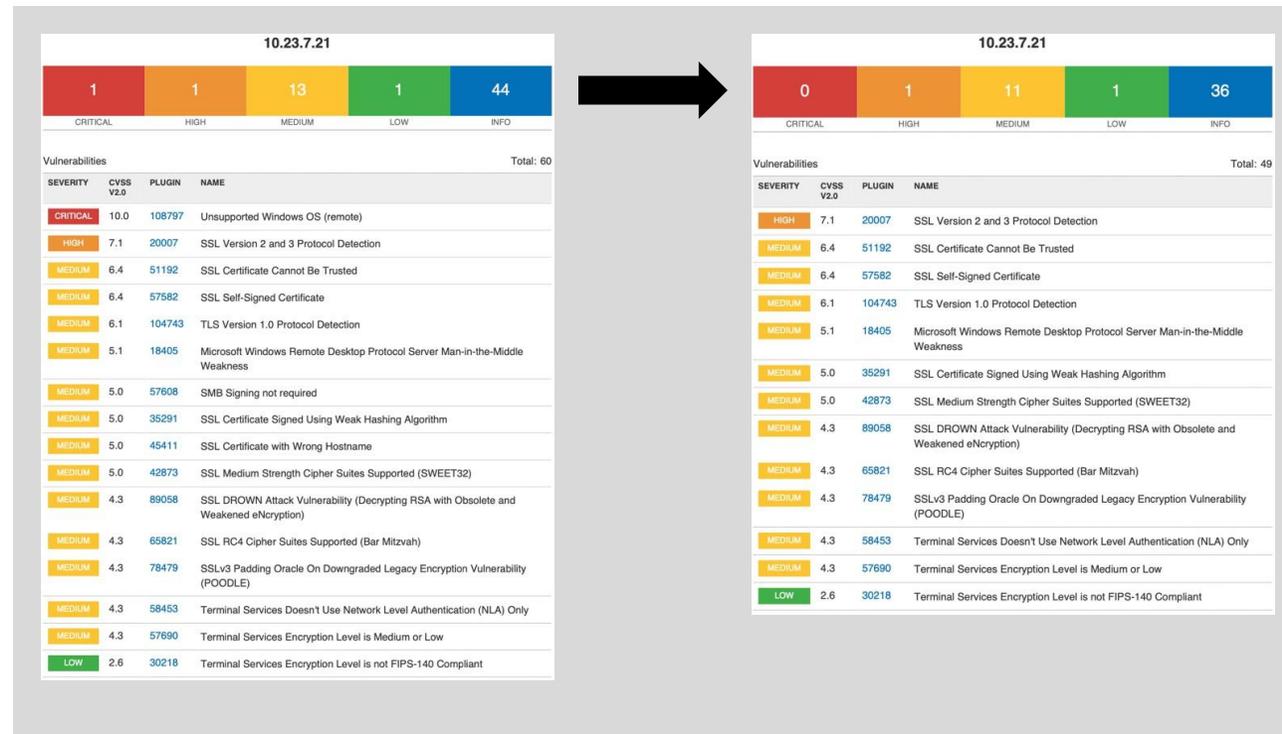
COSA MANCAVA ALLORA? – STRUMENTI

Groundwork / Nagios

- Sistema virtuale linux based scalabile
- Gestione grafica via web di server
- e apparati di rete
- Controllo di sistemi e servizi
- Personalizzazioni e sistemi di alerting remoto
- Diagnosi e reporting facilitati
- Capacità di gestione operativa della sicurezza informatica



