Fondamenti di Cyber Security

Giacomo Tesio

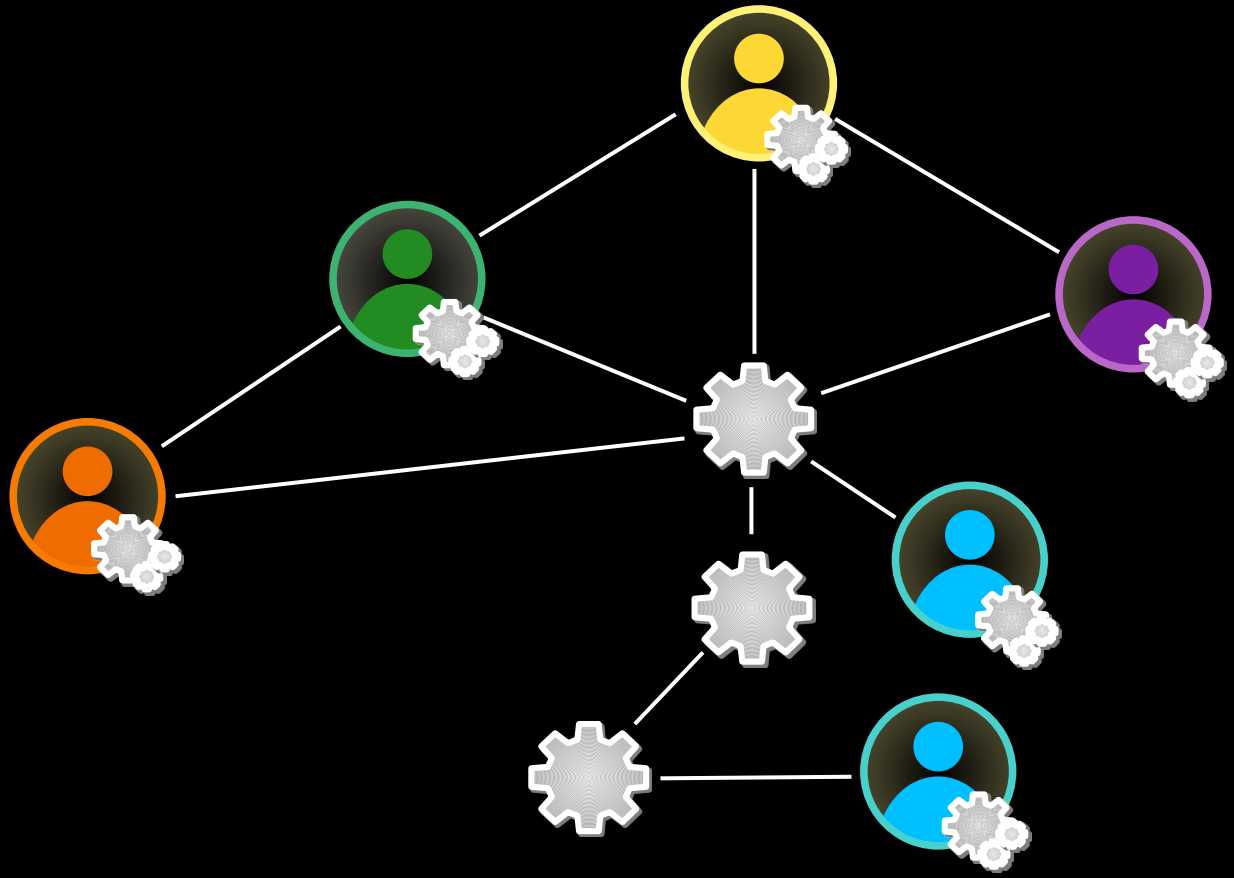
La Sicurezza Informatica…
sul Lavoro

Sicurezza

"*sine cura*" – senza preoccupazione

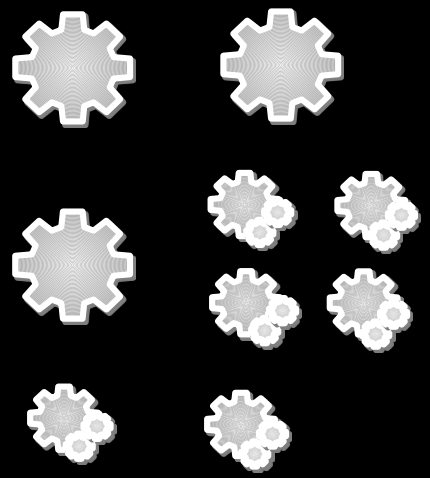
Definiamo "sicuro" un sistema progettato in modo tale che la sua evoluzione non può produrre effetti indesiderati.

Organizzazione Cibernetica



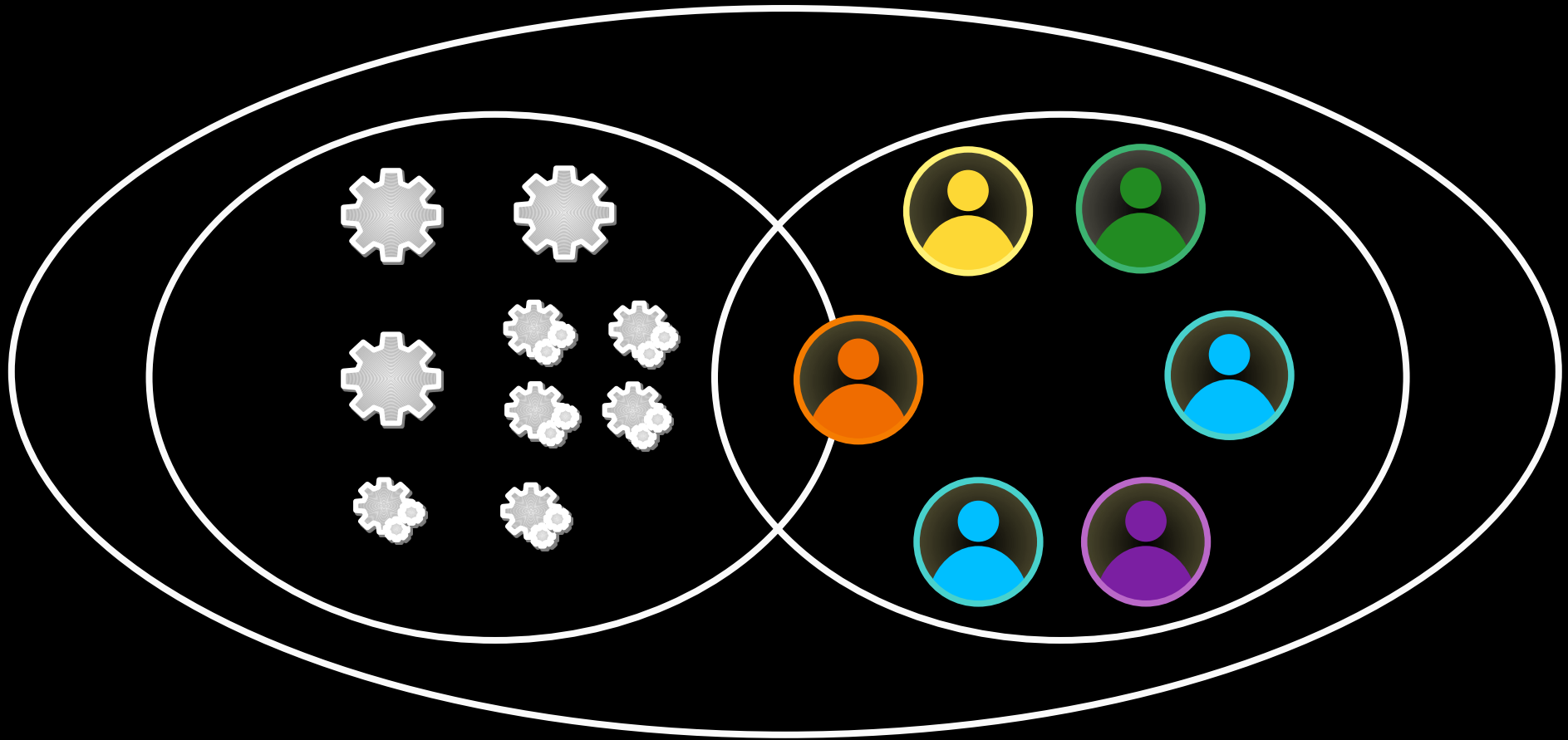
Organizzazione Cibernetica

Automatismi



Autonomie

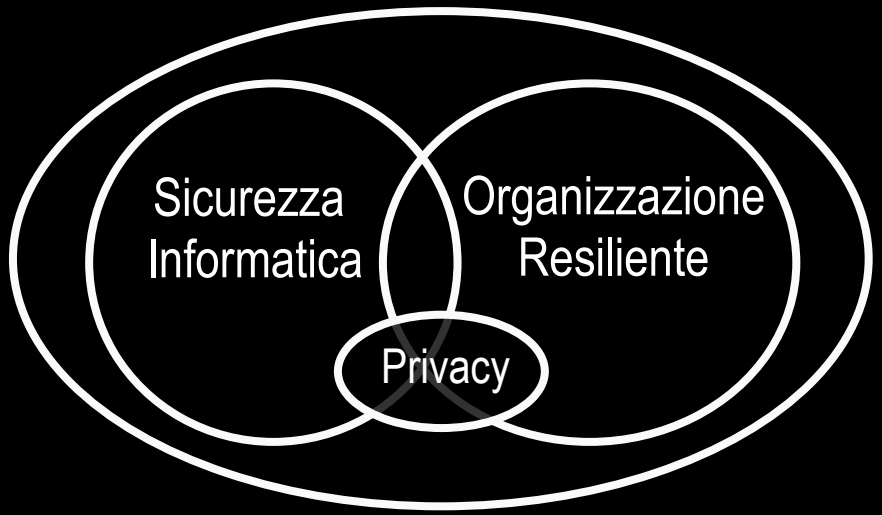
Sicurezza Cibernetica



Sicurezza Cibernetica

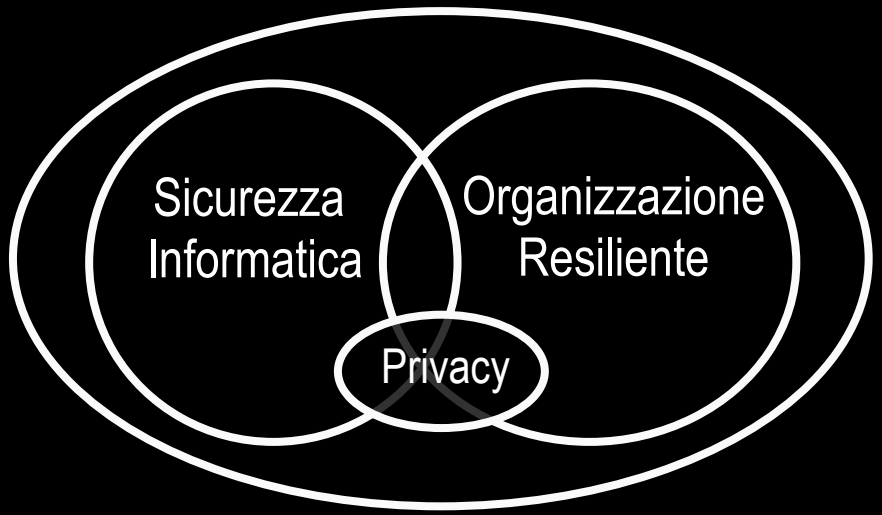
Sicurezza Cibernetica

Sicurezza Cibernetica

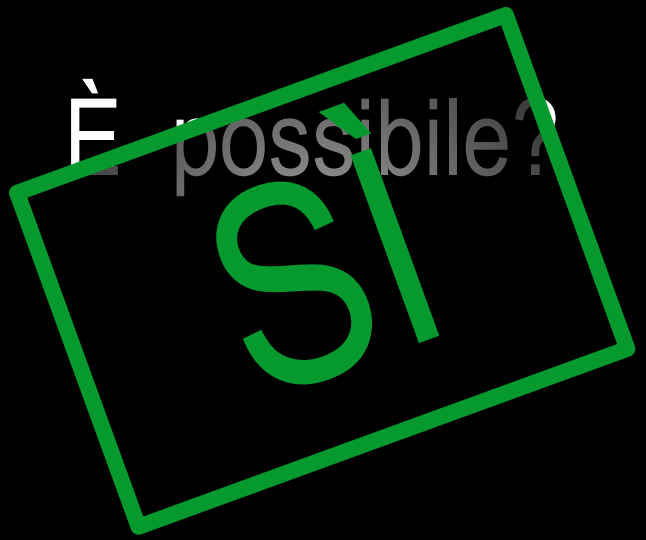


È possibile?

