UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO
Dipartimento di Informatica

Sistemi di sicurezza

Prof. Donato Impedovo

CICSI *Consiglio Interclasse dei Corsi di Studio in Informatica*

Sicurezza Informatica - CyberSecurity

Cosa è?

Sicurezza Informatica - CyberSecurity

L'applicazione di metodi per:

1. **prevenire atti maligni digitali e logici contro le garanzie e gli interessi di sicurezza,**
2. **rilevare gli atti che li verificano,**
3. **rispondere a tali atti.**

(IEEE Std 692-2013)

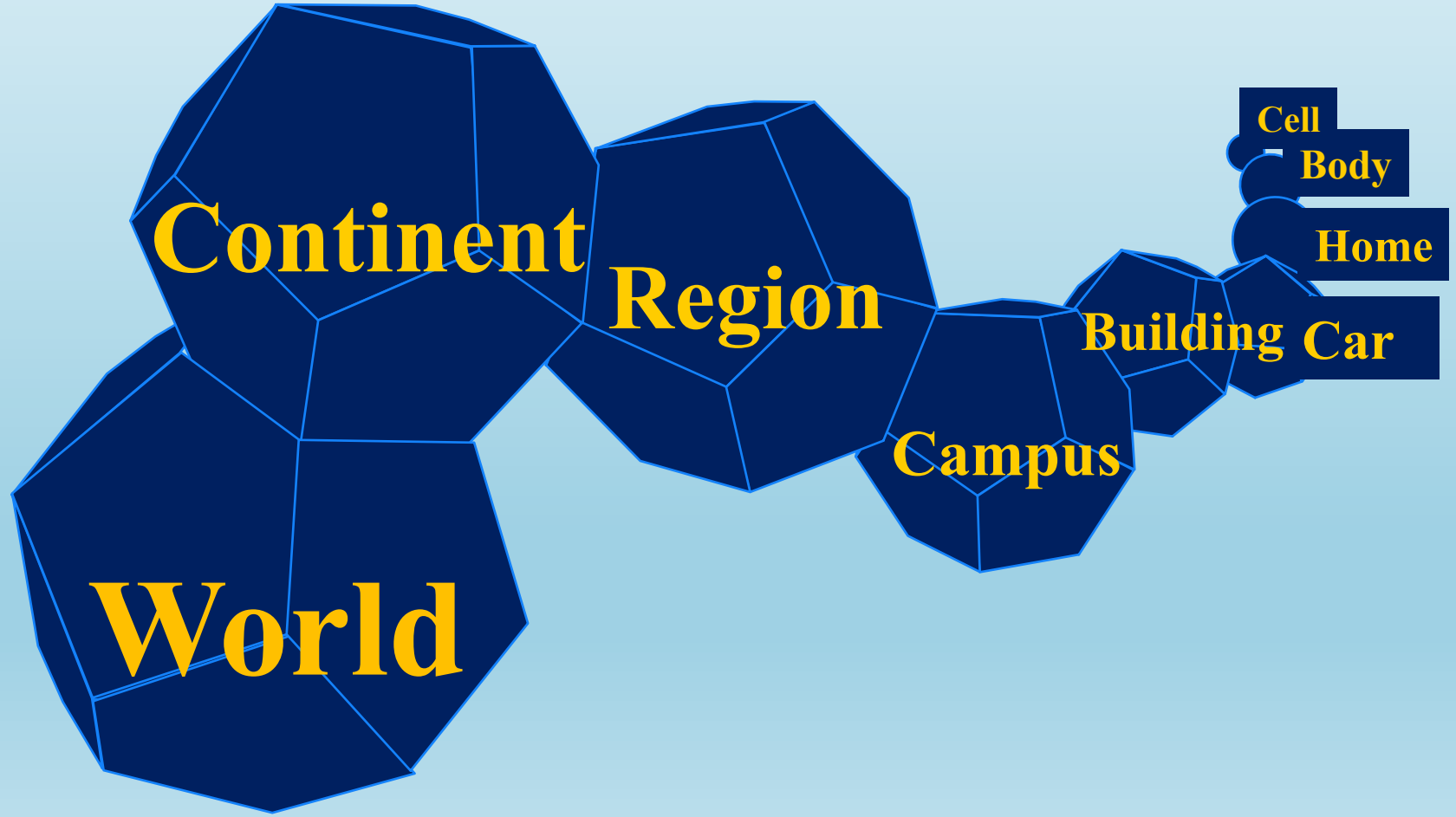
Cyber - Security

Cyberspace

Cosa è?

Sistemi di Sicurezza

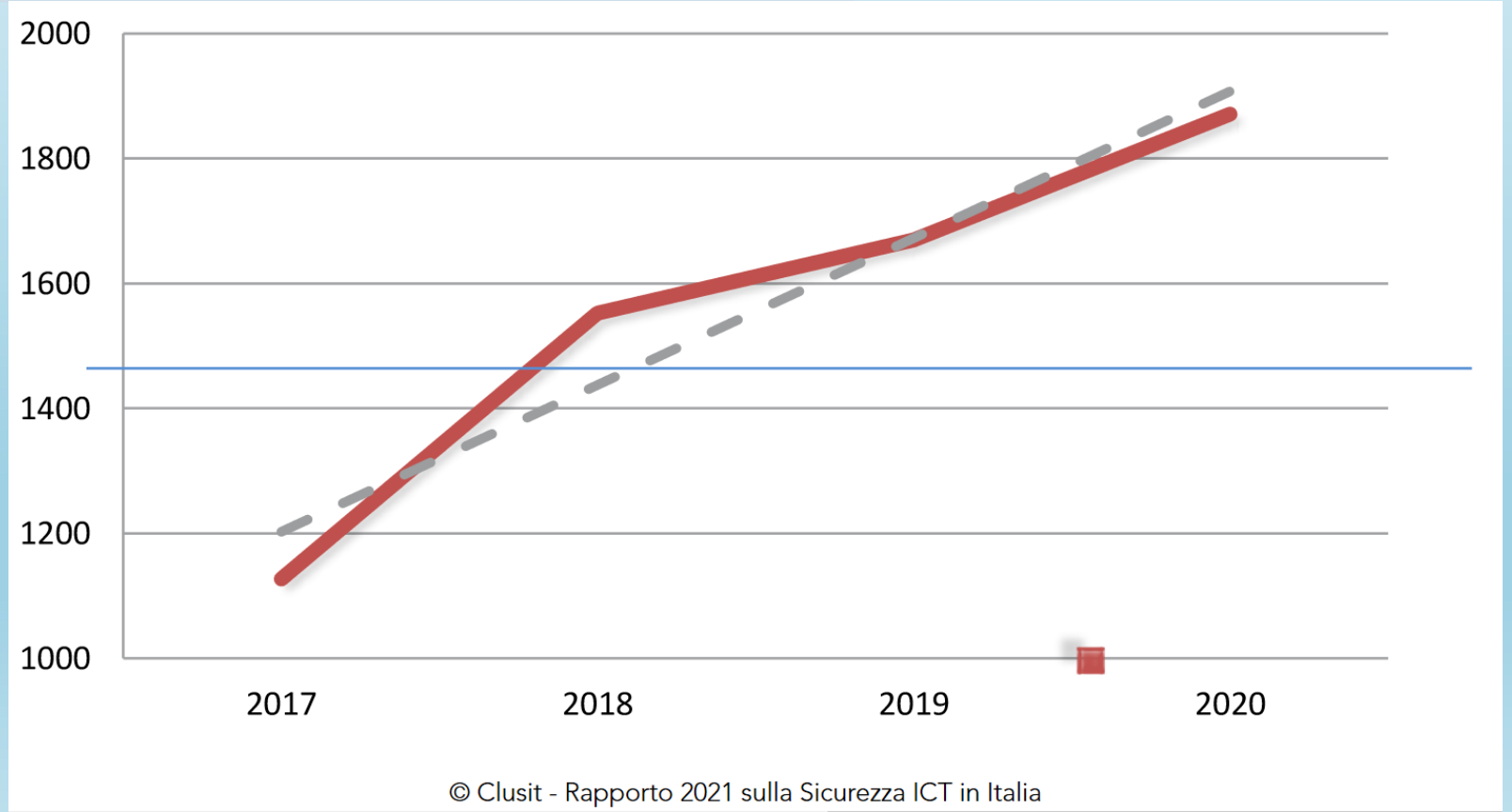
Cyberspace



Sicurezza Informatica - CyberSecurity

REPORT CLUSIT 2021

Incidenti di sicurezza più significativi avvenuti a livello globale



UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO
Dipartimento di Informatica

Sistemi di Sicurezza

NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Sistemi di Sicurezza

Security

- **Physical security** – protezione di items fisici, oggetti, aree di una organizzazione
- **Personal security** – protezione dell'individuo o di un gruppo di individui
- **Operations security** – protezione dei dettagli di una operazione o attività
- **Communications and Network security** – protezione dei mezzi di comunicazione
- **Information Security –** protezione delle informazioni

The need for Security

Quattro motivi fondamentali:

1. Preservare la capacità dell'organizzazione di funzionare/operare,
2. Consentire il funzionamento sicuro delle applicazioni dei sistemi IT,
3. Proteggere i dati,
4. Salvaguardare le risorse tecnologiche in uso.

Sistemi di Sicurezza

Minacce alla sicurezza

- Errori umani (incidenti, fallimenti),
- Compromissione della proprietà intellettuale (pirateria, violazione del copyright),
- Spionaggio (accesso/raccolta di dati non autorizzati),
- Estorsione delle informazioni (ricatto di divulgazione di informazioni),
- Sabotaggio e vandalismo (distruzione di sistemi o informazioni),
- Attacchi software (virus, worm, macros, denaial of service).