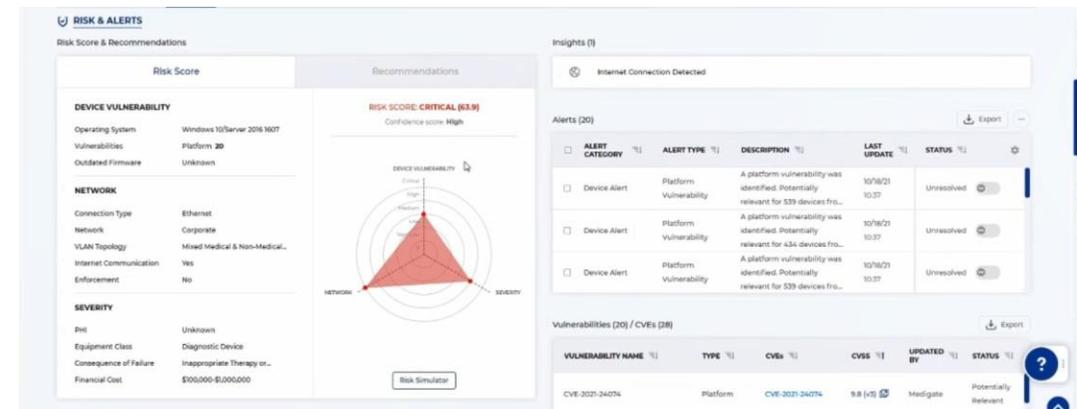
VISIONE DI INSIEME + STRUMENTI = SOC CLINICO



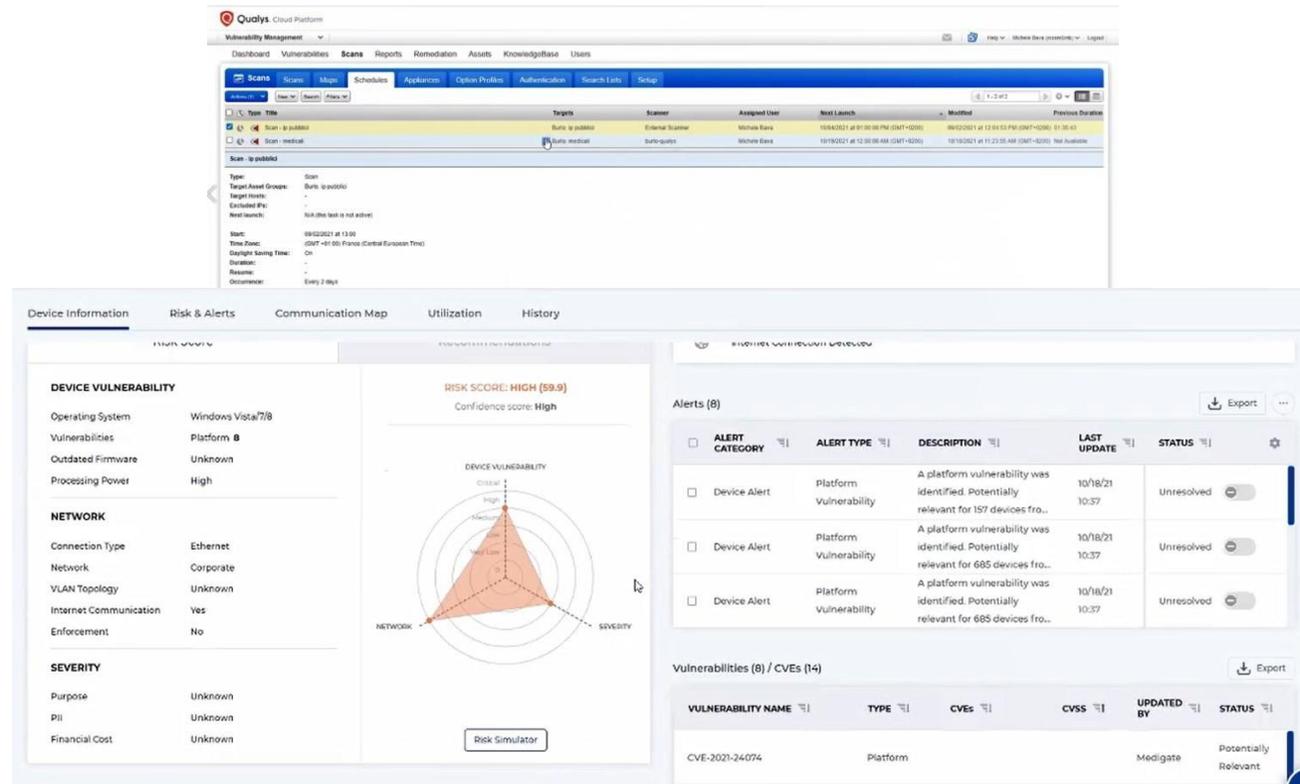
VISIONE DI INSIEME + STRUMENTI = SOC CLINICO

Integrazioni: effettuata con un software *Vulnerability Scanner* che ha eseguito una scansione sulle vulnerabilità, poi importata/visualizzata sulla dashboard.

Il S.O. ha eseguito delle patch di sicurezza che hanno permesso un ricalcolo delle criticità. Risultato soddisfacente: la criticità si è abbassata di un livello, da **'Critical'** a **'High'**.



VISIONE DI INSIEME + STRUMENTI = SOC CLINICO



The screenshot displays the Qualys Cloud Platform interface, divided into two main sections: Vulnerability Management and Device Information.