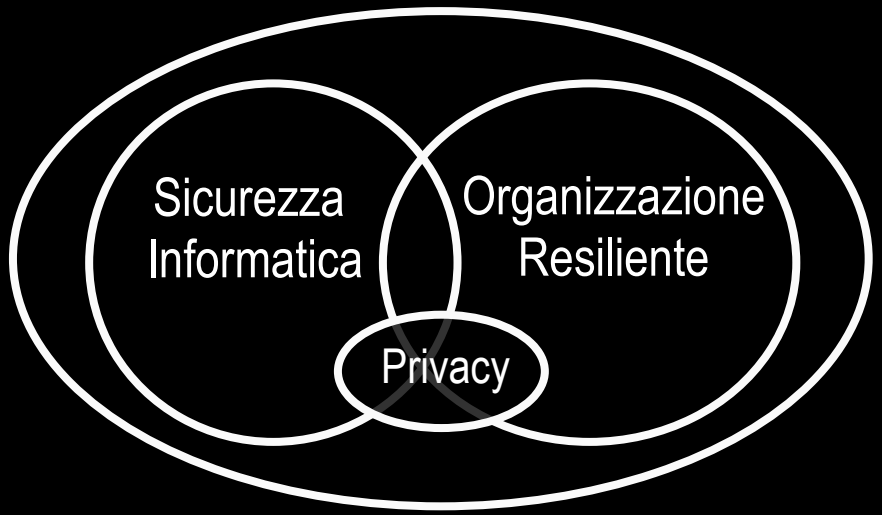
Sicurezza Cibernetica



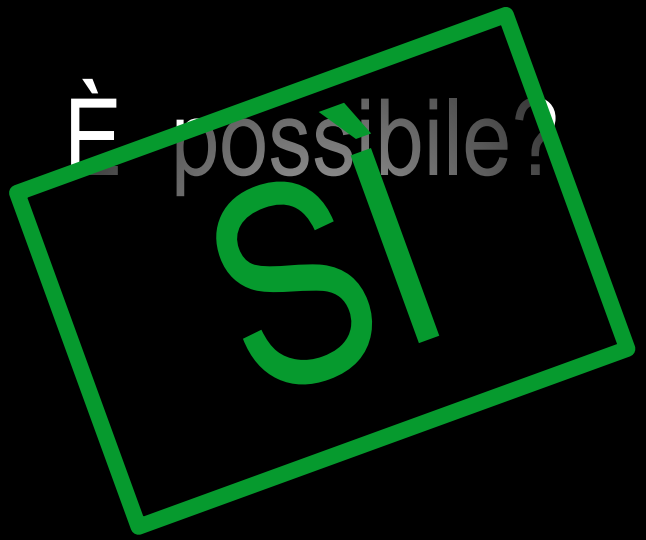
È possibile?



Sicurezza Cibernetica

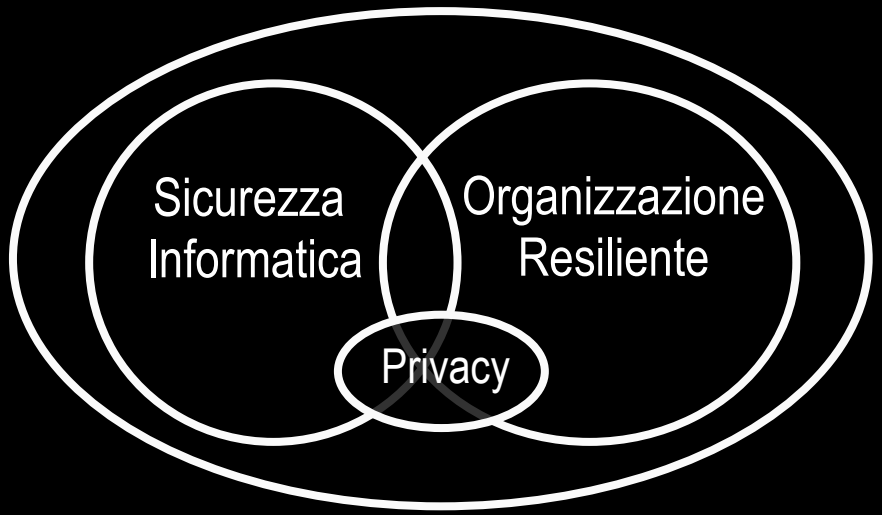


È possibile?



...ma può essere costosa!

Sicurezza Cibernetica



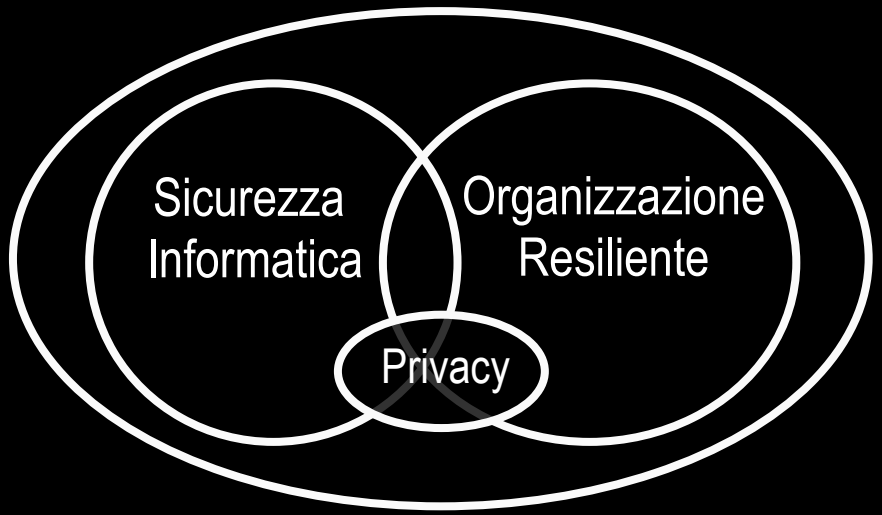
È possibile?

SÌ

...ma può essere costosa!

...tanto più costosa quanto più fragile ed iniqua è l'organizzazione

Sicurezza Cibernetica



È possibile?

SÌ

...ma può essere costosa!

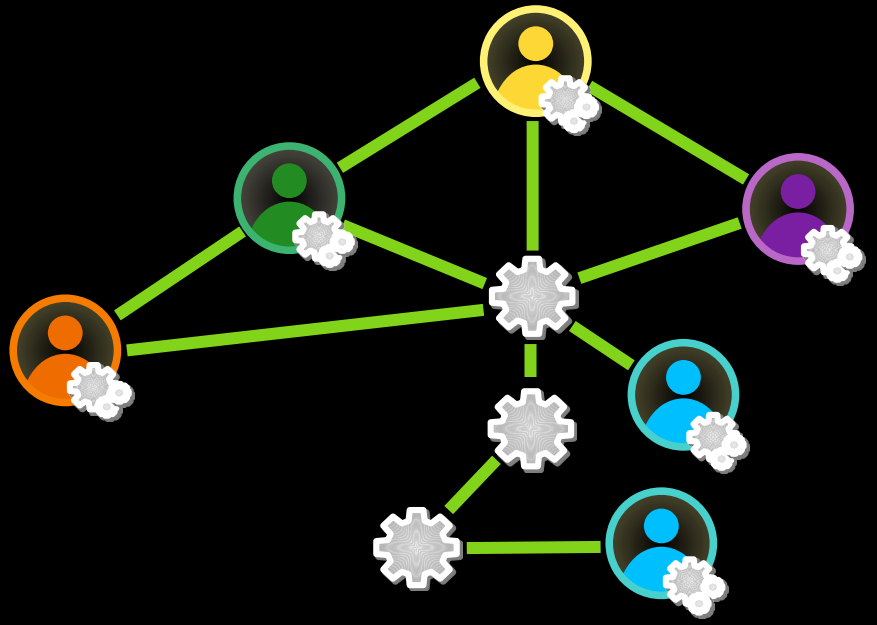
...tanto più costosa quanto più fragile ed iniqua è l'organizzazione

si preferisce scaricarne i rischi sui lavoratori e i danni sulla società

Sicurezza Cibernetica

Sicurezza Cibernetica

Sicurezza Informatica



La Sicurezza Informatica si occupa esclusivamente dei

DATI

Sicurezza Informatica

Insieme di procedure atte a

- garantire l'accesso ai dati alle persone autorizzate
- impedire l'accesso ai dati alle persone **non** autorizzate

Sicurezza Informatica

Insieme di procedure atte a

- garantire l'accesso ai dati alle persone autorizzate
- impedire l'accesso ai dati alle persone **non** autorizzate

Sicurezza Informatica

Insieme di procedure atte a

- garantire l'accesso ai dati alle persone autorizzate
- impedire l'accesso ai dati alle persone **non** autorizzate

Modalità di Accesso DIRETTO

- lettura → copia
- scrittura (aggiunta o modifica)
- esecuzione in locale → accessibilità fisica del binario
  ~~nel "cloud"~~ → software inaccessibile (e "personalizzato")

Accesso INDIRETTO: mediato da automatismi

Sicurezza Informatica

Insieme di procedure atte a

- garantire l'accesso ai dati alle persone autorizzate
- impedire l'accesso ai dati alle persone **non** autorizzate

Diritto positivista: autorizzazione ↔ autorità

- riconosciuto
- protetto
- esercitato

} da chi? come?

Sicurezza Informatica

Insieme di procedure atte a

- garantire l'accesso ai dati alle persone autorizzate
- impedire l'accesso ai dati alle persone **non** autorizzate

Diritto positivista: autorizzazione ↔ autorità

- riconosciuto
- protetto
- esercitato

} da chi? come?

Chi controlla i vostri dati?

Chi li "protegge"
può autorizzarvi ad accedere
può impedirvi di accedere

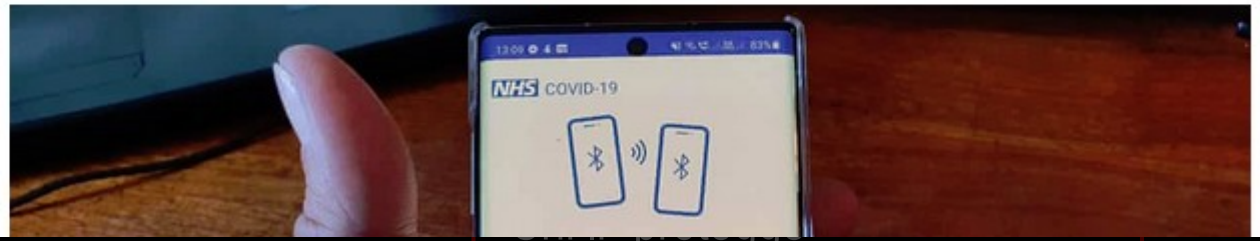
Sicurezza Informatica

Coronavirus outbreak

UK poised to abandon coronavirus app in favour of Apple and Google models

Government will switch to contact-tracing models preferred by smartphone giants in latest embarrassing U-turn

- **Coronavirus - latest updates**
- **See all our coronavirus coverage**



Dan Sabbagh

Thu 18 Jun 2020 09.21 EDT

5,556

– esercitato

può autorizzarvi ad accedere
può impedirvi di accedere

Sicurezza Informatica

Insieme di procedure atte a

- garantire l'accesso ai dati alle persone autorizzate
- impedire l'accesso ai dati alle persone **non** autorizzate

Autonomia → Responsabilità

- *responsum abilem*, capace di spiegare le proprie azioni
  - presuppone conoscenza approfondita del sistema
- presuppone identificabilità → autenticazione degli accessi
  - l'identificativo dichiarato deve corrispondere all'identità autorizzata

Sicurezza Informatica

Insieme di procedure atte a

- garantire l'accesso ai dati alle persone autorizzate
- impedire l'accesso ai dati alle persone **non** autorizzate

Autonomia → Responsabilità → Autenticazione

- credenziali di accesso → segrete (parola d'ordine, firma PGP, 2FA...)
- verificare che l'identità apparente o dichiarata da un membro dell'organizzazione cibernetica corrisponda a quella effettiva
  - furto di identità, per le persone
  - phishing per gli automatismi: siti web, email, spot wifi...