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO
Dipartimento di Informatica

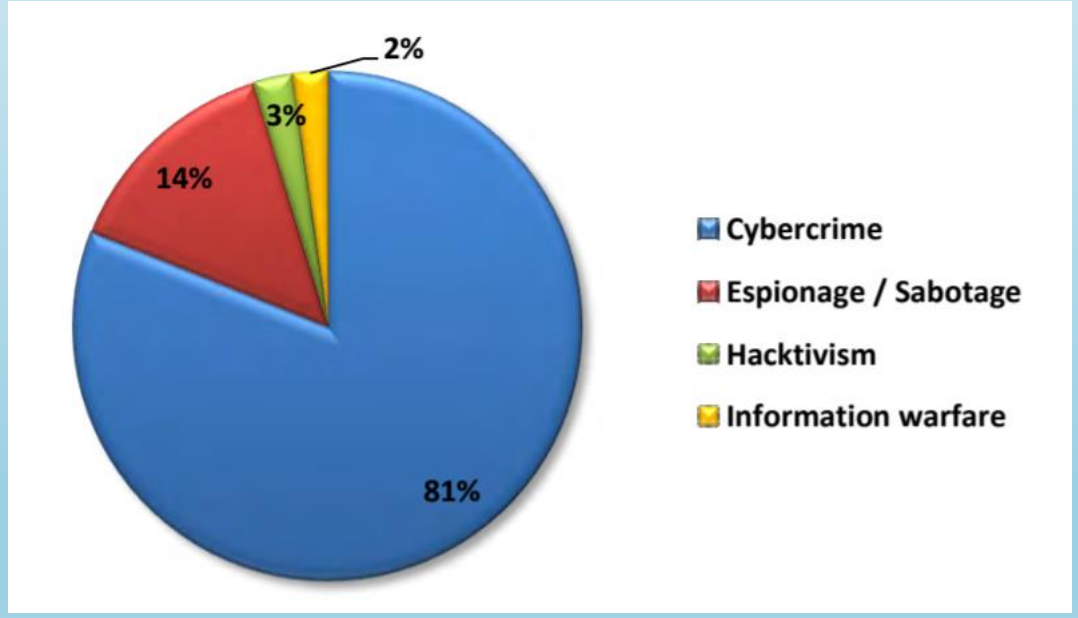
Sistemi di Sicurezza

REPORT CLUSIT 2021

Tecniche di Attacco

TECNICHE DI ATTACCO PER TIPOLOGIA	2017	2018	2019	2020	2020 su 2019	Trend 2020
Malware	446	585	729	783	7.4%	↑
Unknown	277	408	317	372	17.4%	↑
Known Vulnerabilities / Misconfigurations	127	177	127	184	44.9%	↑
Phishing / Social Engineering	102	160	291	289	-0.7%	↗
Multiple Techniques / APT	63	98	65	95	46.2%	↑
Account Cracking	52	56	86	85	-1.2%	↗
DDoS	38	38	23	34	47.8%	↑
0-day	12	20	30	23	-23.3%	↓
Phone Hacking	3	9	1	3	200.0%	↑
SQL Injection	7	1	1	3	200.0%	↑
TOTALE	1127	1552	1670	1871	+12%	

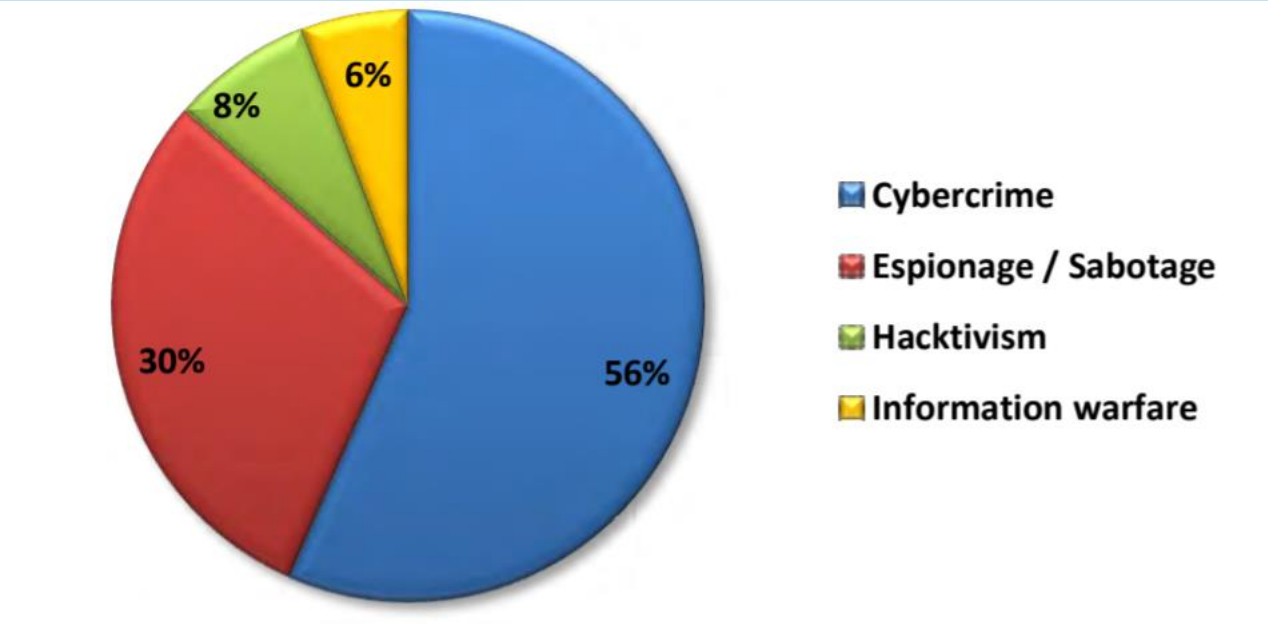
Distribuzione degli attacchi



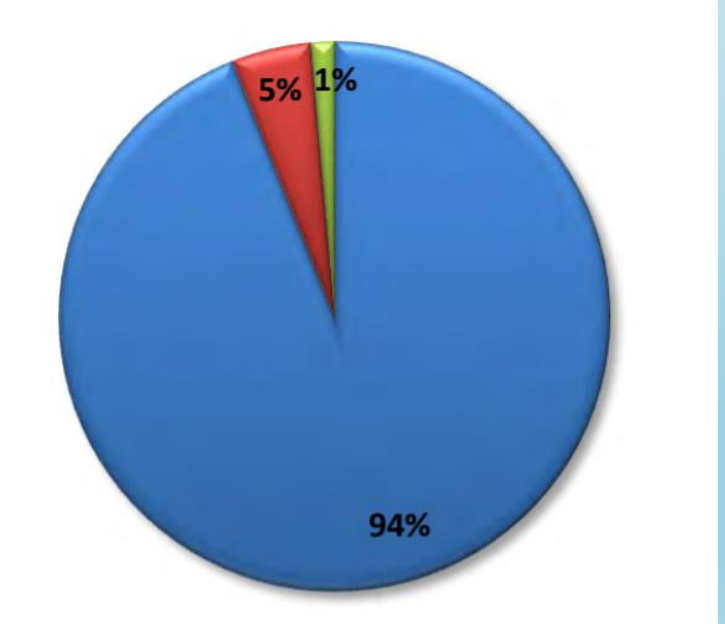
Sistemi di Sicurezza

REPORT CLUSIT 2021

Attacchi vs. Gov/Mil

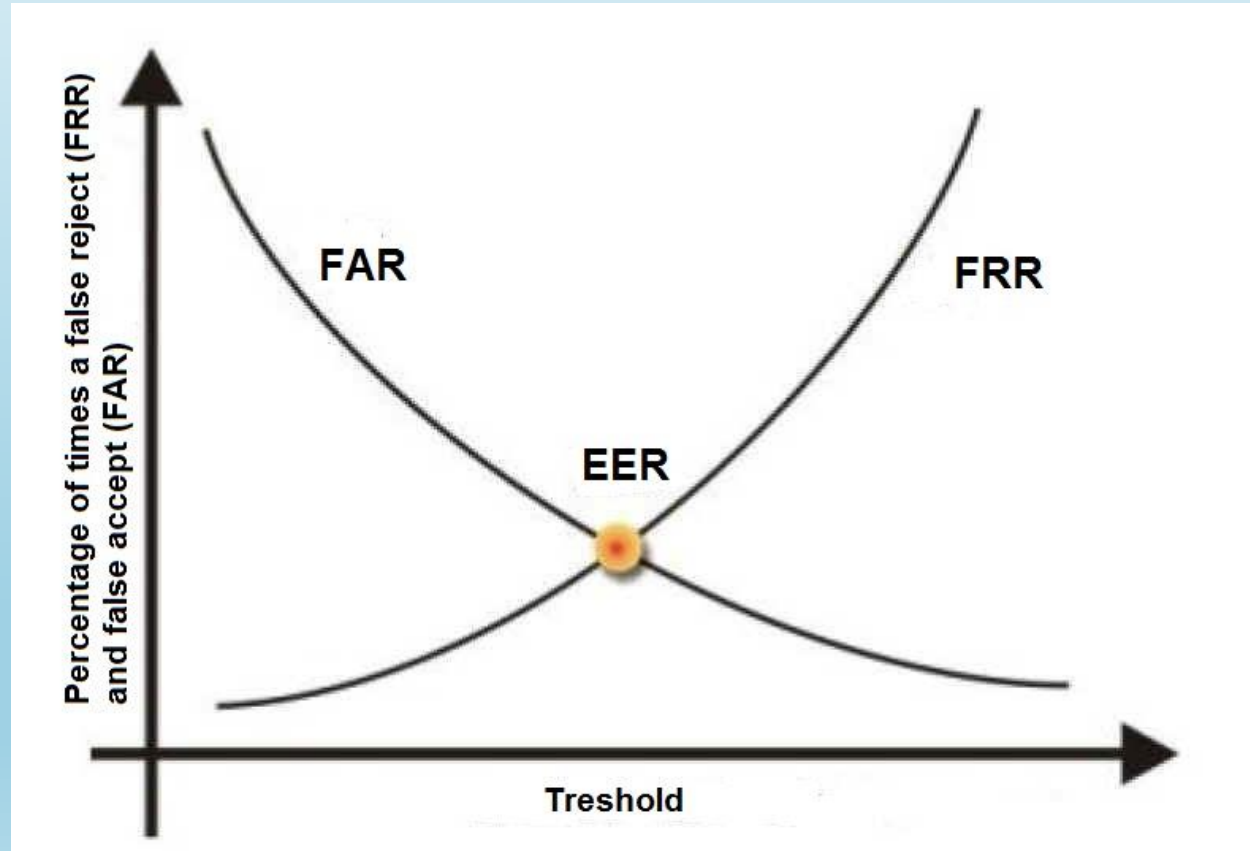


Attacchi vs. Healthcare



Sistemi di Sicurezza

Quanto sicuri possiamo essere?