Vulnerability Management Section:

- Scans Table:**

Type	Title	Targets	Scanner	Assigned User	Next Launch	Modified	Previous Duration
Scan - ip public	Scan - ip public	Burp - ip public	External Scanner	Michela Bana	10/04/2021 at 01:30:00 PM (GMT+02:00)	09/02/2021 at 12:04:10 PM (GMT+02:00)	01:36:43
Scan - ip medical	Scan - ip medical	Burp - ip medical	Burp-qualys	Michela Bana	10/19/2021 at 12:30:00 AM (GMT+02:00)	10/19/2021 at 11:21:38 AM (GMT+02:00)	Not Available
- Scan - ip public Details:**
 - Type: Scan
 - Target Asset Groups: Burp - ip public
 - Target Hosts: -
 - Excluded IP(s): -
 - Real records: 100 (the task is not active)
 - Start: 09/02/2021 at 13:00
 - Time Zone: (GMT +01:00) France (Central European Time)
 - Daylight Saving Time: On
 - Duration: -
 - Resume: -
 - Occurrence: Every 2 days

Device Information Section:

- DEVICE VULNERABILITY:**
 - Operating System: Windows Vista/7/8
 - Vulnerabilities: Platform 8
 - Outdated Firmware: Unknown
 - Processing Power: High
- NETWORK:**
 - Connection Type: Ethernet
 - Network: Corporate
 - VLAN Topology: Unknown
 - Internet Communication: Yes
 - Enforcement: No
- SEVERITY:**
 - Purpose: Unknown
 - Pii: Unknown
 - Financial Cost: Unknown
- RISK SCORE: HIGH (59.9)**
Confidence score: High
- Risk Simulator:** A radar chart showing risk levels across categories: Critical, High, Medium, Low, and Negligible. The current risk score is in the High range.

Alerts (8) Table:

ALERT CATEGORY	ALERT TYPE	DESCRIPTION	LAST UPDATE	STATUS
Device Alert	Platform Vulnerability	A platform vulnerability was identified. Potentially relevant for 157 devices fro...	10/18/21 10:37	Unresolved
Device Alert	Platform Vulnerability	A platform vulnerability was identified. Potentially relevant for 685 devices fro...	10/18/21 10:37	Unresolved
Device Alert	Platform Vulnerability	A platform vulnerability was identified. Potentially relevant for 685 devices fro...	10/18/21 10:37	Unresolved

Vulnerabilities (8) / CVEs (14) Table:

VULNERABILITY NAME	TYPE	CVEs	CVSS	UPDATED BY	STATUS
CVE-2021-24074	Platform			Medigate	Potentially Relevant



MODELLI QUANTITATIVI PER IL CALCOLO DEI PESI DI UN INDICE DI VALUTAZIONE DEL RISCHIO IVR

$$IVR = aX_1 + bX_2 + cX_3 + dX_4 + \dots + kX_n$$

X_1, X_2, \dots, X_n : Categorie di rischio collegate a un processo aziendale

a, b, c, d, ... k: pesi da valutare

MODELLO / METODO DI REGRESSIONE LINEARE MULTIPLA (RLM):

Soddisfa l'obiettivo di studiare la dipendenza di una variabile quantitativa Y (l'IVR) da un insieme di n variabili esplicative quantitative X_1, \dots, X_n , chiamate predittori (i fattori di rischio), per ogni processo aziendale, utilizzando un modello lineare.

$$IVR = \begin{pmatrix} A_{11} & \dots & A_{1j} \\ \vdots & \ddots & \vdots \\ A_{i1} & \dots & A_{ij} \end{pmatrix} \begin{pmatrix} X_1 \\ \vdots \\ X_j \end{pmatrix} + \begin{pmatrix} c_1 \\ \vdots \\ c_j \end{pmatrix} \quad \text{per i-esimo processo aziendale}$$

MODELLO / METODO LOGISTICO:

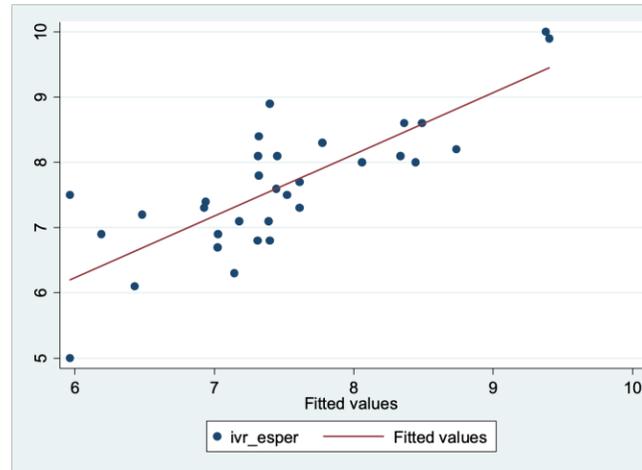
Esistono fattori di rischio X_1, \dots, X_n misurabili e un output Y dicotomico: 0 o 1, mentre i predittori assumono valori reali generici, come nella tradizionale regressione lineare multipla.