Sicurezza Informatica

Insieme di procedure atte a

- garantire l'accesso ai dati alle persone autorizzate
- impedire l'accesso ai dati alle persone **non** autorizzate

Autonomia → Responsabilità → Autenticazione

- credenziali di accesso → segrete (parola d'ordine, firma PGP, 2FA...)
- verificare che l'identità apparente o dichiarata da un membro dell'organizzazione cibernetica corrisponda a quella effettiva
  - furto di identità, per le persone
  - phishing per gli automatismi: siti web, email, spot wifi...

Gli automatismi **non** hanno identità propria: la loro autenticazione serve ad identificare **chi** li controlla

Sicurezza In

Insier … e a
- ga… … i alle p…
- imp… … i alle p… …e

Auton… … à → A…
- cre… … te (paro…
- verificare che l'identità apparente o dich…
  dell'organizzazione cibernetica corrispo…
  - furto di identità, per le persone
  - phishing per gli automatismi: siti we…

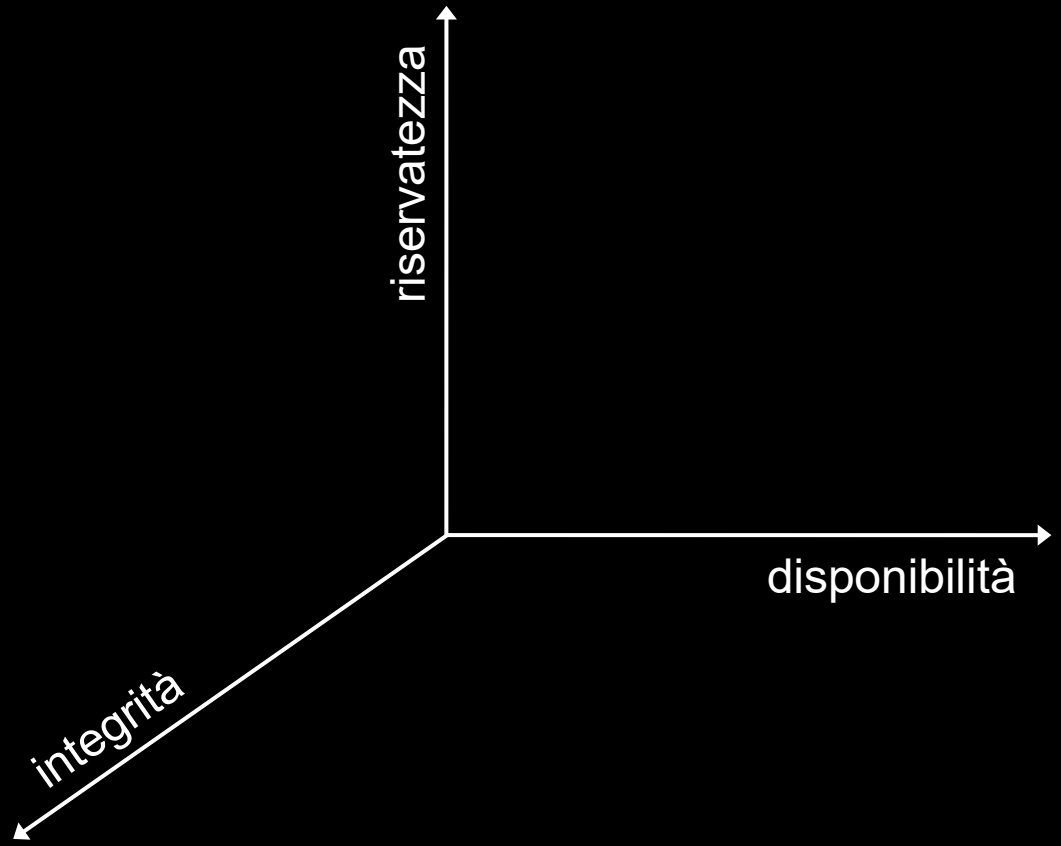
…tomatismi **non**
identità propria:
autenticazione
ad identificare
i li controlla

Sicurezza Informatica

1. Classificare Dati e Canali
   - riservatezza
   - integrità
   - confidenzialità

   } esigenze da garantire
2. Proteggere i Dati
3. Minimizzare i Rischi

Sicurezza Informatica

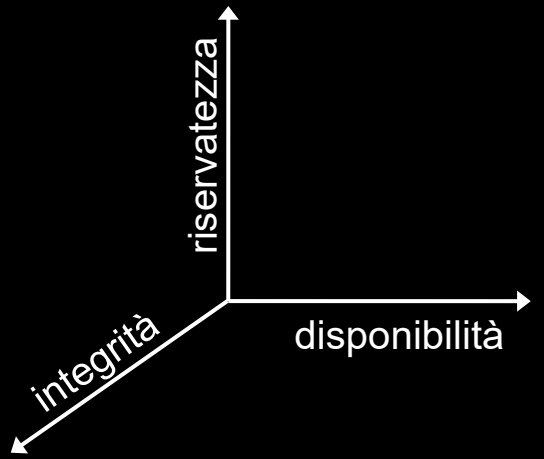


3 esigenze ortogonali

- riservatezza
- integrità
- disponibilità

} diverse per ogni dato

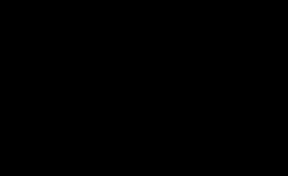
Riservatezza dei Dati



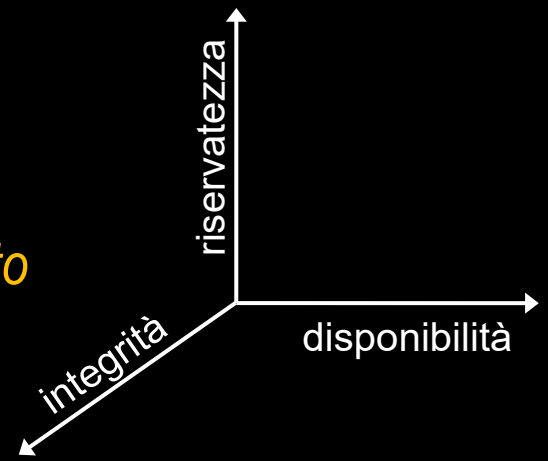
Che succederebbe se questo dato venisse diffuso?

Garantire la riservatezza di un dato significa garantire che solo chi è autorizzato possa effettivamente accedervi

Riservatezza dei Dati



Che succederebbe se questo dato venisse diffuso?

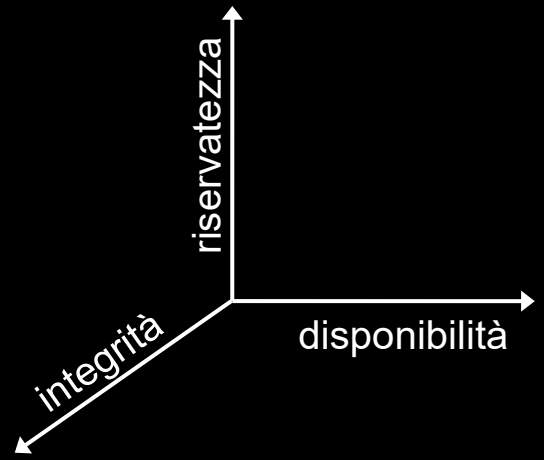


Livelli di riservatezza necessaria:

- Pubblico → può essere pubblicato su un giornale
- Interno → cultura dell'organizzazione: manuali, guide…
- Ristretto → dati operativi dell'organizzazione: configurazioni software...
- Confidenziale → dati protetti dalla legge: GDPR, segreti professionali, bancari…
- Segreto → dati la cui diffusione può causare la fine dell'organizzazione

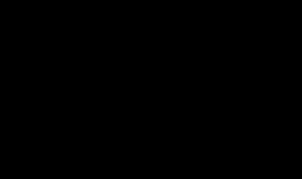
Integrità dei Dati

Che succederebbe se questo dato venisse manomesso?

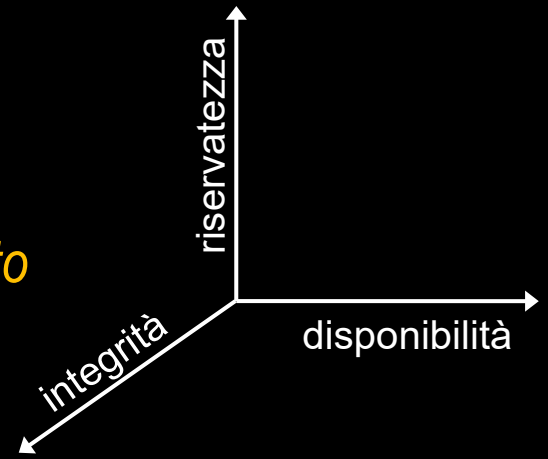


Garantire l'integrità di un dato significa garantire che non possa subire alterazioni non previste dalle regole dell'organizzazione

Riservatezza dei Dati



Che succederebbe se questo dato venisse manomesso?

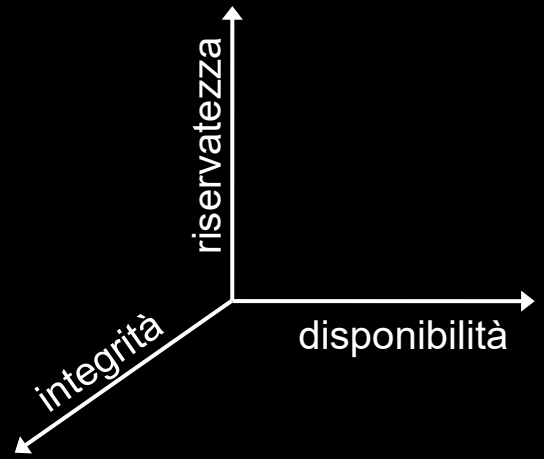


Livelli di integrità necessaria:

- Normale → la manomissione del dato comporta costi sostenibili
- Importante → la manomissione del dato comporta danni irreversibili
  - a membri dell'organizzazione
  - all'organizzazione nel suo complesso
- Vitale → la manomissione del dato può causare la fine dell'organizzazione o la morte di uno o più dei suoi membri

Disponibilità dei Dati

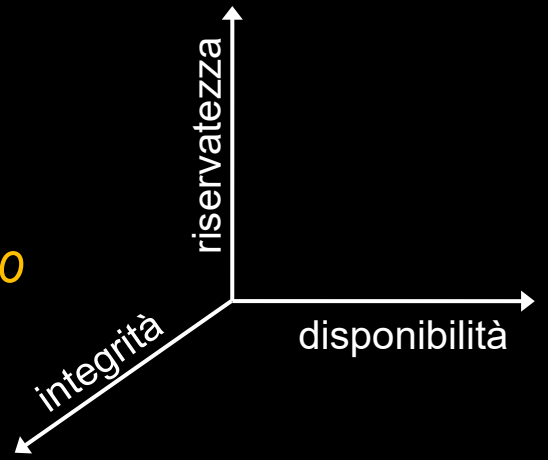
Che succederebbe se questo dato venisse perso?



Garantire la disponibilità di un dato significa garantire che chi è autorizzato possa effettivamente accedervi in tempi compatibili con le esigenze dell'organizzazione

Disponibilità dei Dati

Che succederebbe se questo dato venisse perso?