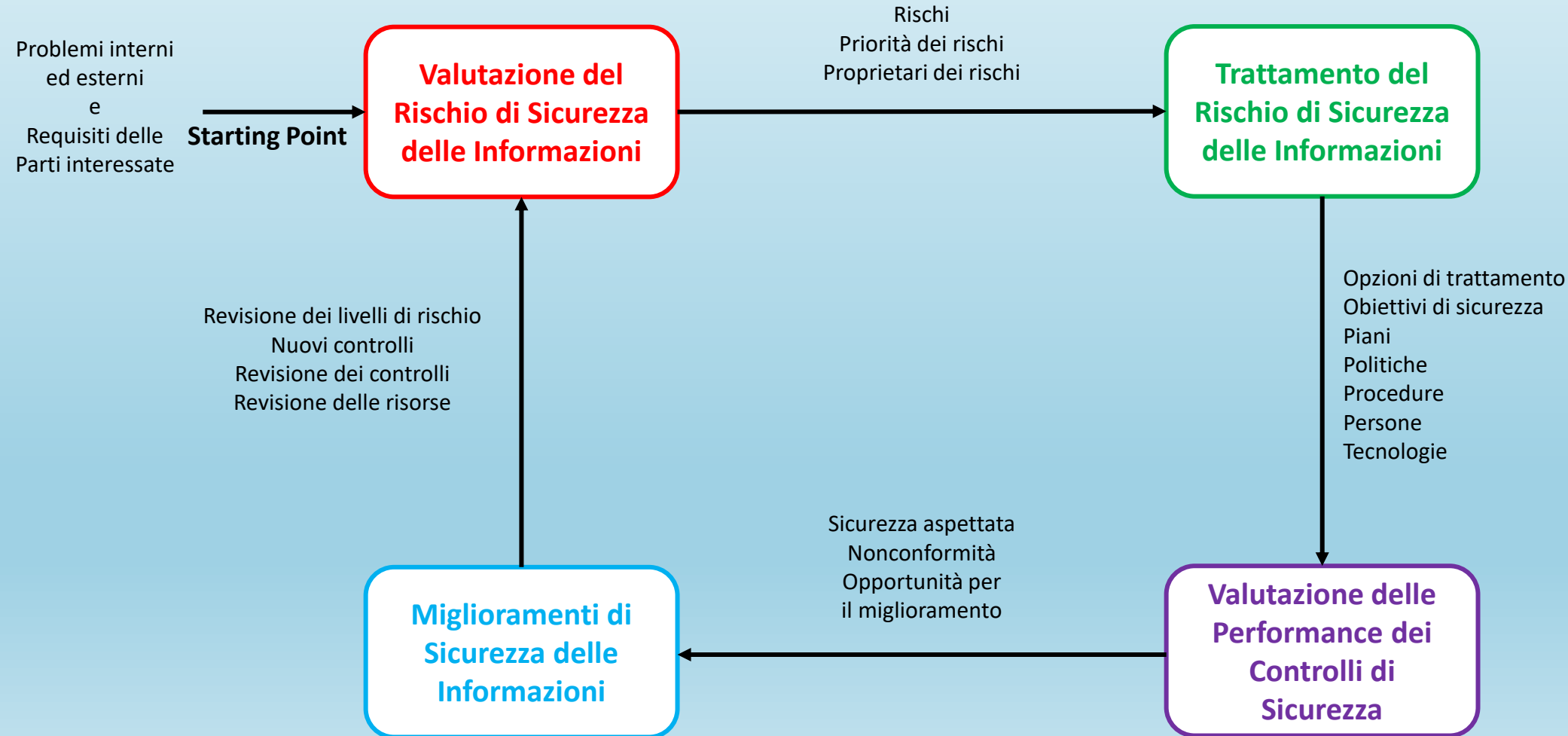


Standard ISO/IEC 27001

Norma internazionale che definisce i requisiti di un sistema di gestione della sicurezza delle informazioni

- **Scopo**: raggiungere e assicurare un determinato livello di sicurezza delle informazioni su tutti gli ambiti dell'organizzazione/azienda.
- Lo scopo viene raggiunto applicando un **Sistema di Gestione delle Sicurezza delle Informazioni.**
- Il **Sistema** deve integrare tutti i processi dell'organizzazione.

Standard ISO/IEC 27001



Standard ISO/IEC 27001

Per iniziare:

- Comprendere il **contesto**, **i bisogni** e **l'aspettativa** dell'organizzazione e delle sue parti interessate.
- Indagini all'interno e all'esterno
- Identificare i requisiti di sicurezza

Standard ISO/IEC 27001

Valutazione del rischio

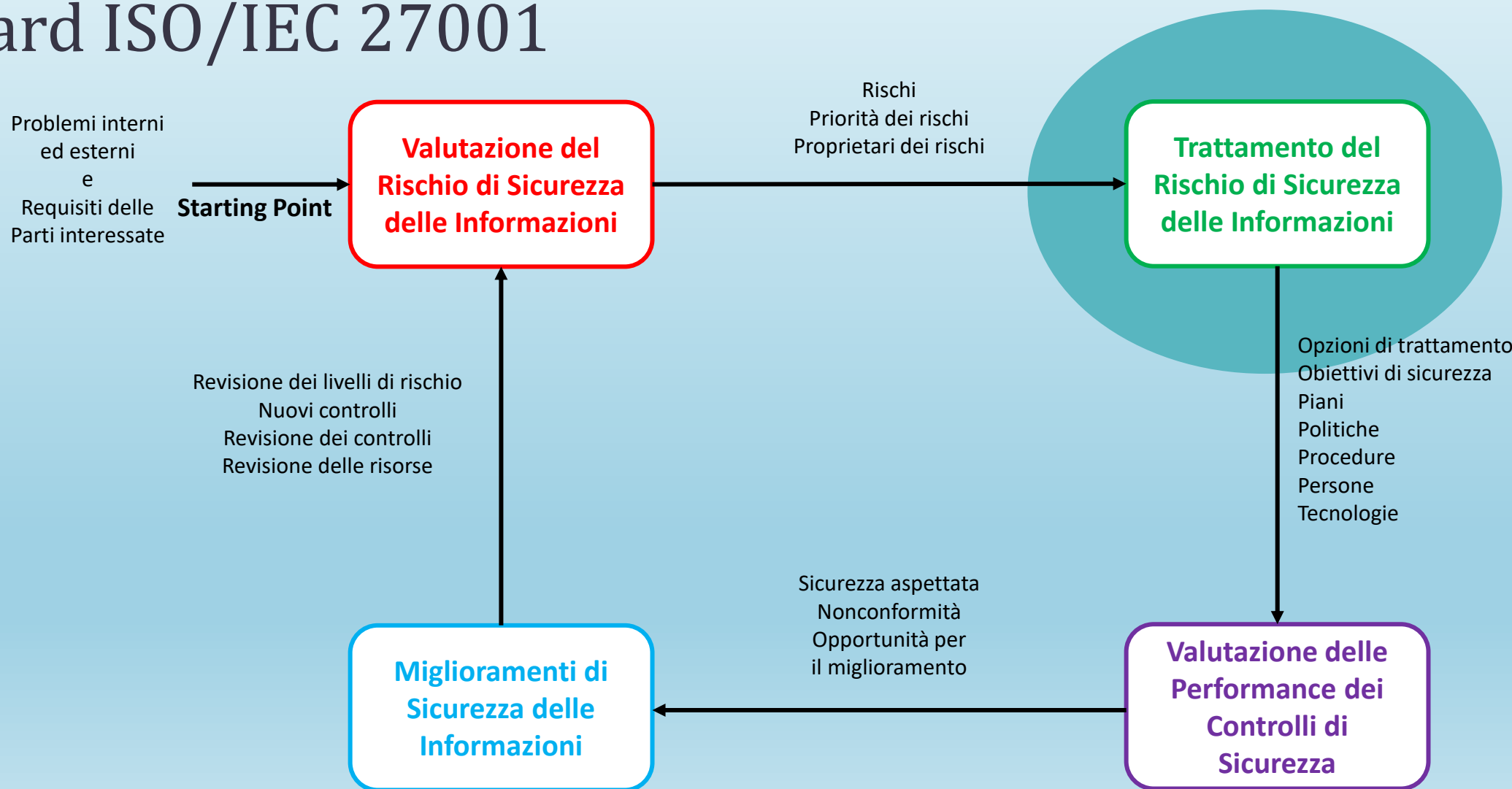
- **Identificazione dei rischi**: identificare i rischi dei processi dalle minacce o dalle vulnerabilità;
- **Proprietari di rischio**: scegliere la persona adatta per poter risolvere il rischio nel miglior modo possibile;
- **Valutare le conseguenze e la probabilità**: valutare le conseguenze e le probabilità su ciascun rischio;
- **Metodo del calcolo dei rischi**: usare un metodo per calcolare il livello generale di rischio;
- **Criteri di accettazione dei rischi**: definire l'accettabilità di un livello rischio;
  - su una soglia scelta l'interno della scala di valutazione,
  - sull'esperienza personale,

Standard ISO/IEC 27001

controlli e obiettivi dei controlli

- Organizzazione interna
  - Compiti
  - Contatti con le autorità
- Dispositivi Mobile e telenetworking
- Risorse Umane
  - Prima dell'assunzione
  - Durante
  - Dopo il termine
- Assets (beni)
  - responsabili
- Classificazione delle informazioni
- Gestione dei media
- Controllo degli accessi
- Responsabilità degli utenti
- Sicurezza fisica ed ambientale
- Sicurezza delle operazioni
- Ecc.