RISULTATI – REGRESSIONE LINEARE MULTIPLA

$P < 0.05$ $IVR_{RLM} = 4.885831 + 0.7508848 * x_2 + 1.04312 * y_3 + 0.8905431 * z_4 + 1.249948 * z_5 + 0.8873042 * z_6 + 1.541112 * c_2$

IVR	BASSO	MEDIO	ALTO	TOTALE
5.966222	1	1	0	2
6.188858	1	0	0	1
6.42859	1	0	0	1
6.481668	1	0	0	1
6.927285	1	0	0	1
6.938226	1	0	0	1
7.023084	1	0	0	1
7.026323	1	0	0	1
7.145525	1	0	0	1
7.179129	1	0	0	1
7.309159	1	0	0	1
7.313668	0	0	1	1
7.319133	0	1	1	2
7.389307	1	0	0	1
7.398526	1	0	1	2
7.446793	0	1	0	1
7.451604	0	0	1	1
7.522618	0	1	0	1
7.610842	1	0	0	1
7.611943	0	1	0	1
7.773969	0	0	1	1
8.059469	0	1	0	1
8.336267	0	0	1	1
8.362253	0	0	1	1
8.444885	0	1	0	1
8.488844	0	0	1	1
8.737696	0	0	1	1
9.379388	0	0	1	1
9.404847	0	0	1	1
TOTALE	14	7	11	32

IVR	BASSO	MEDIO	ALTO	TOTALE	
(>= 7.313...)	100.00%	63.16%	78.12%	2.7143	0.0000
(>= 7.319...)	92.31%	63.16%	75.00%	2.5055	0.1218
(>= 7.389...)	84.62%	68.42%	75.00%	2.6795	0.2249
(>= 7.398...)	84.62%	73.68%	78.13%	3.2154	0.2088
(>= 7.446...)	76.92%	78.95%	78.12%	3.6538	0.2923
(>= 7.451...)	76.92%	84.21%	81.25%	4.8718	0.2740
(>= 7.522...)	69.23%	84.21%	78.13%	4.3846	0.3654
(>= 7.610...)	69.23%	89.47%	81.25%	6.5769	0.3439
(>= 7.611...)	69.23%	94.74%	84.38%	13.1539	0.3248
(>= 7.773...)	69.23%	100.00%	87.50%		0.3077
(>= 8.059...)	61.54%	100.00%	84.38%		0.3846
(>= 8.998...)	69.96%	100.00%	81.96%		0.4816



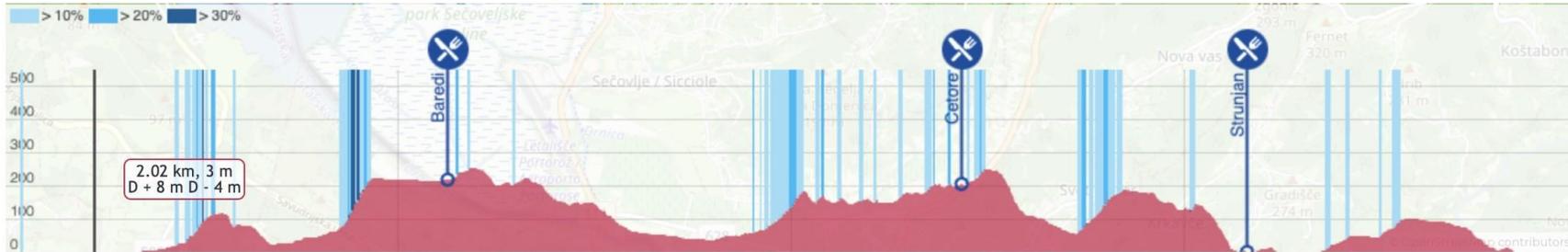
IVR	BASSO/MEDIO	ALTO	TOTALE
5.966222	2	0	2
6.188858	1	0	1
6.42859	1	0	1
6.481668	1	0	1
6.927285	1	0	1
6.938226	1	0	1
7.023084	1	0	1
7.026323	1	0	1
7.145525	1	0	1
7.179129	1	0	1
7.309159	1	0	1
7.313668	0	1	1
7.319133	1	1	2
7.389307	1	0	1
7.398526	1	1	2
7.446793	1	0	1
7.451604	0	1	1
7.522618	1	0	1
7.610842	1	0	1
7.611943	1	0	1
7.773969	0	1	1
8.059469	1	0	1
8.336267	0	1	1
8.362253	0	1	1
8.444885	1	0	1
8.488844	0	1	1
8.737696	0	1	1
9.379388	0	1	1
9.404847	0	1	1
TOTALE	21	11	32