Classi di disponibilità necessaria:

Classe 2 → il dato deve essere disponibile il 99% del tempo

- il dato **non** sarà disponibile per 500 minuti ogni anno (~ 8 ore)

Classe 4 → il dato deve essere disponibile il 99.99% del tempo

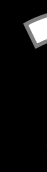
- il dato **non** sarà disponibile per 1 ora ogni anno

Classe 7 → il dato deve essere disponibile il 99.99999% del tempo

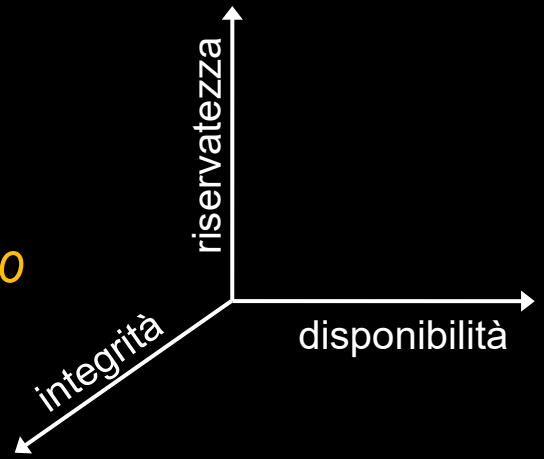
- il dato **non** sarà disponibile per 1 secondo ogni anno

…

Disponibilità dei Dati



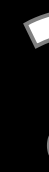
Che succederebbe se questo dato venisse perso?



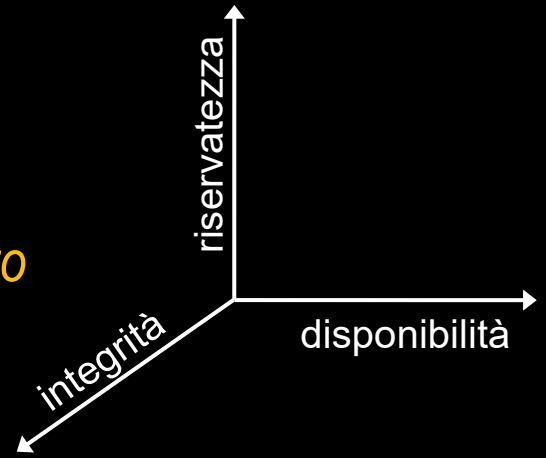
Cause "*low tech*"

- cancellazione involontaria
- difetti hardware
- furti
  - portatili
  - smartphone
  - chiavette USB
- incendi

Disponibilità dei Dati



Che succederebbe se questo dato venisse perso?

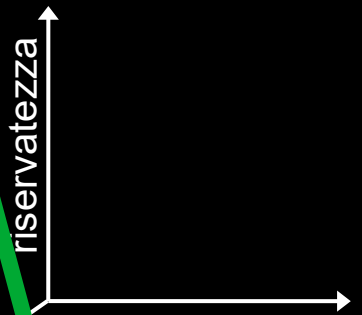


Cause "*low tech*"

- cancellazione involontaria
- difetti hardware
- furti
  - portatili
  - smartphone
  - chiavette USB
- incendi

Il **70%** delle aziende che perdono i propri dati per un incendio dichiara fallimento entro 1 anno.

Disponibilità dei Dati



? *Che succederebbe se questo dato venisse perso?*

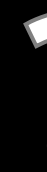
Cause "*low tech*"

- cancellazione involontaria
- difetti hardware
- furti
  - portatili
  - smartphone
  - chiavette USB
- incendi

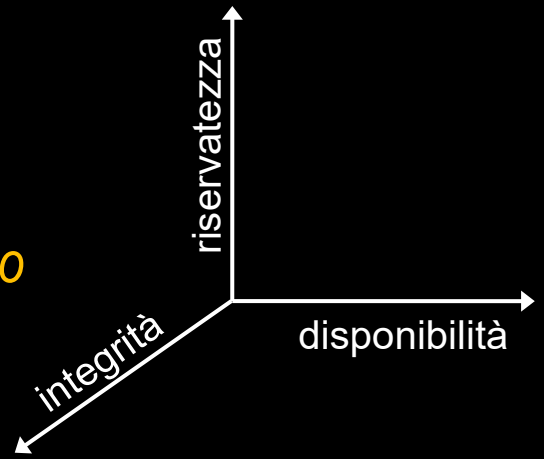
BACKUP !!!

Il **70%** delle aziende che perdono i propri dati per un incendio dichiara fallimento entro 1 anno.

Disponibilità dei Dati



Che succederebbe se questo dato venisse perso?

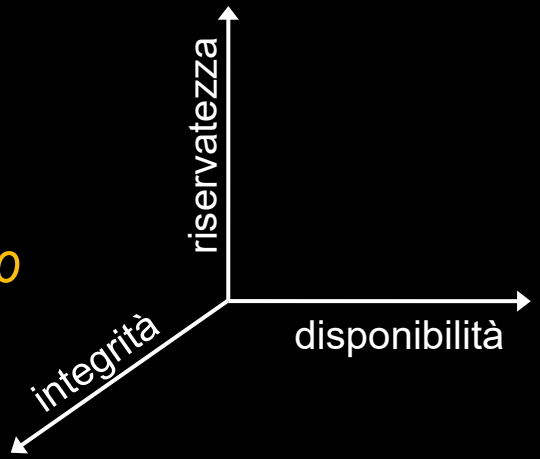


Cause "*low tech*"

- cancellazione involontaria
- difetti hardware
- furti
  - portatili
  - smartphone
  - chiavette USB
- incendi

Disponibilità dei Dati

Che succederebbe se questo dato venisse perso?



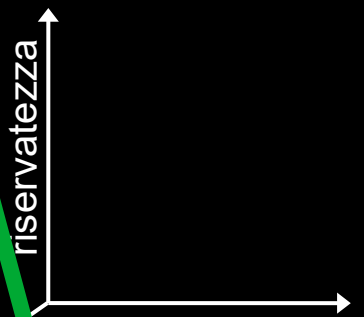
Cause "*low tech*"

- cancellazione involontaria
- difetti hardware
- furti
  - portatili
  - smartphone
  - chiavette USB
- incendi

Cause "*high tech*"

- distributed denial of service (DDoS)
  - solo per i dati online !
- supply chain attacks
  - node-ipc (protestware anti-russo)
- ransomware

Disponibilità dei Dati



? *Che succederebbe se questo dato venisse perso?*

Cause "*low tech*"

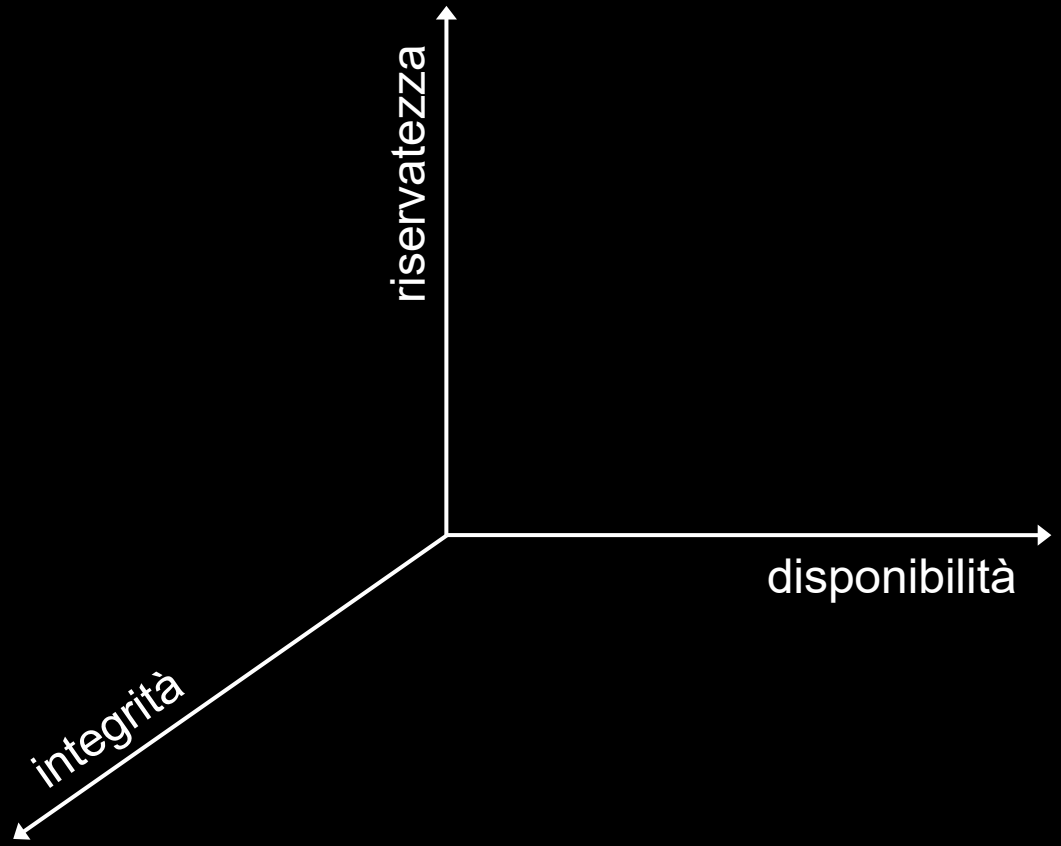
- cancellazione involontaria
- difetti hardware
- furti
  - portatili
  - smartphone
  - chiavette USB
- incendi

Cause "*high tech*"

- distributed denial of service (DDoS)
  - solo per i dati online !
- supply chain attacks
  - node-ipc (protestware anti-russo)
- ransomware

BACKUP!!!

Sicurezza Informatica



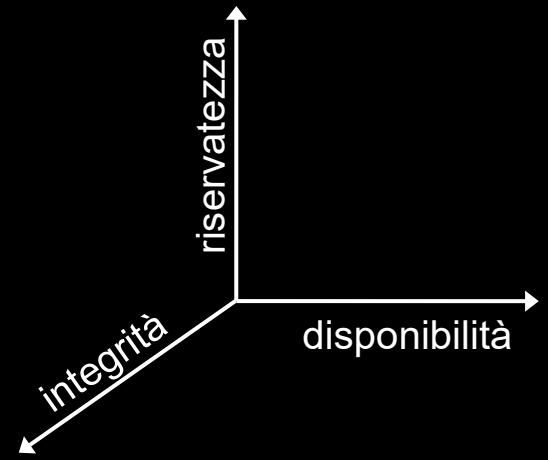
3 esigenze ortogonali

- riservatezza
- integrità
- disponibilità

} diverse per ogni dato

ESEMPI

Classificazione dei Dati

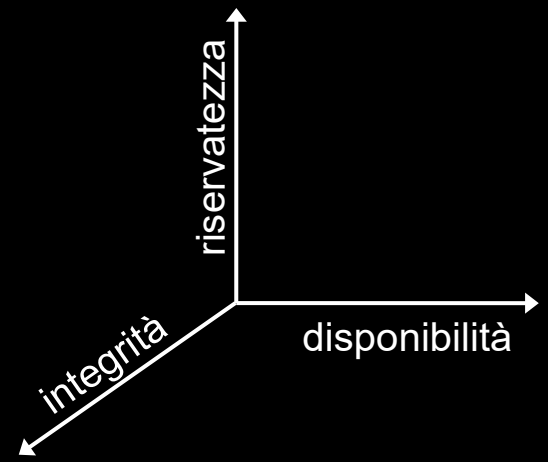


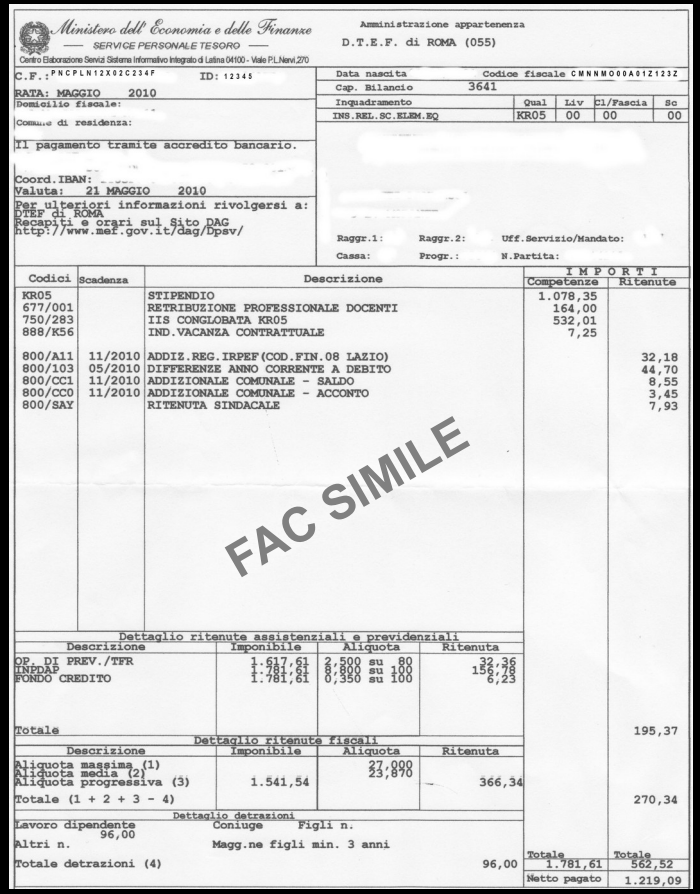
Riservatezza: Pubblico

Integrità: Normale

Disponibilità: Classe 1

Classificazione dei Dati





Ministero dell'Economia e delle Finanze
SERVICE PERSONALE TESORO
Centro Elaborazione Servizi Sistema Informativo Integrato di Latina 04100 - Viale P.L.Nervi,270