Standard ISO/IEC 27001



Standard ISO/IEC 27001

Trattamento del rischio

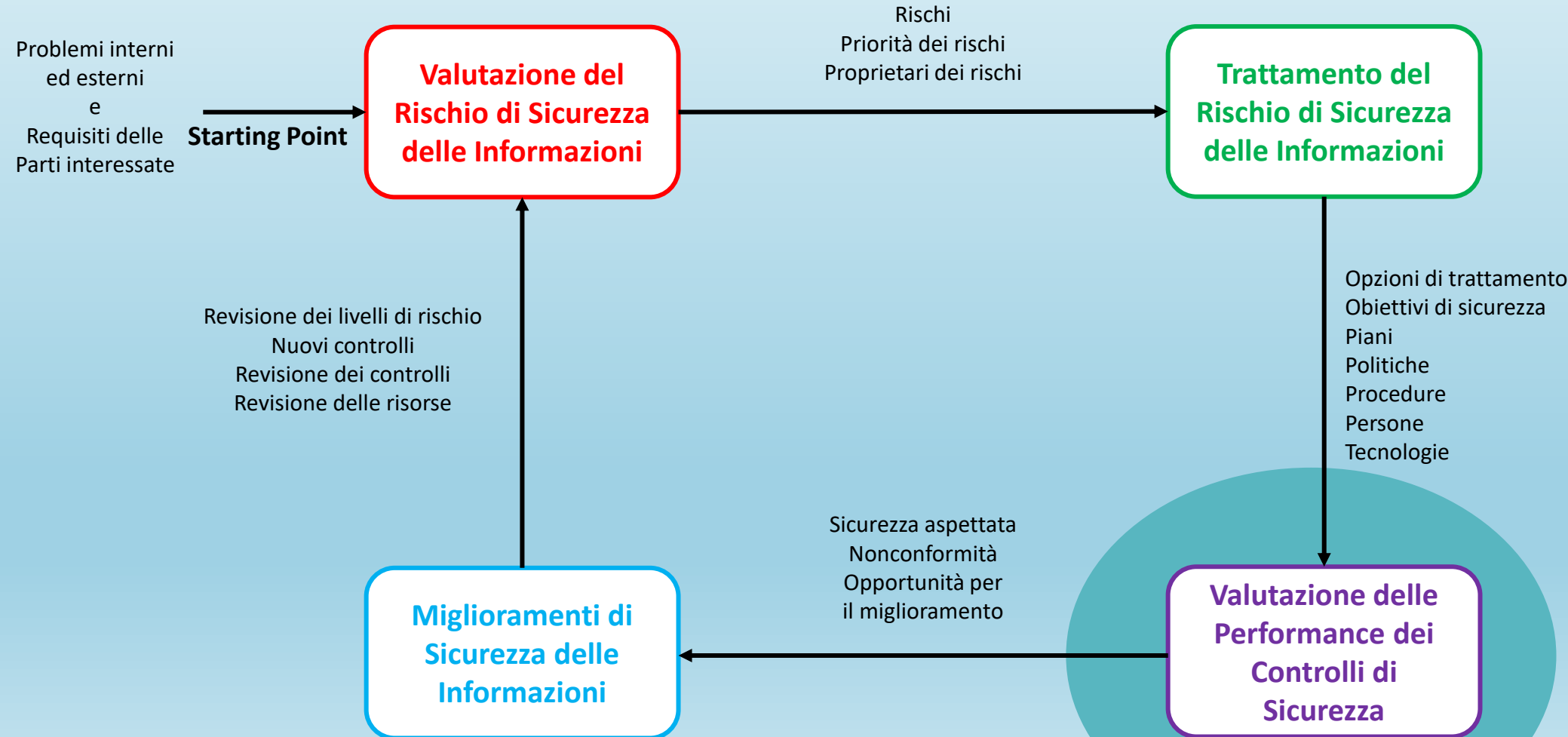
1. si stila un elenco di tutti gli asset e delle possibili minacce e vulnerabilità, valutando l'impatto, le probabilità e il livello di rischio;

2. Non tutti i rischi vanno trattati allo stesso modo:

   - selezionare i rischi più importanti e pesanti,
   - si può trasferire il rischio a compagnie di assicurazioni tramite un polizza assicurativa,
   - si possono arrestare attività considerate troppo rischiose, o
   - accettare il rischio;

Selezionare chi implementerà ogni controllo, in quali tempi, con quale budget ecc.

Standard ISO/IEC 27001



Standard ISO/IEC 27001

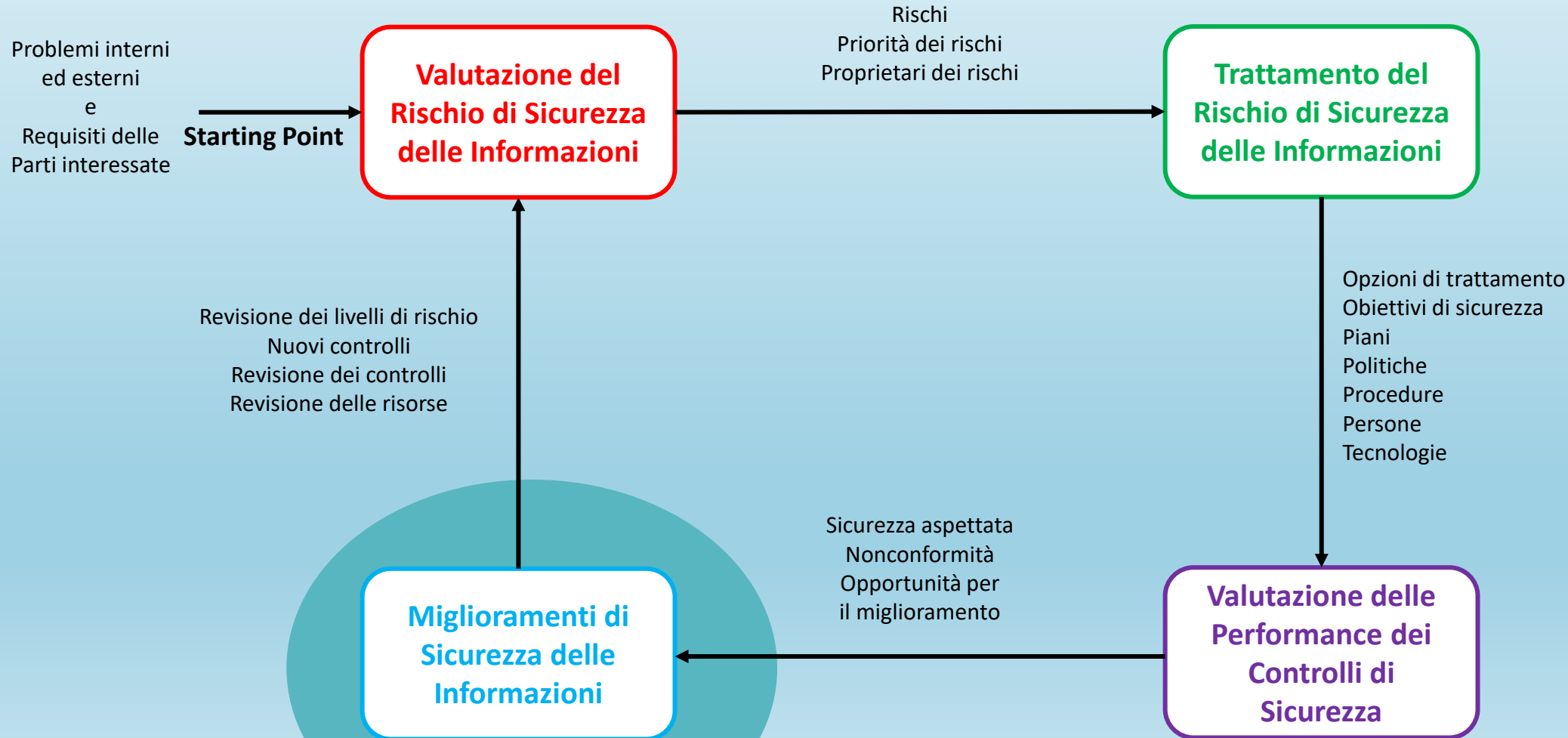
Monitoring, measurement, analysis and evaluation

L'organizzazione deve determinare:

a) Cosa monitorare
b) Il metodo per misurare, analizzare e valutare
c) Quando effettuare il monitoraggio
d) Chi deve effettuare il monitoraggio
e) Quando analizzare i risultati del monitoraggio
f) Chi deve effettuare l'analisi

L'organizzazione redige un documento

Standard ISO/IEC 27001



Sistemi di Sicurezza

Non conformità e azioni correttive

In caso di non-conformità

a) reagire:
   1. Azioni correttive
   2. Gestire le conseguenze

b) Valutare azioni per eliminare le cause della non-conformità

c) Implementare le azioni richieste

d) Valutare l'effettività di tali azioni

e) Modificare il sistema di sicurezza

Gestione degli accessi

Sistemi di Sicurezza

Task: recognize a person…

Standard Techniques:

- possession of an object (something you have)
  - Key,
  - Badge,
  - ID card,
  - …
- knowledge of something (something you know)
  - Password,
  - Key phrase,
  - …
- Possession + knowledge:
  - Key + the knowledge of the right lock
  - Credit Card + PIN,
  - …

Problems:
- Lost
- Stolen
- Forgotten

Sistemi di Sicurezza

Task: recognize a person…

we have an average of 21 passwords;

- 81% of users choose common passwords
- 30% writes or stores it on file

FURTI DI IDENTITA'

- I ladri d'identità rubano i numeri della patente e cognomi da celibi/nubili – spesso utilizzati come password per proteggere un conto – per aprire conti dai quali prelevare fondi.

- crimine con il tasso di crescita maggiore negli U.S.A.

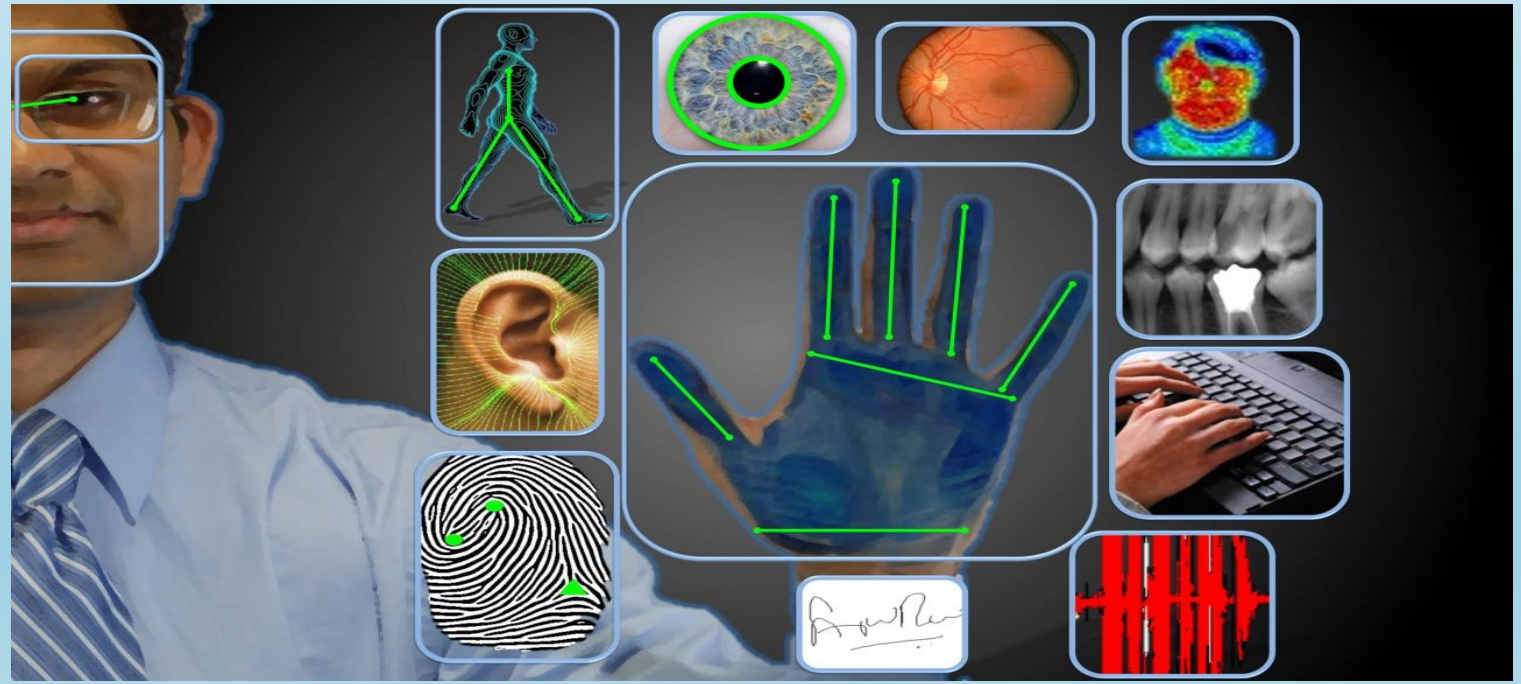
- Fino all'anno scorso per usare la vostra carta di credito per acquisti on line mi è sufficiente vederla per 10s (numero, nome, exp date, ultime 3 cifre sul retro)

Sistemi di Sicurezza

Biometric: the method of establishing the identity of an individual based on a person's distinguishing characteristics.