Assegnando **rischio basso: 1-7.49**; **rischio medio: 7.5- 8**; **rischio alto: 8.1-10** il modello identifica correttamente 13 su 14 DM a basso rischio

Se si scegliesse **1-7.309** come **basso-medio rischio** e **7.313-10** come **alto rischio** la predittività del modello migliora per l'alto rischio e il modello sovrastima il rischio per i DM a basso-medio rischio (abbiamo 7 falsi positivi): 11 su 11 ad alto rischio identificati

TRAIL RUNNING E ICT SECURITY

Complesso (es. Università)



Critico (es. Banca)



TRAIL RUNNING E ICT SECURITY

Complesso + Critico = sanità



IN UNITS COSA FACCIAMO?



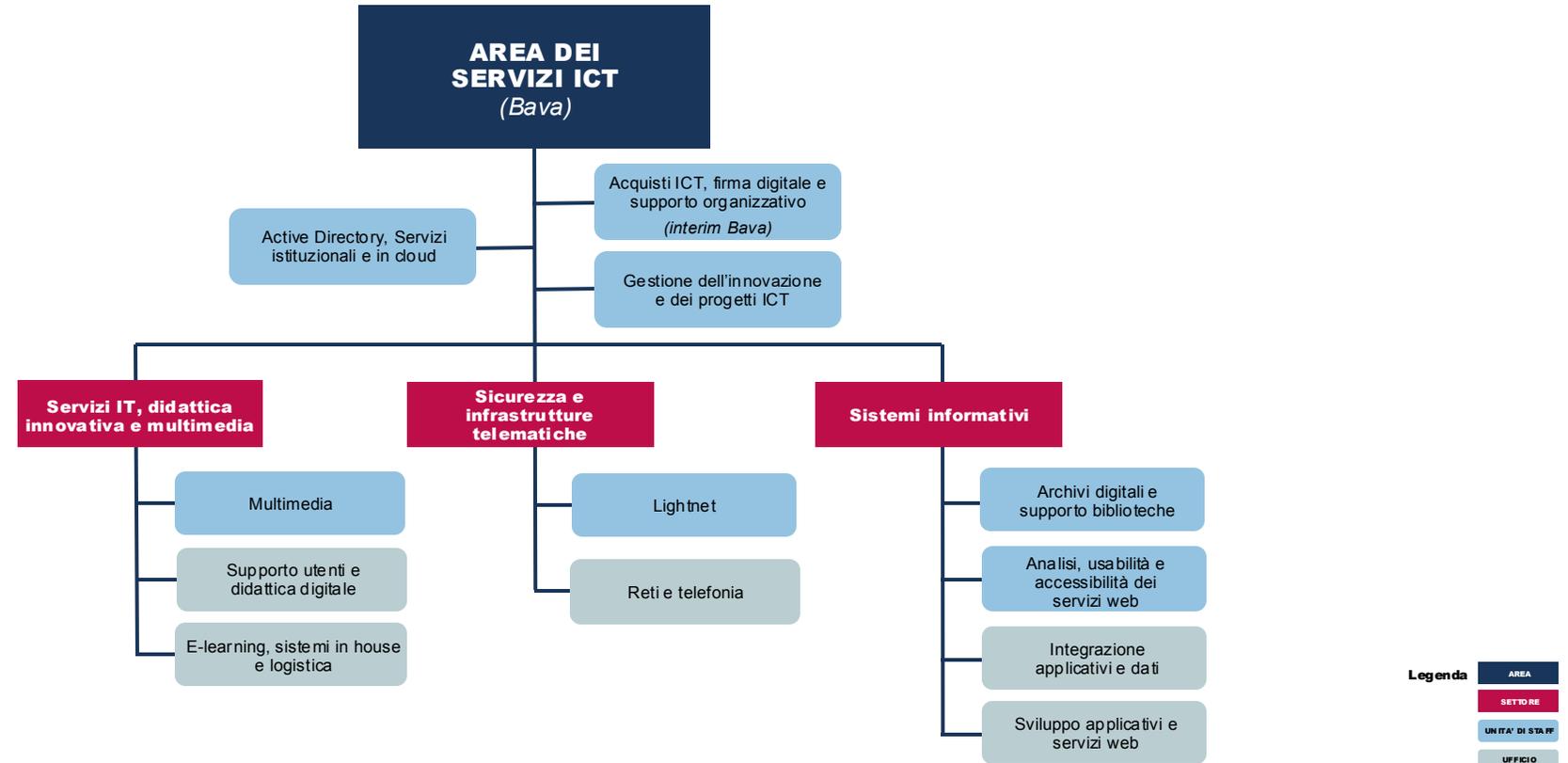
IN UNITS COSA FACCIAMO?