Amministrazione appartenenza
D.T.E.F. di ROMA (055)

C.F.: PNCPLN12X02C234F ID: 12345
RATA: MAGGIO 2010
Domicilio fiscale:
Comune di residenza:
Il pagamento tramite accredito bancario.
Coord.IBAN:
Valuta: 21 MAGGIO 2010
Per ulteriori informazioni rivolgersi a:
DTEF di ROMA
Recapiti e orari sul Sito DAG
http://www.mef.gov.it/dag/Dpsv/

Data nascita | Codice fiscale CMNNMO00A01Z133Z
Cap. Bilancio 3641

Inquadramento	Qual	Liv	Cl/Fascia	Sc
INS.REL.SC.ELEM.EQ	KR05	00	00	00

Raggr.1: Raggr.2: Uff.Servizio/Mandato:
Cassa: Progr.: N.Partita:

Codici	Scadenza	Descrizione	IMPORTI Competenze	Ritenute
KR05		STIPENDIO	1.078,35	
677/001		RETRIBUZIONE PROFESSIONALE DOCENTI	164,00	
750/283		IIS CONGLOBATA KR05	532,01	
888/K56		IND.VACANZA CONTRATTUALE	7,25	
800/A11	11/2010	ADDIZ.REG.IRPEF(COD.FIN.08 LAZIO)		32,18
800/103	05/2010	DIFFERENZE ANNO CORRENTE A DEBITO		44,70
800/CC1	11/2010	ADDIZIONALE COMUNALE - SALDO		8,55
800/CC0	11/2010	ADDIZIONALE COMUNALE - ACCONTO		3,45
800/SAY		RITENUTA SINDACALE		7,93

FAC SIMILE

Dettaglio ritenute assistenziali e previdenziali

Descrizione	Imponibile	Aliquota	Ritenuta
OP. DI PREV./TFR	1.617,61	2,500 su 80	32,36
INPDAP	1.781,61	8,800 su 100	156,78
FONDO CREDITO	1.781,61	0,350 su 100	6,23
Totale			195,37

Dettaglio ritenute fiscali

Descrizione	Imponibile	Aliquota	Ritenuta
Aliquota massima (1)		27,000	
Aliquota media (2)		23,870	
Aliquota progressiva (3)	1.541,54		366,34
Totale (1 + 2 + 3 - 4)			270,34

Dettaglio detrazioni

Lavoro dipendente 96,00 Coniuge Figli n.
Altri n. Magg.ne figli min. 3 anni
Totale detrazioni (4) 96,00

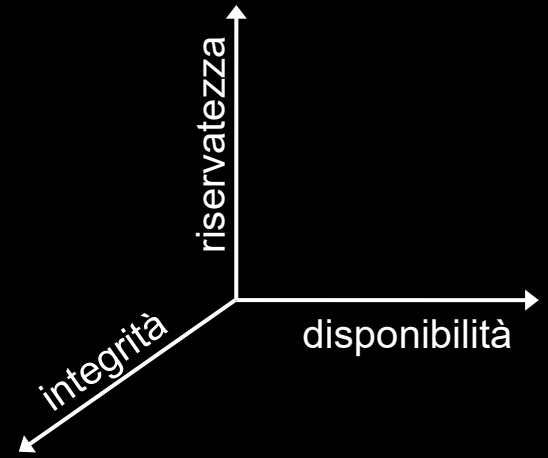
	Totale Competenze	Totale Ritenute
	1.781,61	562,52
Netto pagato		1.219,09

Riservatezza: Confidenziale

Integrità: Importante

Disponibilità: Classe 4

Classificazione dei Dati



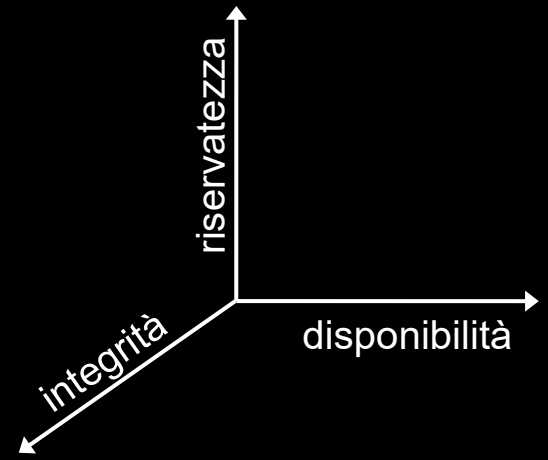
Riservatezza: Ristretto*

Integrità: Importante

Disponibilità: Classe 4

* se **non** contiene dati personali

Classificazione dei Dati



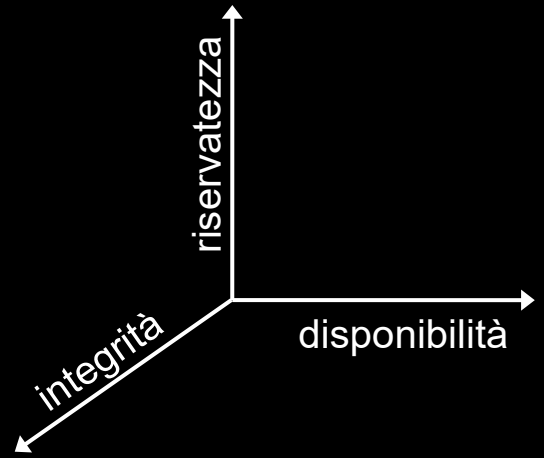
Riservatezza: Confidenziale*

Integrità: Importante

Disponibilità: Classe 4

* se contiene dati personali

Classificazione dei Dati



Riservatezza: Segreto

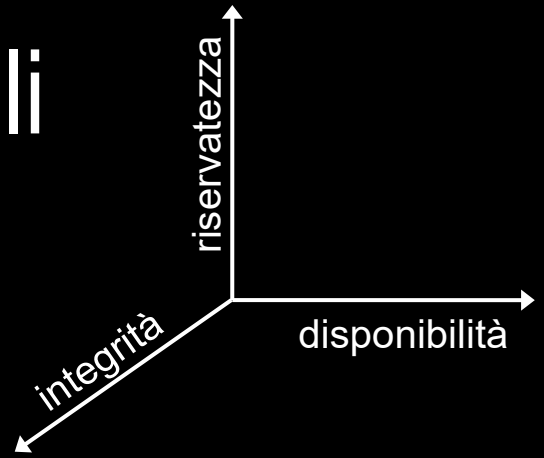
Integrità: Vitale

Disponibilità: Classe 7

Classificazione dei Canali

Canale: mezzo che può trasmettere un dato

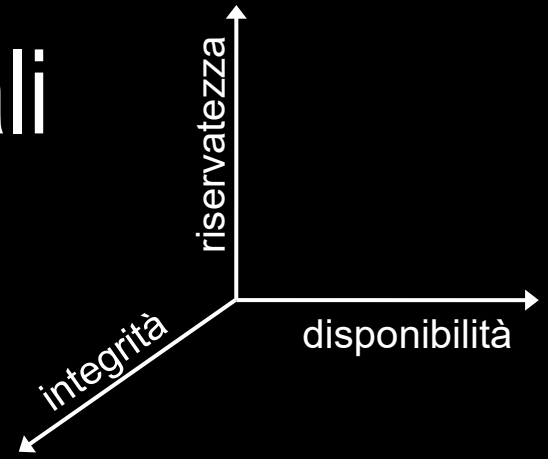
che riservatezza / integrità / disponibilità **garantisce**?



- Chiavetta USB
- Portatile
- RAM
- Cavo Ethernet
- Fibra Ottica
- Fotoni (Wi-Fi, 5G)
- Stampante
- Cestino
- Browser Web
- Smartphone
- Sistema Operativo
- Storage nel “cloud”
- CPU
- Fotocamera
- qualsiasi software connesso ad Internet

Qualsiasi mezzo, fisico o informatico, che può ricevere un dato, **può** anche trasmetterlo.