Something you are: You are your authenticator!

- difficult to be counterfeit,
- cannot be lent or forgotten



Sistemi di Sicurezza

Vantaggi

- Non possono essere perse, prestate, rubate o dimenticate
- L'utente deve "semplicemente" presentarsi di persona
- Garantiscono la presenza della persona

Svantaggi

- Non garantiscono un'accuratezza del 100%
- Esistono utenti che non possono utilizzare alcune tecnologie
- Possono mutare nel tempo
- I dispositivi biometrici, in alcune circostanze, possono non essere affidabili

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO
Dipartimento di Informatica

Sistemi di Sicurezza

Physiological


•Fingerprints


•Face

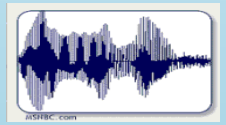

•Hand geometry


•Iris


•Retina

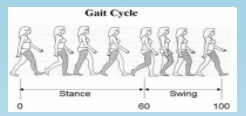
Behavioural

•Signature


•Voice


•Keystroke Dynamic


•Touch dynamics



•Gait

Sistemi di Sicurezza

- Fingerprint. The user places his finger on a postage-stamp sized optical or silicon surface. The user generally must hold the finger in place for 1-2 seconds. Typical verification time from "system ready" prompt: 2-3 seconds.

Piezoelectric sensors

Optical sensors

Ultrasuoni

Sistemi di Sicurezza

Vantaggi

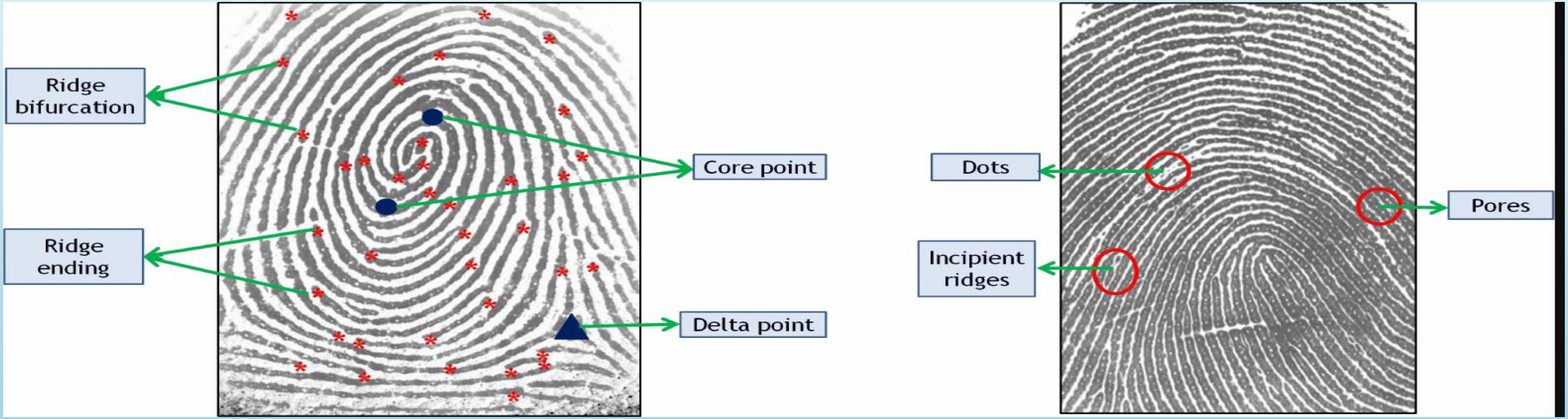
- Elevato potere discriminante e unicità
- Non mutano nel corso della vita di una persona (anche se possono variare temporaneamente a causa di tagli e abrasioni o delle condizioni meteorologiche)
- Pubblicamente riconosciute come affidabili
- Gemelli identici hanno impronte diverse

Svantaggi

- Sporcizia sul sensore o sul dito può compromettere il riconoscimento
- Alcune persone presentano impronte di bassa qualità intrinseca

UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO
Dipartimento di Informatica

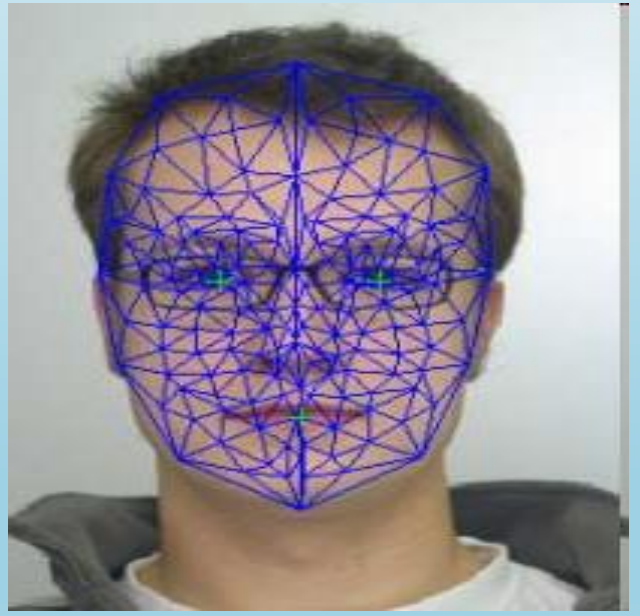
Sistemi di Sicurezza



Sistemi di Sicurezza

- Face recognition User faces the camera, preferably positioned within 50-60 cm of the face. The system locate face and perform matches. In some situations, the user may need to alter his facial aspect slightly to be verified. Verification time: 3-4 seconds.

- Problems:
  - Aging,
  - Different facial expressions
  - Changes in the environment (eg. Complex background, lighting)
  - Changes in the position of the face relative to the camera



UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO
Dipartimento di Informatica

Sistemi di Sicurezza

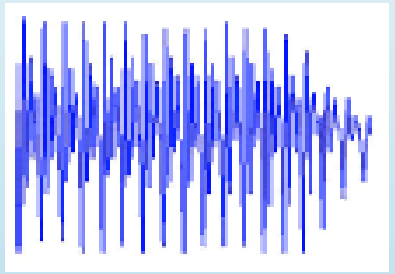
- Problems

UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO
Dipartimento di Informatica

Sistemi di Sicurezza

Sistemi di Sicurezza

- Voice recognition. User positions himself near the microphone. At the prompt, user either recites enrollment pass phrase or repeats pass phrase given by the system. Verification time: 4-6 seconds.



Vantaggi

- Accettabilità elevata da parte dell'utente

Svantaggi

- Caratteristica comportamentale che può mutare nel tempo ed essere influenzata da fattori fisici ed emotivi, e dal rumore dell'ambiente
- Bassa sicurezza, facilmente falsificabile

Applicazioni

- Sistemi locali/remoti, dipendenti/indipendenti dal testo
- Di fatto l'unica tecnologia possibile nel caso di accesso via telefono

Sistemi di Sicurezza

- Iris recognition. User positions himself near the acquisition device. User centers eye on device so he can see the eye's reflection. Depending on the device, the user is between 5-20 cm away. Verification time: 3-5 seconds.

Iride: la corona di tessuto colorato che circonda la pupilla dell'occhio

Vantaggi

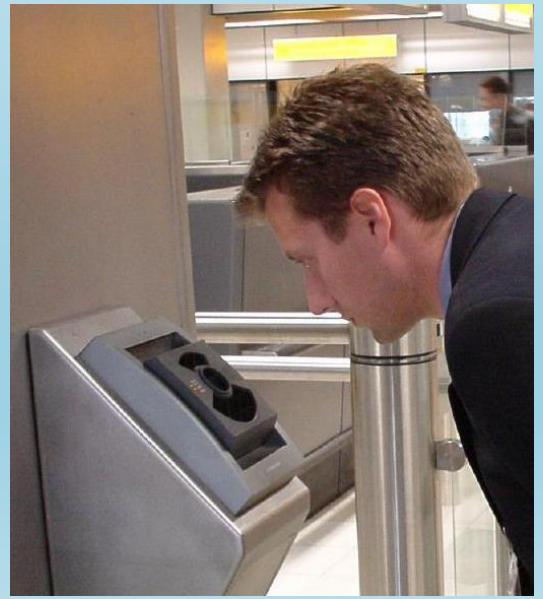
- Estremamente discriminante
- Stabile e invariante durante tutto il corso della vita

Svantaggi

- Richiede un appropriato controllo ambientale
- Tecnica che a volte può essere considerata invasiva (a seconda del dispositivo adottato)
- Costi medio/alti (telecamere a elevata precisione)
- L'acquisizione dell'iride può richiedere un certo grado di collaborazione da parte del soggetto
- Adatta per applicazioni che richiedono un elevato grado di sicurezza

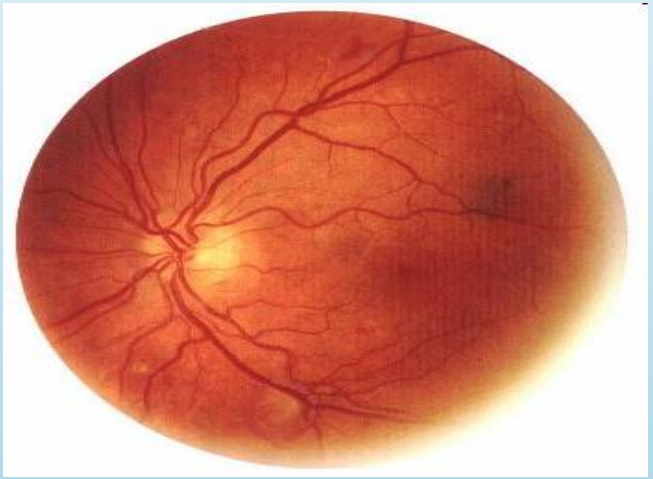
UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO
Dipartimento di Informatica

Sistemi di Sicurezza



Sistemi di Sicurezza

- Retina-scan. User looks into a small opening on a desktop or wall-mounted device. User holds head very still, looking at a small green light located within the device. Verification time: 10-12 seconds.