Scenario complesso

- Forniamo e formiamo **competenze** (es. Ingegneri clinici)
- Proponiamo e offriamo **esperienza**
- Diamo una **visione**



IN UNITS COSA FACCIAMO?

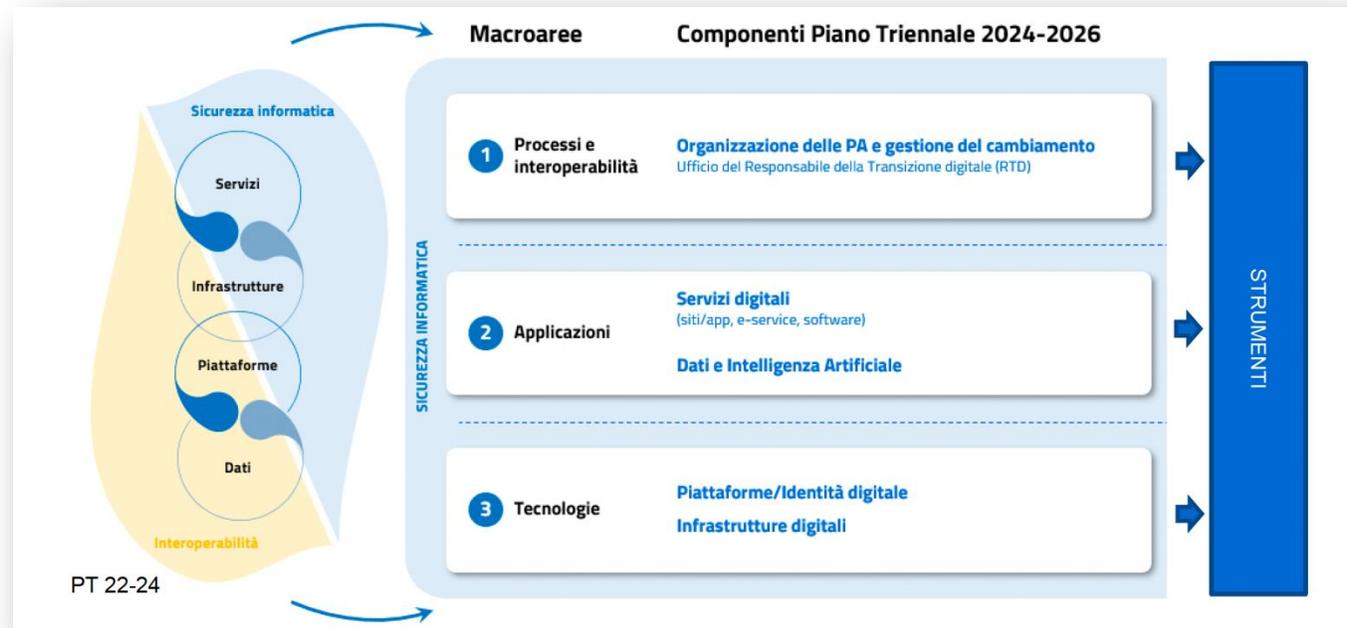


Aggiornato al 1° luglio 2023



FORMAZIONE CONTINUA: LEGGI, NORMATIVE, REGOLAMENTI

Security Awareness



SENSIBILITÀ DEL TOP MANAGEMENT

- Forte commitment aziendale
- Piano strategico – Piano Triennale per la Transizione al digitale
- Figura del RTD