Classificazione dei Canali

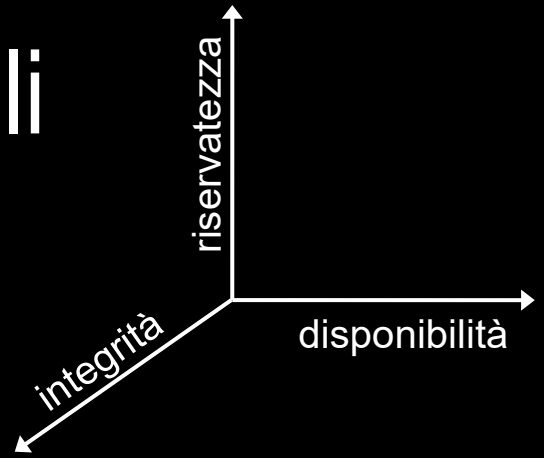


Riservatezza: Pubblico

Integrità: Normale

Disponibilità: Classe 1

Classificazione dei Canali



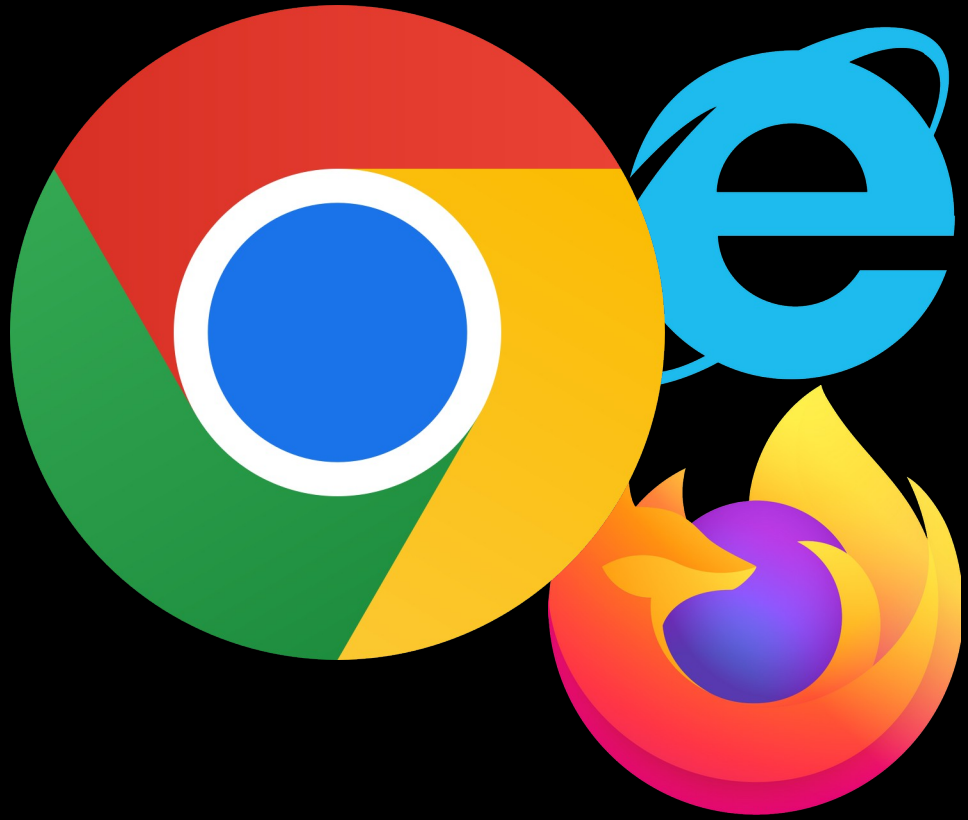
Riservatezza: Segreto*

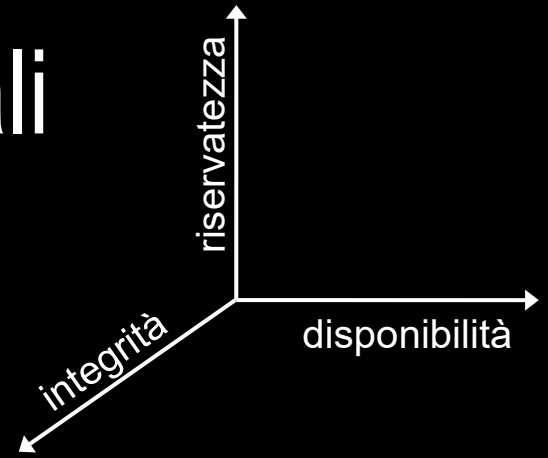
Integrità: Vitale

Disponibilità: Classe 7

* fin quando rimane sotto il controllo fisico dell'organizzazione

Classificazione dei Canali



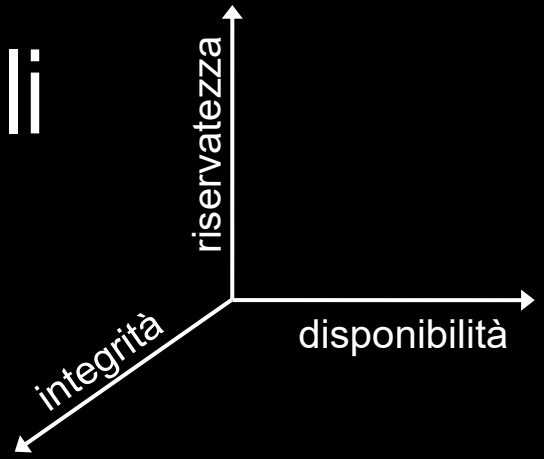


Riservatezza: Pubblico

Integrità: Normale

Disponibilità: Classe 2

Classificazione dei Canali

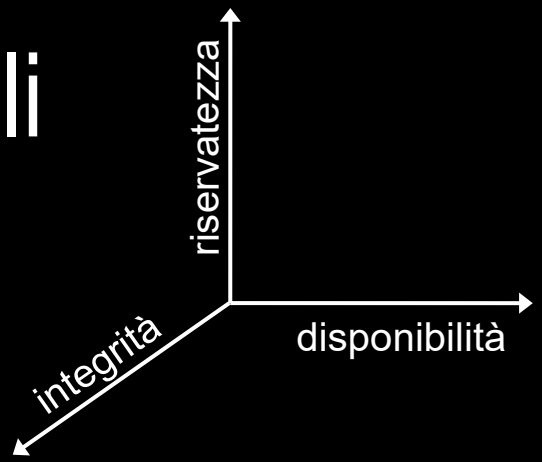


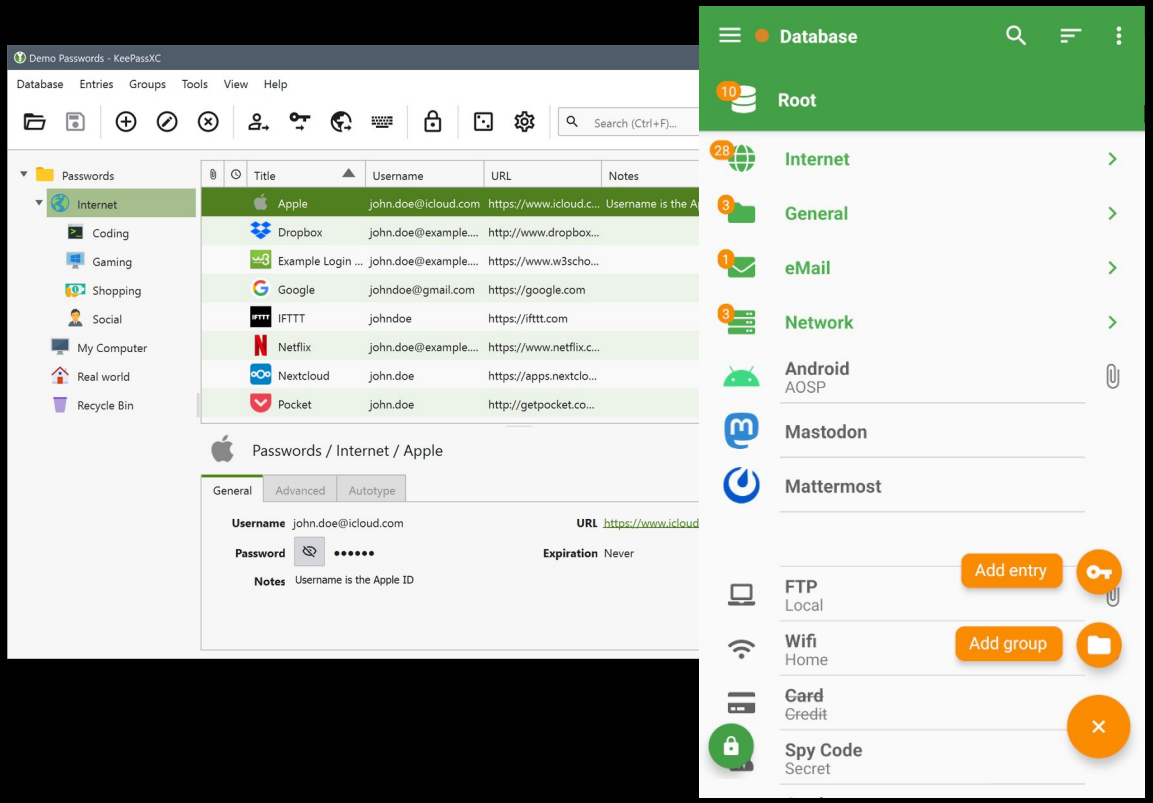
Riservatezza: Segreto

Integrità: Vitale

Disponibilità: Classe 4

Classificazione dei Canali





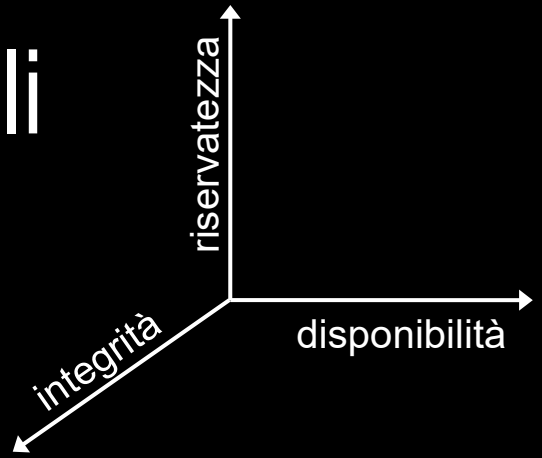
Riservatezza: Segreto*

Integrità: Vitale

Disponibilità: Classe 7*

* se eseguito su hardware che offre garanzie equivalenti o superiori

Classificazione dei Canali

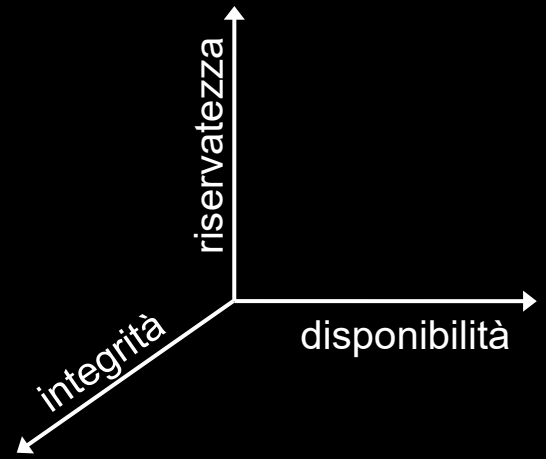


Riservatezza: Pubblico

Integrità: Normale

Disponibilità: Classe 0

Sicurezza Informatica



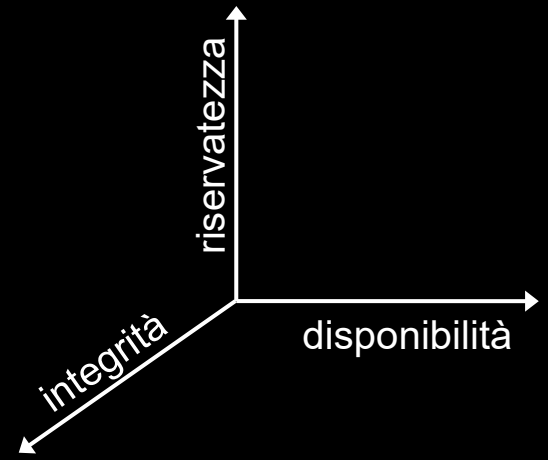
1. Classificare Dati e Canali
   - ✔ riservatezza
   - ✔ integrità
   - ✔ confidenzialità

   } esigenze da garantire

2. Proteggere i Dati

3. Minimizzare i Rischi

Protezione dei Dati



Ogni dato necessita di determinate garanzie di

- riservatezza
- integrità
- disponibilità

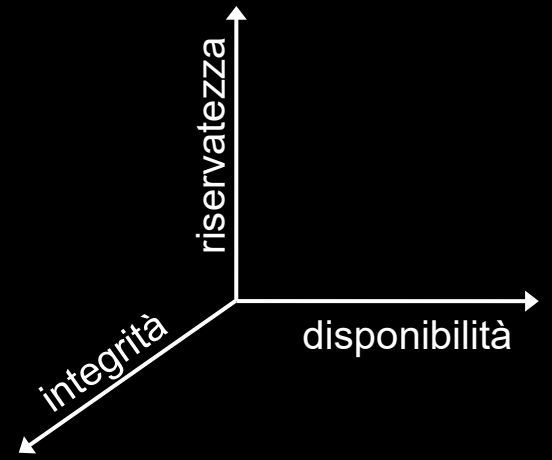
} esigenze

Ogni canale garantisce determinati livelli di

- riservatezza
- integrità
- disponibilità

} disponibilità

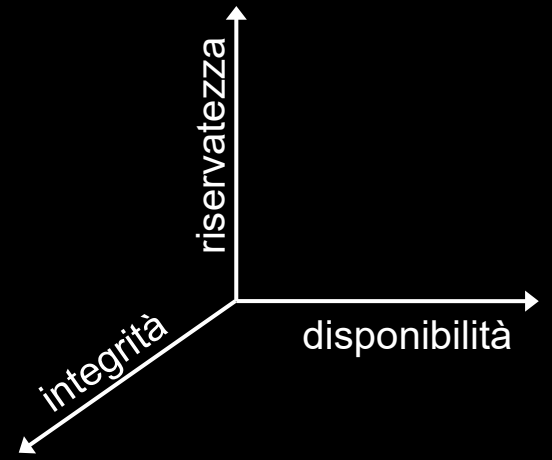
Protezione dei Dati



1. Garantire che ogni dato sia trasmesso esclusivamente su canali che offrono garanzie pari o superiori alle esigenze

2. Garantire la pulizia del canale al termine del suo utilizzo
   - incenerire documenti confidenziali obsoleti
   - sovrascrivere dischi fissi prima di dismetterli
   - svuotare la cache del browser alla chiusura