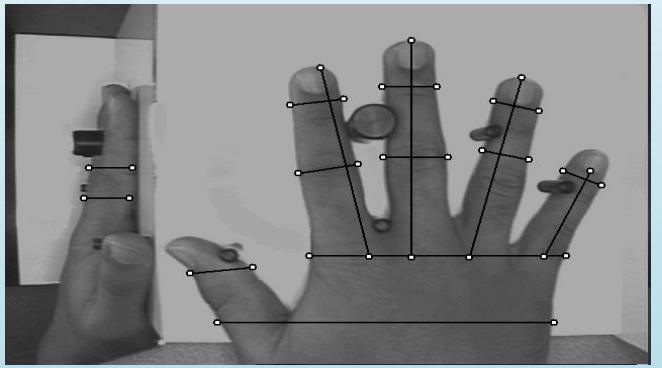
Vantaggi
- Estremamente discriminante
- Una delle caratteristiche biometriche più sicure

Svantaggi
- Richiede collaborazione e uno sforzo consapevole da parte dell'utente
- È una tecnica invasiva – bassa accettabilità
- Costi molto elevati

Adatta per applicazioni che richiedono un grado di sicurezza molto elevato

Sistemi di Sicurezza

- Hand geometry. User places hand, palm-down, on a metal surface with five guidance pegs. Pegs ensure that fingers are placed properly, ensure correct hand position. Verification time: 2-3 seconds.



Caratteristiche della mano (es., lunghezza delle dita)

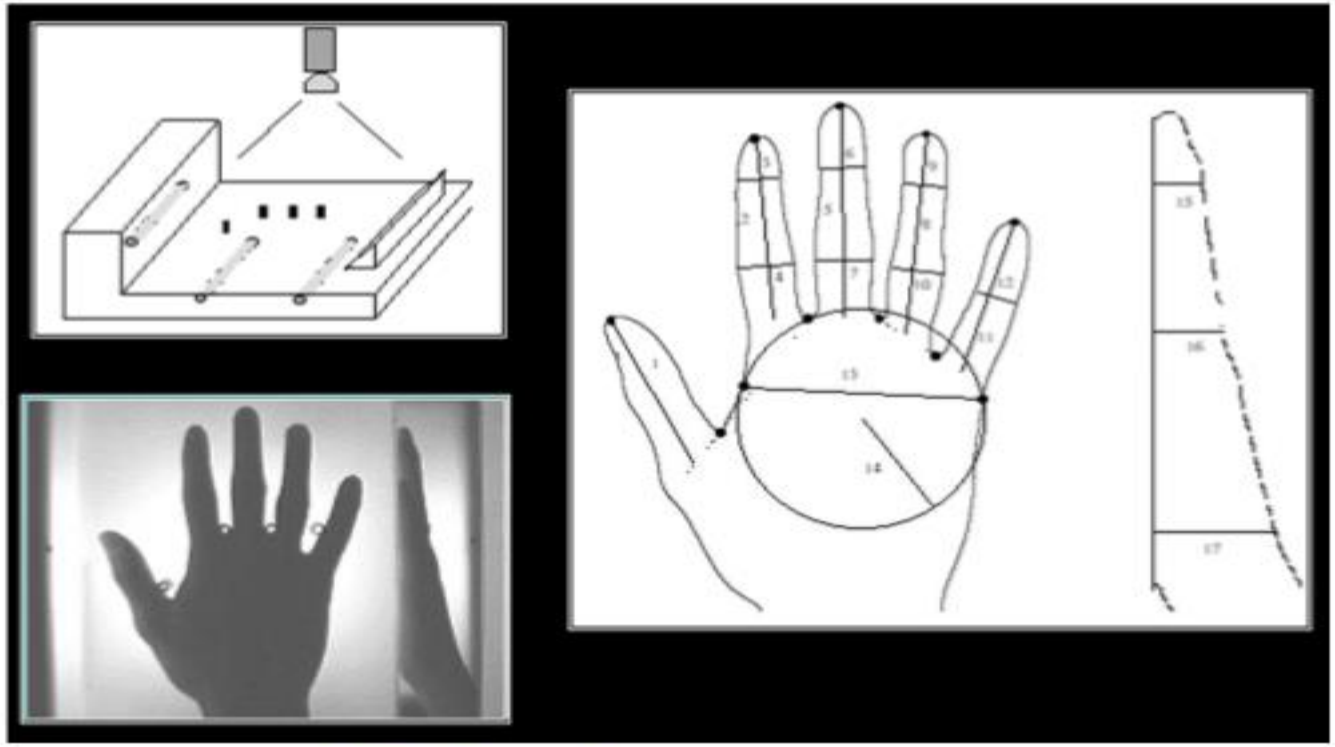
- Relativamente invarianti (anche se non molto discriminanti)
- Tecnologie tipicamente impiegate per la verifica (non adatte per applicazioni di identificazione)
- Il dispositivo di acquisizione è solitamente abbastanza voluminoso

Dispositivi per l'acquisizione della forma di dita

- Misurano solo la forma di un dito o due dita
- Preferibili per le dimensioni ridotte

UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO
Dipartimento di Informatica

Sistemi di Sicurezza



3D- hand geometry

Geometria della mano

Time & Attendance Terminal

HandPunch
Recognition Systems

Geometria del dito

FingerPhoto
BioMet Partners

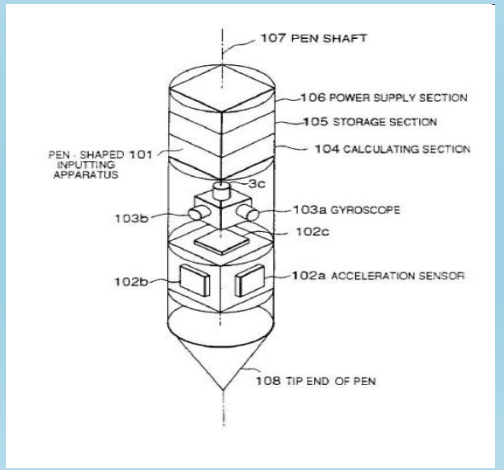
Sistemi di Sicurezza

- Signature verification. User positions himself to sign on tablet (if applicable). When prompted, user signs name in tablet's capture area. Verification time: 4-6 seconds.

Off-line

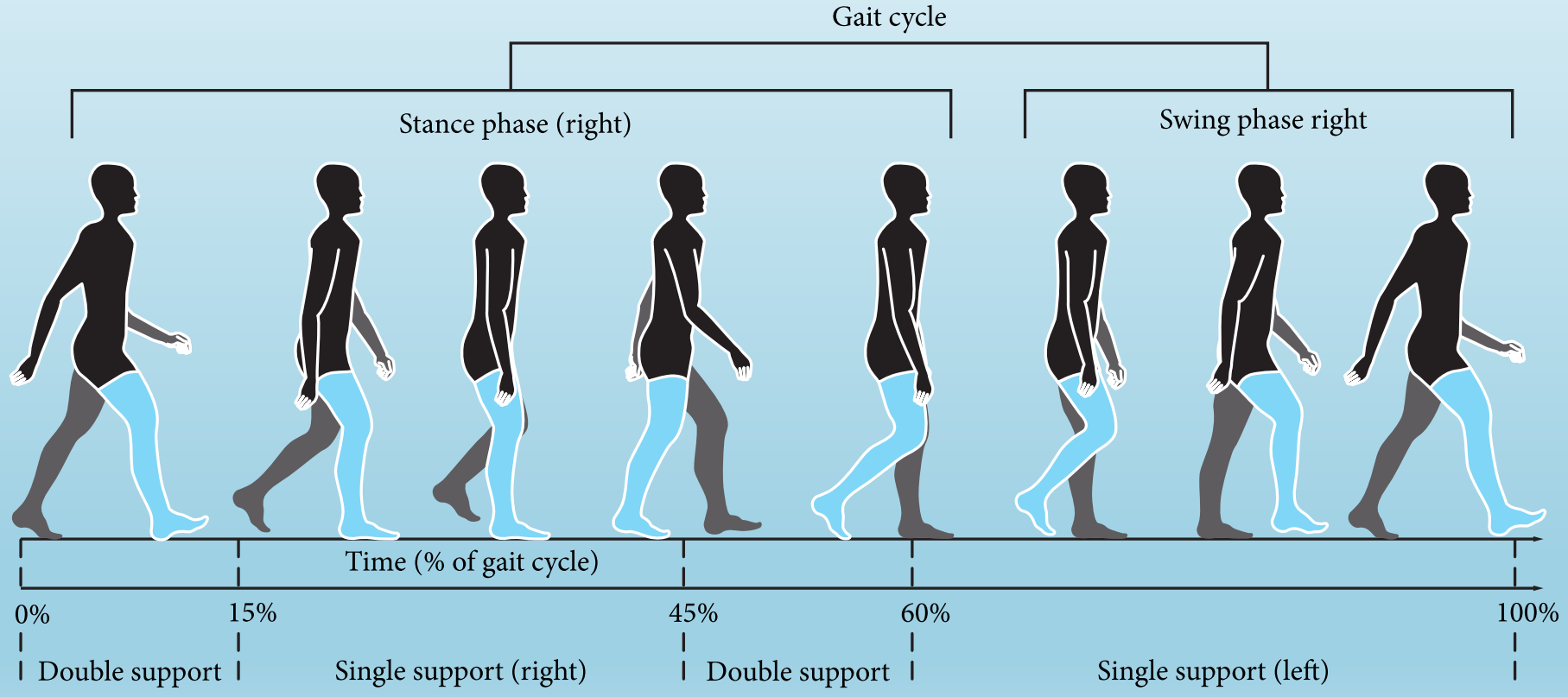
+

On-line



Sistemi di Sicurezza

- Gait: the way you walk.