AMBITI	
	<p>FORMAZIONE E STUDENTI</p> <ul style="list-style-type: none"> •DID-O.1 Promuovere un'offerta formativa che risponda alle sfide attuali puntando su innovazione, interdisciplinarietà, connessione con la ricerca e con il territorio •DID-O.2 Migliorare la qualità dei servizi che orientano, supportano e completano il percorso formativo di studentesse e studenti •DID-O.3 Promuovere l'introduzione di metodologie didattiche innovative e la formazione di docenti, tutor e insegnanti •DID-O.4 Implementare, sostenere e favorire un'esperienza di studio internazionale
	<p>RICERCA</p> <ul style="list-style-type: none"> •RIC-O.1 Migliorare la capacità di attrarre risorse per la ricerca •RIC-O.2 Promuovere in tutti i settori una ricerca aperta al confronto internazionale •RIC-O.3 Rafforzare la collaborazione interdipartimentale nonché le sinergie con gli istituti di ricerca, gli enti e le aziende del territorio per sviluppare una ricerca multidisciplinare e interdisciplinare •RIC-O.4 Rafforzare la produzione scientifica di qualità eccellente
	<p>IMPEGNO PUBBLICO E SOCIALE – TERZA MISSIONE</p> <ul style="list-style-type: none"> •TM-O.1 Perfezionare il sistema di assicurazione qualità per l'ambito impegno pubblico e sociale – TM •TM-O.2 Rafforzare le competenze della comunità accademica sulla programmazione e realizzazione di attività di impegno pubblico e sociale – TM e incentivare la partecipazione di tutte le componenti •TM-O.3 Consolidare e sviluppare le attività tradizionali e/o già intraprese •TM-O.4 Sviluppare nuove attività di IPS – TM di interesse per la società, anche in ottica internazionale
	<p>PERSONE E ORGANIZZAZIONE</p> <ul style="list-style-type: none"> •ORG-O.1 Promuovere l'immagine di UniTS valorizzando l'occasione del centenario dell'Ateneo •ORG-O.2 Valorizzare le persone all'interno di UniTS •ORG-O.3 Migliorare l'efficienza dell'organizzazione
	<p>STRUTTURE, INFRASTRUTTURE E SOSTENIBILITÀ</p> <ul style="list-style-type: none"> •SIS-O.1 Incrementare e qualificare gli spazi di studio, di lavoro e di socialità, sotto il profilo della fruibilità, dell'accessibilità e della sicurezza •SIS-O.2 Favorire l'applicazione di principi di sostenibilità •SIS-O.3 Investire nelle nuove tecnologie e nella digitalizzazione dei processi •SIS-O.4 Migliorare l'infrastruttura informatica, ridurre l'obsolescenza impiantistica e incrementare il livello di cyber-sicurezza
OBIETTIVI	

SENSIBILITÀ DEL TOP MANAGEMENT

Indicatori:

- migrazione su cloud
- piano DR
- nuovo DC
- sviluppo interno secondo linee guida AgID
- certificazione ISO 27001

Azioni strategiche	SIS-O.4-A.2	Aumentare il livello di affidabilità/sicurezza/resilienza da un punto di vista infrastrutturale e impiantistico incrementando l'affidabilità del piano di Business Continuity / Disaster Recovery (BC/DR)
	SIS-O.4-A.3	Sviluppare e adottare soluzioni per la prevenzione delle minacce e la mitigazione del rischio relative alla cybersicurezza di reti, applicazioni, servizi e infrastrutture

IL MAN(AGER) - HACKER

- **Modello:** aspetti tecnici/tecnologici e organizzativi/gestionali:
 - - Information security (top down)
 - - Cybersecurity (bottom up)
- La figura dell'**RTD** (nella PA)

- Convenzione con la **Polizia Postale**
- ..**formazione** (privacy + security)



IL MAN(AGER) - HACKER

I compiti del **RTD** e del suo team sono definiti dall'art. 17 del CAD:



- coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni
- indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
- *indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1;*

ISO 27001:2022

E' uno dei principali standard in tema di sicurezza delle informazioni e definisce i requisiti per un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS dall'inglese Information Security Management System).

E' un modello organizzativo. Non è uno standard tecnico, non dice il **come fare** ma solo il **cosa fare** per impostare un SGSI.

Fornisce un indirizzo strategico e tattico:

- considera la gestione della sicurezza delle informazioni come un argomento da affrontare con un approccio sistemico
- definisce la sicurezza come un insieme di processi ciclici e si concentra in particolar modo sugli aspetti di gestione, definendo un catalogo di contromisure di sicurezza ad un livello tale da poter essere applicate a qualsiasi azienda
- ha valenza internazionale

ISO 27001:2022

Lo standard **ISO/IEC 27001:2022** propone un catalogo di 93 controlli suddivisi in 4 gruppi:

- A.5: Organizational controls (37 controls)
- A.6: People controls (8 controls)
- A.7: Physical controls (14 controls)
- A.8: Technological controls (34 controls)

ISO27001 e **NIS 2** (governance-responsabilità; gestione del rischio; supply chain)