Protezione dei Dati

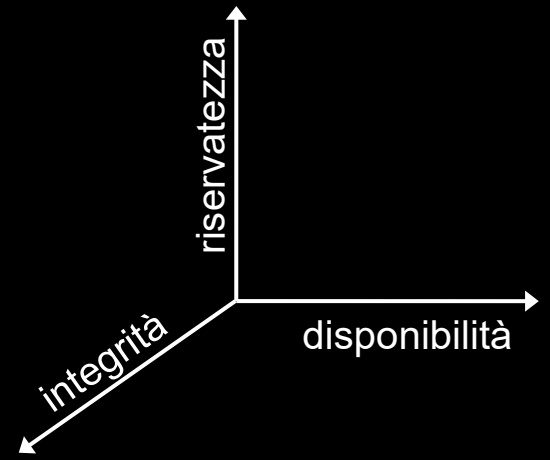


1. Garantire che ogni dato sia trasmesso esclusivamente su canali che offrono garanzie pari o superiori alle esigenze

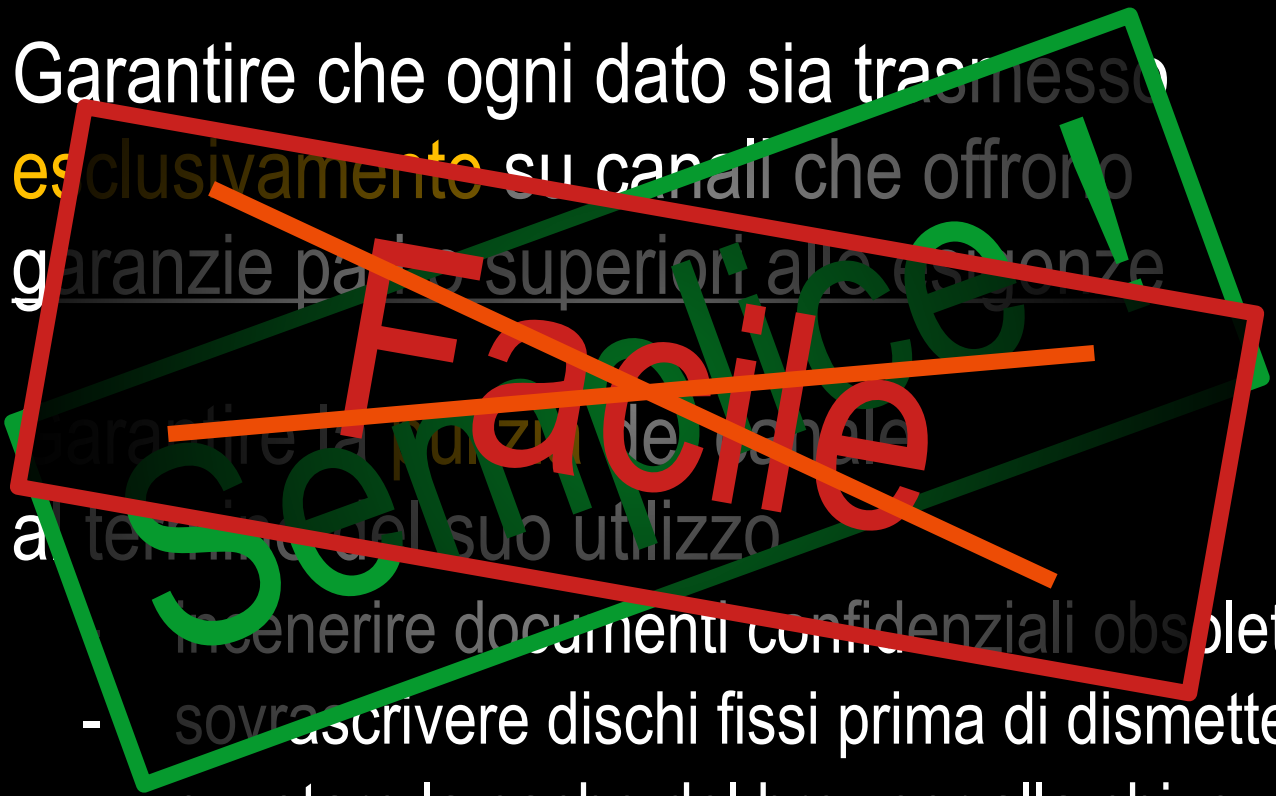
2. Garantire la pulizia del canale al termine del suo utilizzo
   - incenerire documenti confidenziali obsoleti
   - sovrascrivere dischi fissi prima di dismetterli
   - svuotare la cache del browser alla chiusura

Semplice!

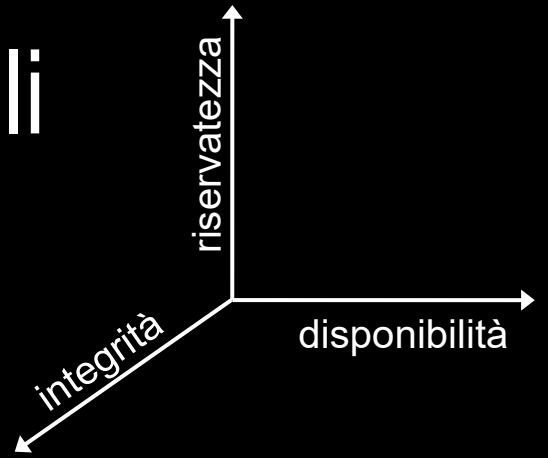
Protezione dei Dati



1. Garantire che ogni dato sia trasmesso esclusivamente su canali che offrono garanzie pari o superiori alle esigenze
2. Garantire la distruzione sicura a termine del suo utilizzo
   - incenerire documenti confidenziali obsoleti
   - sovrascrivere dischi fissi prima di dismetterli
   - svuotare la cache del browser alla chiusura



Classificazione dei Canali

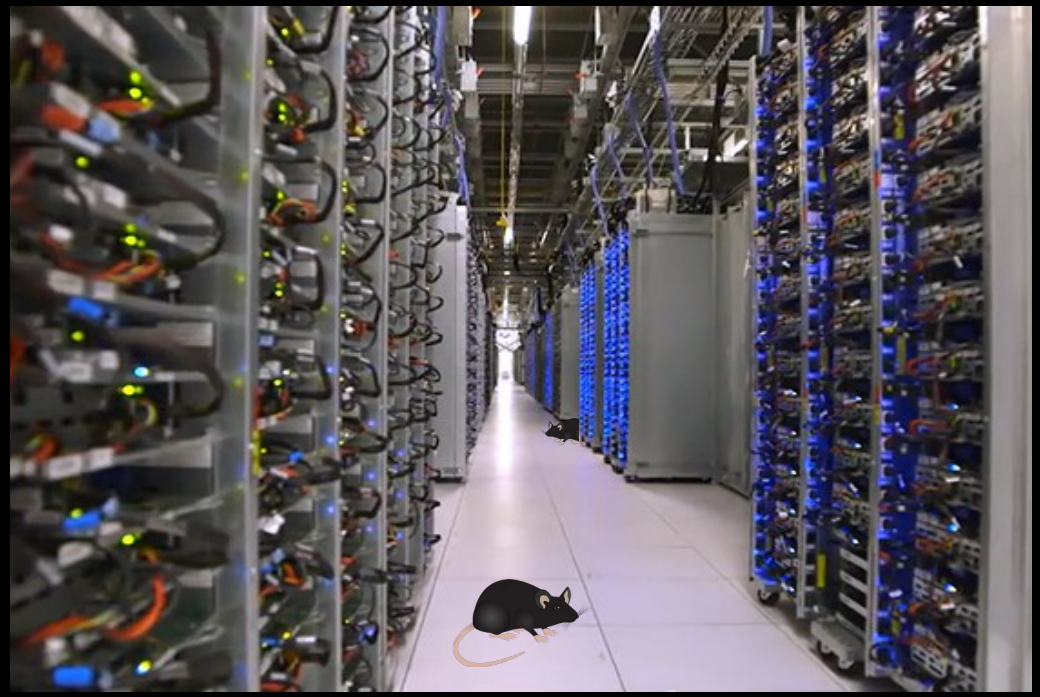


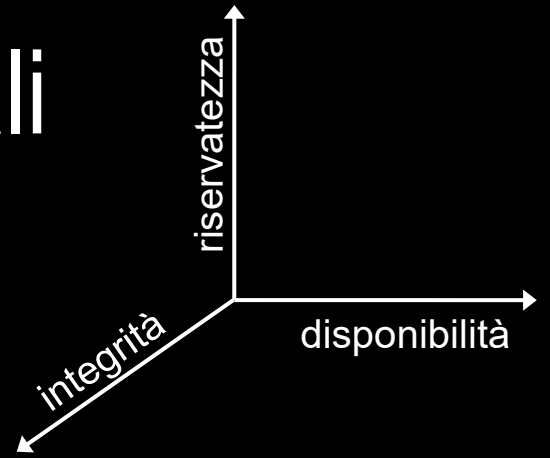
Riservatezza: Confidenziale

Integrità: Importante

Disponibilità: Classe 4+

Classificazione dei Canali





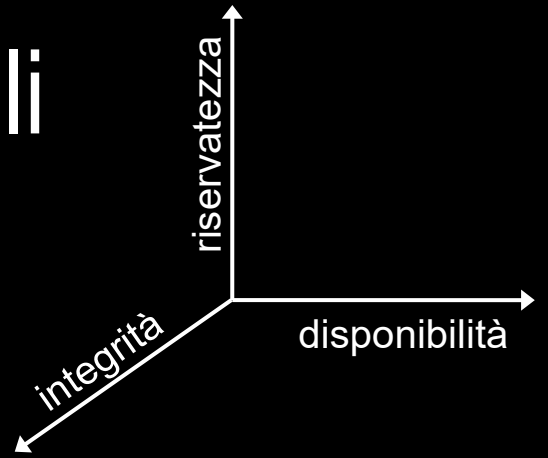
Riservatezza: Confidenziale

Integrità: Importante

Disponibilità: Classe 4+

?

Classificazione dei Canali

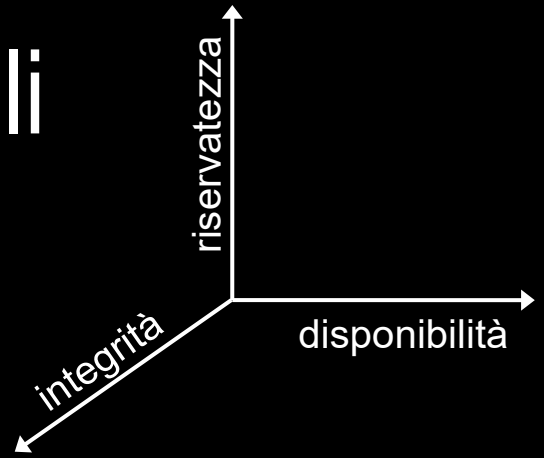


Riservatezza: Confidenziale

Integrità: Importante

Disponibilità: Classe 4+

Classificazione dei Canali



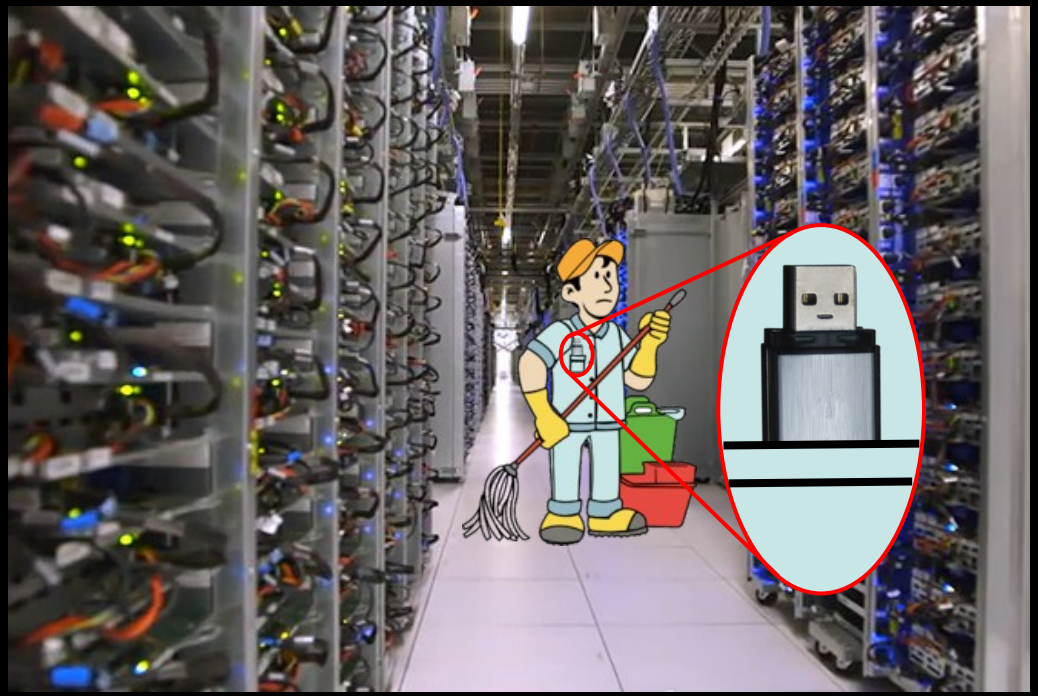
Riservatezza: Confidenziale

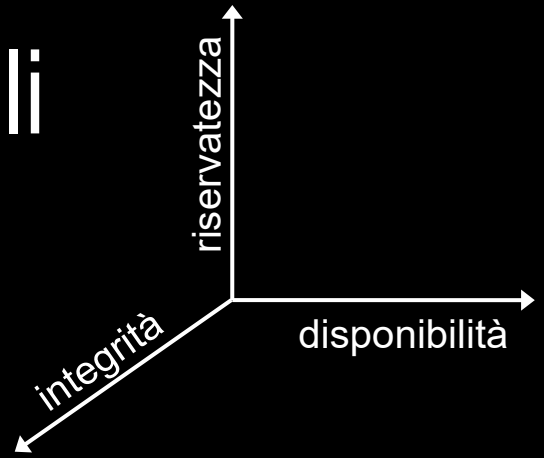
Integrità: Importante

Disponibilità: Classe 4+

?