Sistemi di Sicurezza

Which one?
How to compare?

Sistemi di Sicurezza

- Universality: diffusion of the biometric trait over a population

- Distinctiveness: capability of the biometric trait in distinguish two or more users:
  - among the global population
  - in a closed set

  Es:
  - DNA is the most distinctive trait: unambiguous link with individuals
  - The face:
    - same universality of DNA,
    - lower distinctiveness.

Sistemi di Sicurezza

- Permanence: tendency of the trait to not be affected by variations as time goes by.

Robustness of the trait is judged by its variability over time due to:

- age,
- injury,
- illness,
- chemical exposure etc.

Intrinsic variations:

- Short period (beard / face)
- Long period (age)

Contingent variations:

- Psychological aspects
- Physical aspects:
  - Illumination (beard / face)
  - Microphone (voice)
  - Paper/pen tipe

Sistemi di Sicurezza

- Collectability: easiness in collecting samples, including:
  1. Amount of automated tasks
  2. Amount of manual tasks
  3. Easiness in storing samples.

  DNA not very simple to be collected…

- Performance: Error Rate (ER) related to:
  1. Technological systems and theories,
  2. Parameters here listed (permanence, etc.)

Performance represents the reliability of the system.

Sistemi di Sicurezza

- Acceptability: inclination of final users:
  - To psychologically accept the recognition based on the specific trait,
  - To physically perform it.

  DNA and Retina are less acceptable then signature or voice, moreover they require full cooperation by users.

- Spoofing: possibility and easiness in fake reproduction of the biometric trait by an impostor.
  - Liveness detection

Sistemi di Sicurezza

	Universality	Distinct.	Permanence	Collectability	Performance	Acceptability	Spoof
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial Ther.	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand Geom.	M	M	M	H	M	M	M
Hand Vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Odor	H	H	H	L	L	M	L
Retina	H	H	M	L	H	L	L
Signature	M	L	L	H	L	H	H
Voice	M	L	L	H	L	H	H

H – High, M – Medium, L - Low

Sistemi di Sicurezza

A wide set of biometrics has been considered so far:

No trait is able to completely satisfy all the desirable characteristics required for a biometric system

The assessment of a biometric trait is strongly dependent on the specific application since it involves:

1. Technical issues
2. Social and cultural aspects.

Commercial applications, aspects to be considered:

- impact on the users
- costs
- easiness of implementation

Sistemi di Sicurezza

Biometrics are not expected to replace standard technologies.

Multi Factor Analysis
Fusion with existing systems

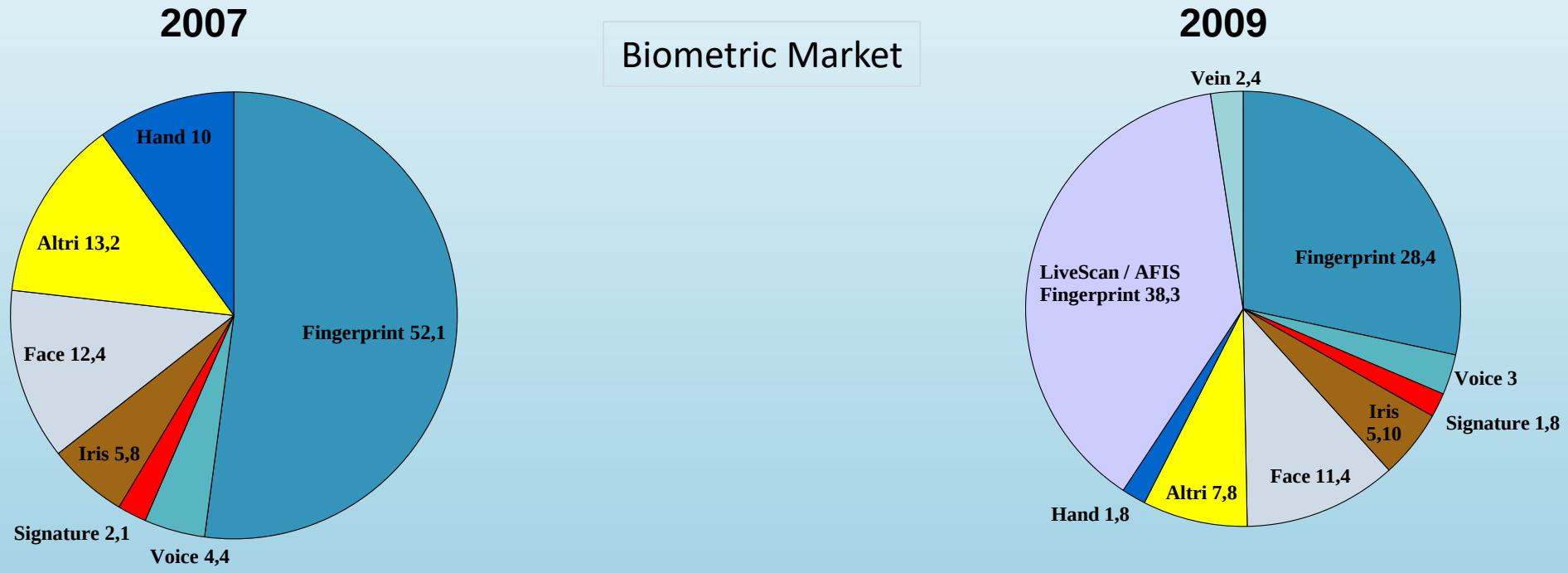
Multi biometric systems:

- Multiple fingers (fingerprints)
- Face + Voice
- Face + Eye
- Signature + Fingerprint
- Signature + Voice
- Hand Geometry + Fingerprint + Veins

Increase performance
Reduce the percentage of acquisition inability
More robust to fraud attempts

Sistemi di Sicurezza

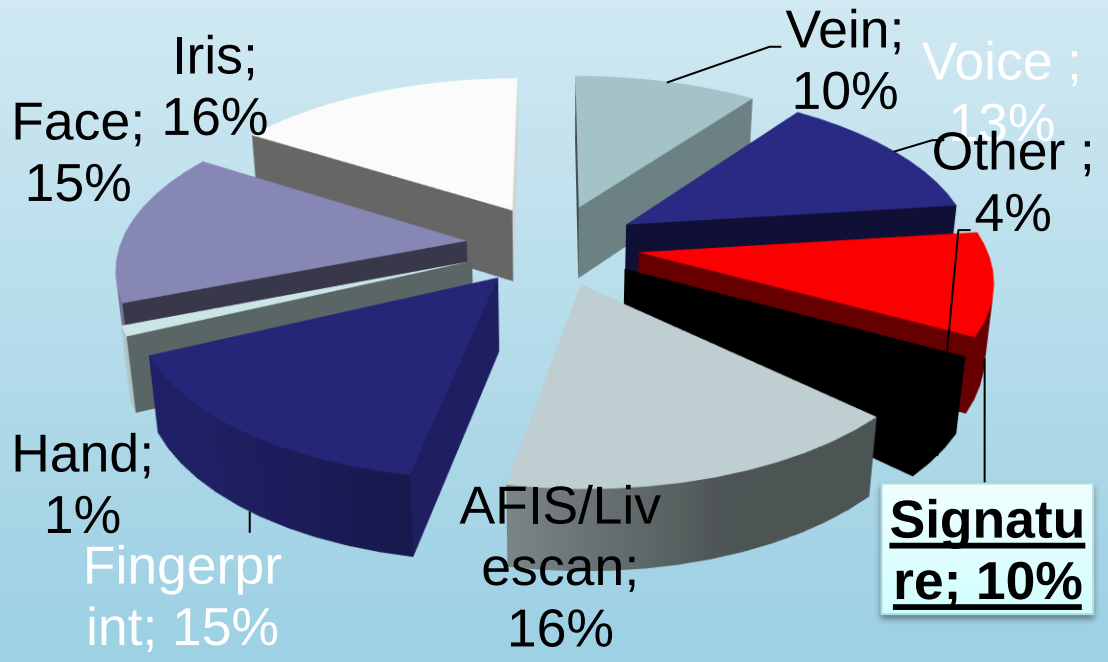
Biometric Market



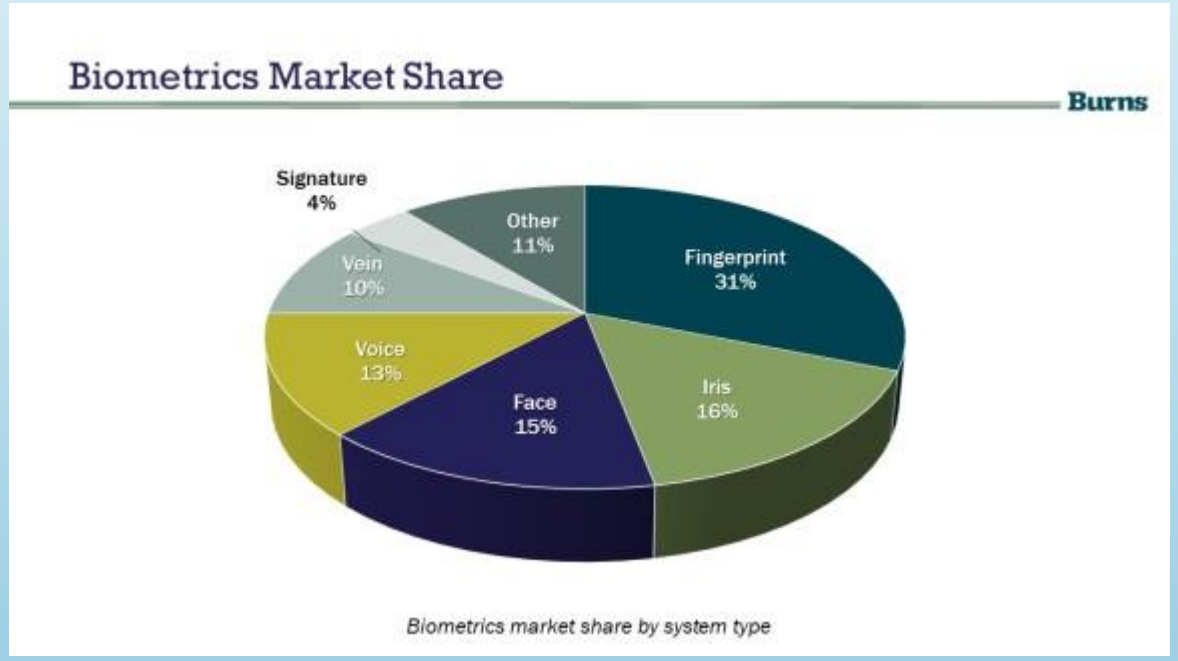
(Source: International Biometric Group)