ISO 27001:2022

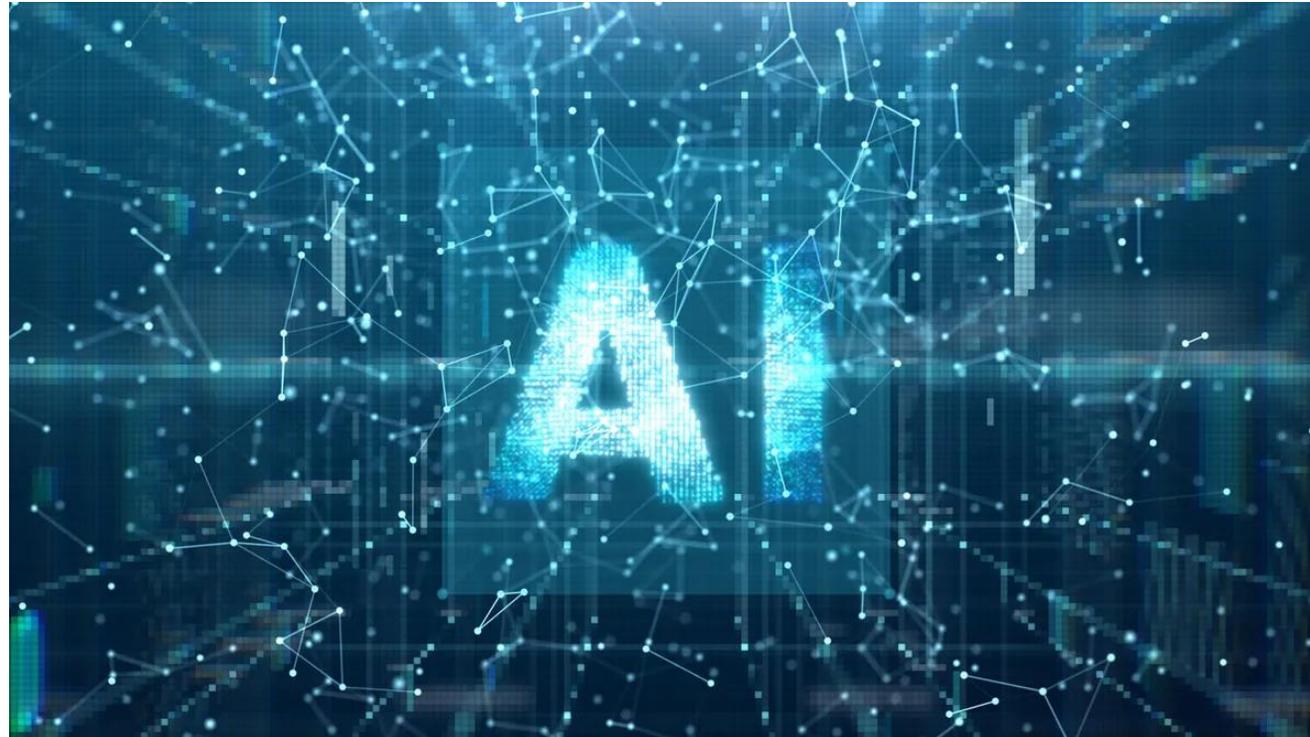
Il regolamento di esecuzione della NIS2, recentemente pubblicato dalla Commissione europea, stabilisce nel dettaglio i requisiti tecnici e metodologici delle misure per la gestione dei rischi cyber previsti dalla direttiva e, di fatto, conferma che **la strada giusta per adeguarsi è adottare la ISO/IEC 27001**. Ecco perché

[NIS2: ecco le regole della Commissione UE per una corretta attuazione della direttiva - Cyber Security 360](#)

L'art. 8 della LEGGE 28 giugno 2024, n. 90 definisce la creazione di una struttura per la cybersicurezza e di un ruolo, quello del referente*, che, come riportato al comma 3, *possono essere individuati, rispettivamente, nell'ufficio e nel responsabile per la transizione al digitale previsti dall'articolo 17 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82.*



COSA MANCA ANCORA?



CONCLUDO

Rise of AI... o A(H)I A(H)I !!! non sappiamo quanto possiamo farci male ancora: opportunità vs rischio

Complessità + criticità: dobbiamo allenarci (politiche e modelli di gestione)

Trasformazione digitale: prima si ottimizza poi si digitalizza (ITIL?)

Furto dell'identità: nuovo perimetro e nuova vulnerabilità

Facciamo (siamo) rete

Diamo valore a 



Forum Risk Management

obiettivo sanità salute

26-29 NOVEMBRE 2024
AREZZO FIERE E CONGRESSI

19

CONCLUDO



o



LA CYBER-SICUREZZA TRA COMPLESSITÀ E CRITICITÀ

Michele Bava

Direttore Area dei Servizi ICT e Privacy manager e RTD

michele.bava@units.it

www.units.it