LiveScan is the computer system that electronically captures and transmits the fingerprint images and data to an Automated Fingerprint Identification System (AFIS).
Ex.: Michigan State Police (AFIS) contains 1,285,314 fingerprints (ten fingerprints)

Sistemi di Sicurezza

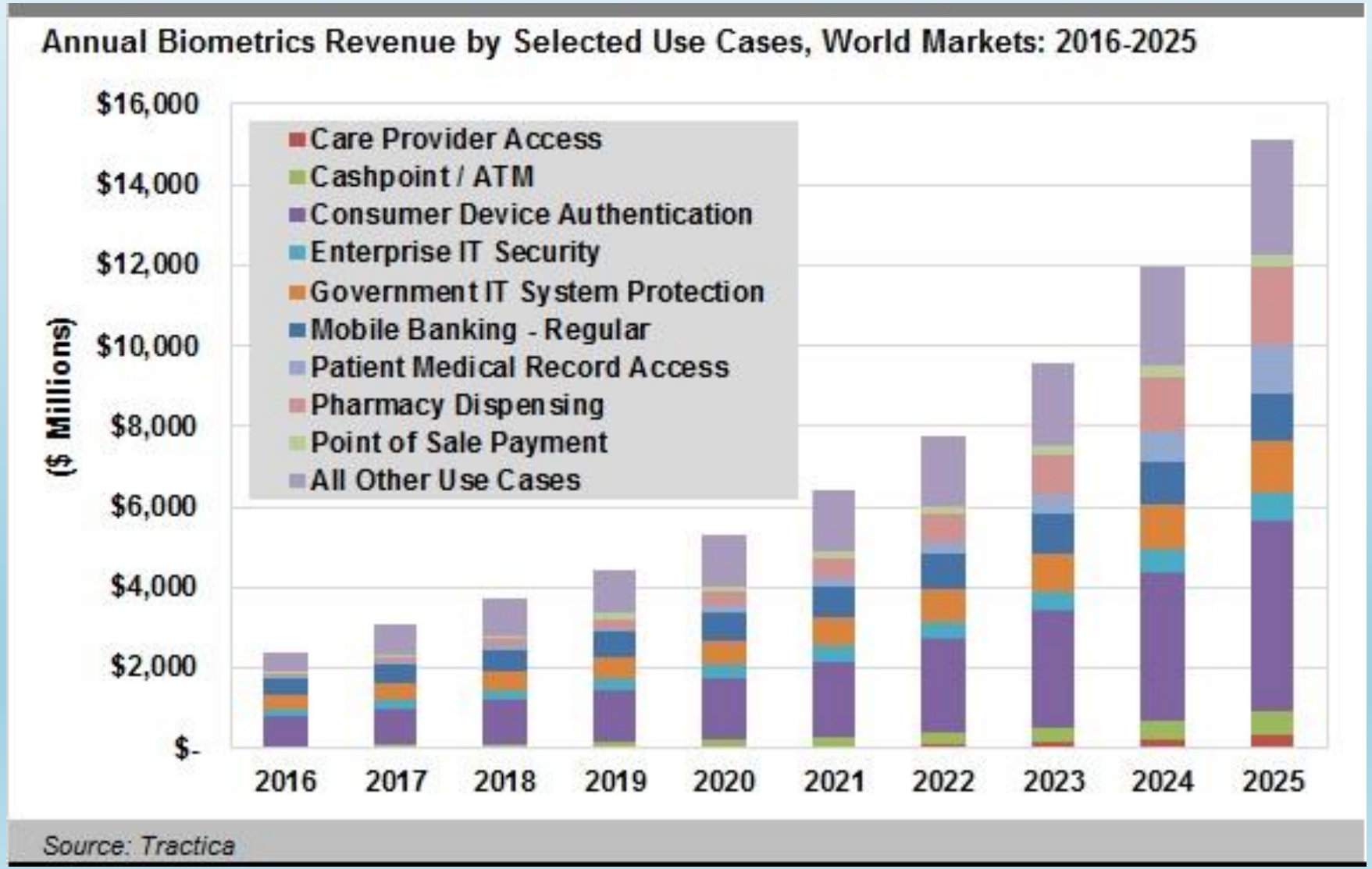


(2015)



(2020)

Sistemi di Sicurezza



Sistemi di Sicurezza

Scenario Globale

USA

- sviluppo di programmi di formazione del personale
- creare competenze e forza lavoro

CINA

- favorire cooperazione tra aziende, università e intelligence militare

UK

- sostenere la formazione e la cultura della cyber-security a livello nazionale
- interagire con le aziende private sullo scambio di informazioni e sostenere l'adozione di best practices

FRANCIA

- acquisire soluzioni tecniche e risorse umane

Mercato del lavoro (fonte http://www.cyberdegrees.org)

Chief Information Security Officer

Security Manager

Forensic Expert

Incident Responder

Penetration Tester

Security Administrator

Security Analyst

Security Auditor

Security Consultant

Security Software developer

Vulnerability Assessor

Sistemi di Sicurezza

Sbocchi Professionali

- → Secure ICT service settori civili e militari
- → Aziende specializzate in cyber security
- → Industria
- → Telecomunicazioni e media
- → Società di servizi / consulenza
- → Banche - Assicurazioni
- → Logistica e trasporti
- → Settori R&D

Mercato del lavoro

- Italia (March 2020) Information Security:
  - Indeed >197 annunci
  - Linkedin >276 annunci
  - Monster > 98 annunci
  - Careerjet > 500 annunci

Italia (Febr. 2022):

Indeed >423 annunci
Linkedin >661 annunci
Monster > 100 annunci
Careerjet > 904 annunci

- Titolo di studio:
  - Laurea magistrale in Computer Science, Computer Systems or related field;
  - Laurea specialistica o formazione superiore (es. master o corsi specialistici universitari in ambito ICT security) conseguita nei tempi;
    - Tesi in sicurezza informatica
  - Laurea Magistrale in Sicurezza Informatica

Mercato del lavoro – entry level skills

Profili Manageriali: Conoscenza di:

- metodologie,
- Framework,
- best practice,
- standard internazionali,

di Information Security, IT Risk & Security Assessment, Governance&Compliance e Data Privacy/Data Protection

Profili Tecnici: Esperienza nella realizzazione di progetti accademici nell'area Information Security (Security Strategy, Security Governance, IT Risk Analysis, Business Continuity & Disaster Recovery, Threat & Vulnerability Assessment)

- Conoscenza di soluzioni tecnologiche di sicurezza informatica
- Analisi dei requisiti e disegno di architetture di soluzioni di sicurezza
- Conoscenza di politiche, modelli e meccanismi di controllo degli accessi;
- Economia della sicurezza IT, visione strategica del conflitto tra sicurezza e business;

Mercato del lavoro – entry level skills

- Eccellente percorso accademico
  - Voto
  - Tempi
- Ottima conoscenza della lingua inglese parlata e scritta
- Essere costantemente focalizzato sul risultato, sulla responsabilità individuale e sulla qualità del lavoro;
- Ottime capacità di comunicazione e relazione
- Orientamento al teamworking

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO
Dipartimento di Informatica

Laurea Magistrale in Sicurezza Informatica LM-66

L'Offerta di UNIBA: Percorso e suoi obiettivi

Classe LM-66 – Classe delle lauree magistrali in Sicurezza Informatica, presso la sede di TARANTO.

Obiettivo: Formare specialisti per attività di

- **analisi**,
- **progettazione**,
- **sviluppo**,
- **testing**,
- **assessment, coordinamento e gestione**

di **sistemi informatici sicuri.**

Fornire competenze

- **informatiche,**
- **di gestione aziendale,**
- **aspetti giuridici,**

che riguardano il trattamento dei dati da un punto di vista della loro elaborazione, trasmissione e conservazione.

Laurea Magistrale in Sicurezza Informatica LM-66

Elenco dei principali corsi/argomenti

- Approcci per la segretezza delle informazioni ed **integrità dei dati**;
- Metodi e principi per la realizzazione di **architetture sicure**;
- Sicurezza nelle reti e nei **sistemi distribuiti**;
- Tecniche e metodi per l'**analisi della sicurezza**;
- Tecniche e metodi per l'autenticazione in **sistemi biometrici**;
- **Regolamentazione giuridica** circa l'utilizzo di soluzioni informatiche per la sicurezza;
- Processi per la valutazione e tecniche per la **mitigazione del rischio.**

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO
Dipartimento di Informatica

Laurea Magistrale in Sicurezza Informatica LM-66

Corsi/argomenti (1° anno)

I semestre		
Lingua Inglese	L-LIN/12	Competenze Linguistiche
Sicurezza nelle reti e nei sistemi distribuiti	INF/01	Competenze Informatiche
Crittografia	INF/01	Competenze Informatiche
Analisi dei dati per la sicurezza	ING/INF-05	Competenze Informatiche
Trattamento dei dati sensibili	IUS/04	Competenze Giuridiche
II semestre		
Sistemi biometrici	ING/INF-05	Competenze Informatiche
Organizzazione aziendale	SECS-P/10	Competenze Socio-Economiche
Sicurezza nelle applicazioni	ING/INF-05	Competenze Informatiche
Analisi e gestione del rischio	SECS-S/01	Competenze Socio-Economiche

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO
Dipartimento di Informatica

Laurea Magistrale in Sicurezza Informatica LM-66

Corsi/argomenti (2° anno)

I semestre		
Metodi formali per la sicurezza	INF/01	Competenze Informatiche
Sicurezza in ambienti mobile	INF/01	Competenze Informatiche
Sicurezza delle architetture orientate ai servizi	ING/INF-05	Competenze Informatiche
Insegnamenti a scelta		
II Semestre		
Tirocinio presso aziende del settore, enti pubblici o privati e laboratori dell'Università (20 CFU)		

Progettazione di Sistemi Sicuri	INF/01 – INF-ING/05	Competenze Informatiche
Informatica Forense	INF/01 – INF-ING/05	Competenze Informatiche
Informatica Giuridica	IUS/20	Competenze Giuridiche
Teoria dell'informazione	INF/01	Competenze Informatiche
Logica applicata	INF/01	Competenze Informatiche

UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO
Dipartimento di Informatica

Sistemi di sicurezza

Prof. Donato Impedovo

CICSI *Consiglio Interclasse dei Corsi di Studio in Informatica*