Classificazione dei Canali





Riservatezza: Pubblica

Integrità: Normale

Disponibilità: Classe 0

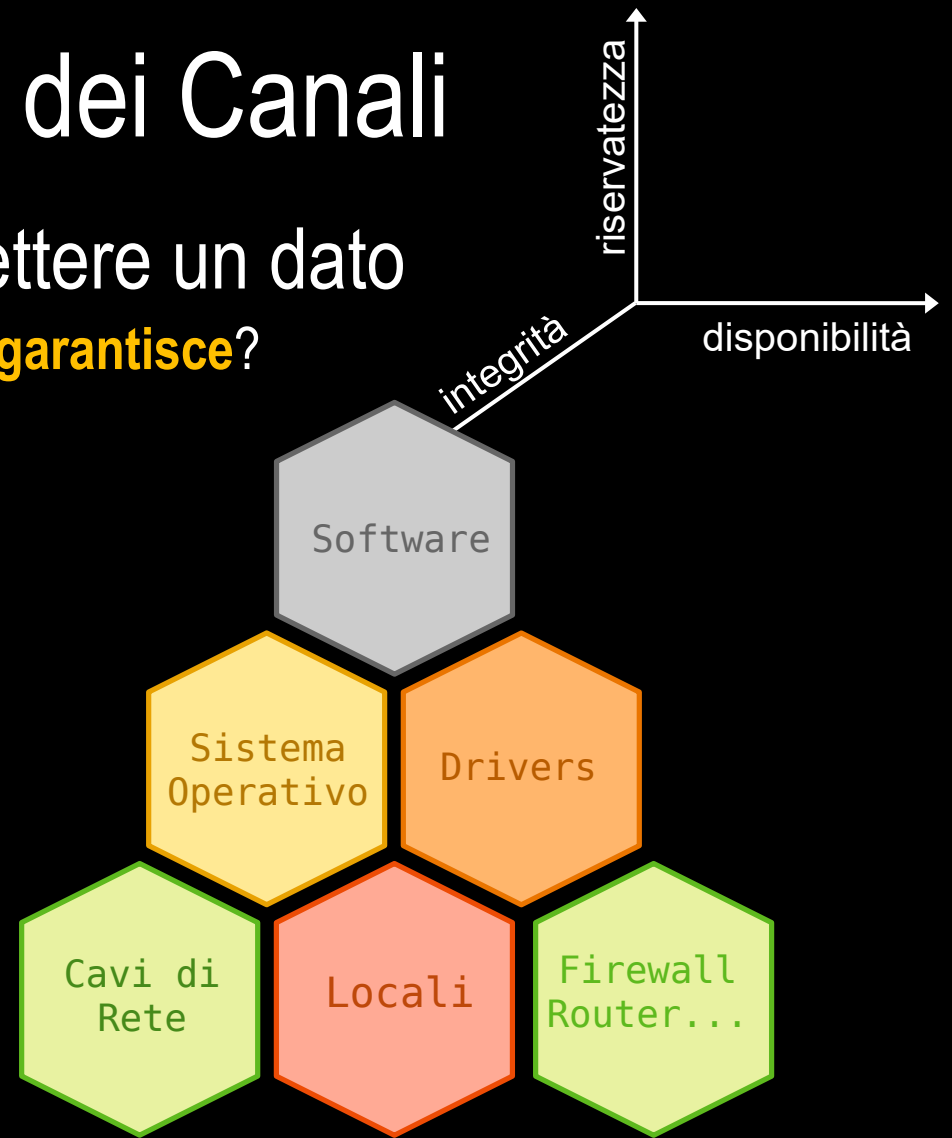
!

Classificazione dei Canali

Canale: mezzo che può trasmettere un dato

che riservatezza / integrità / disponibilità **garantisce**?

La stragrande maggioranza dei canali di comunicazione è costruita componendo altri canali di comunicazione



Protezione dei Dati

Canale: mezzo che può trasmettere un dato

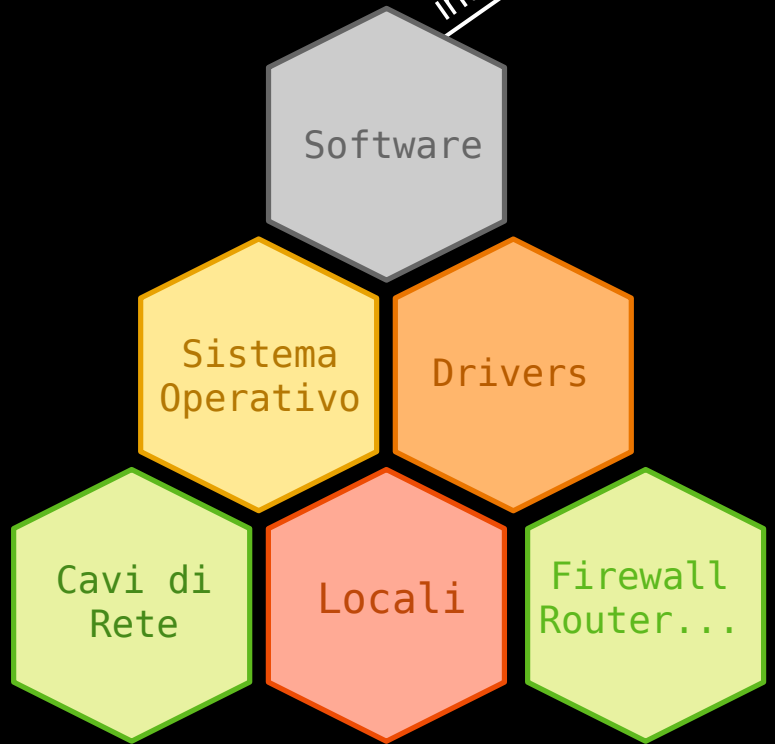
che riservatezza / integrità / disponibilità **garantisce**?

riservatezza

integrità

disponibilità

ogni catena è forte quanto
il suo anello più debole



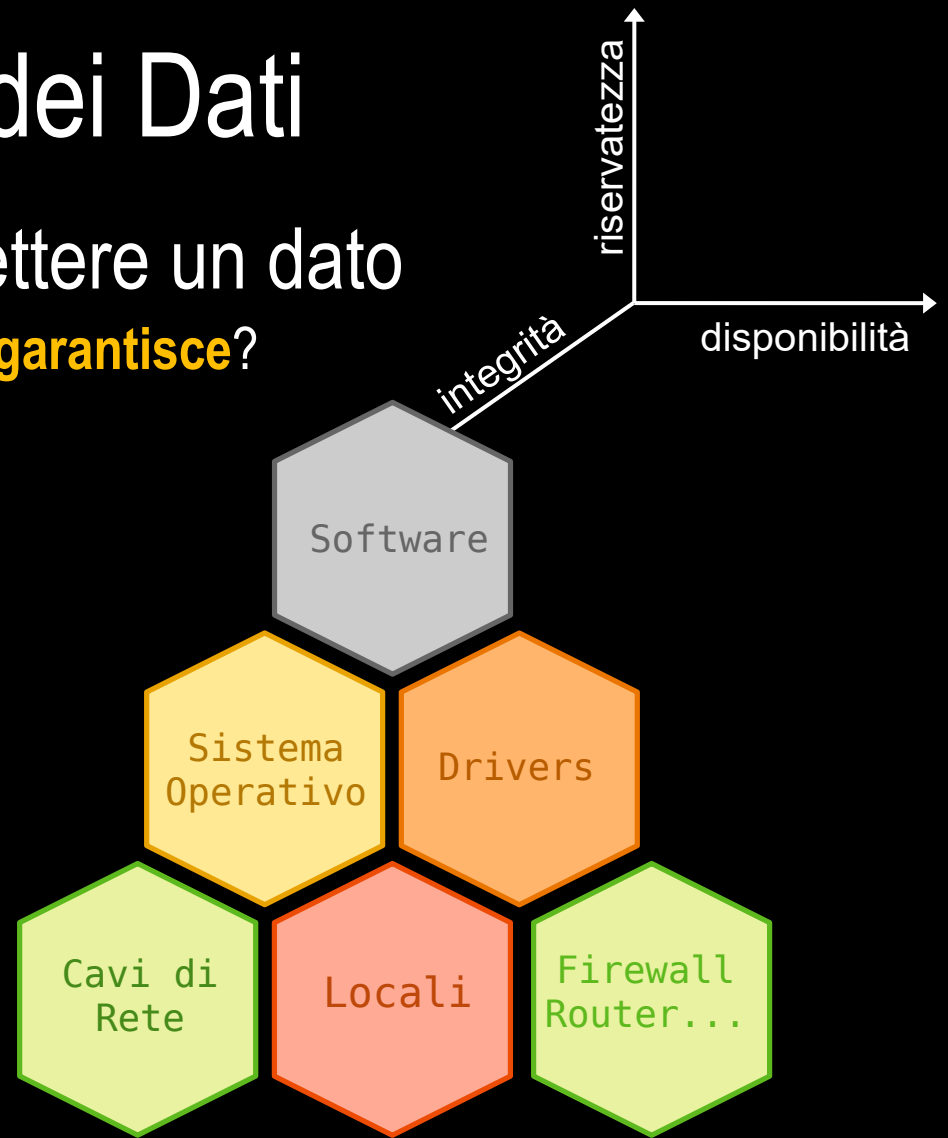
Protezione dei Dati

Canale: mezzo che può trasmettere un dato

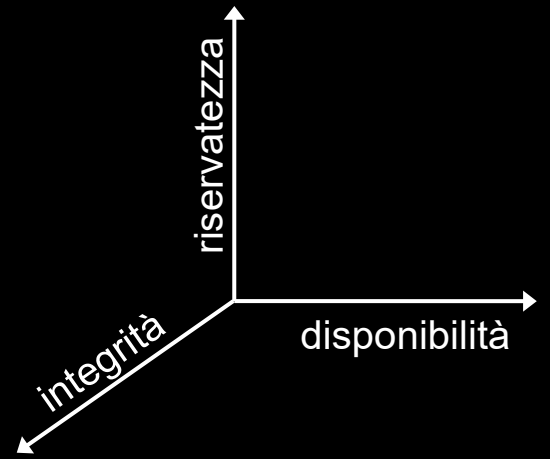
che riservatezza / integrità / disponibilità **garantisce**?

ogni catena è forte quanto
il suo anello più debole

un canale composito garantisce
riservatezza / integrità / disponibilità
pari al minimo di quelle garantite
da ciascuno dei suoi componenti



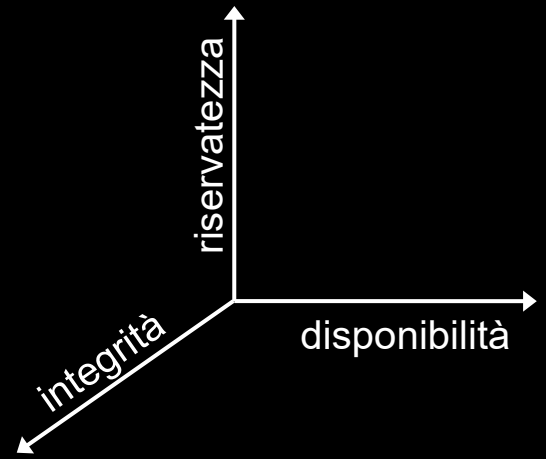
Protezione dei Dati



Problemi aperti:

- misurare le garanzie offerte da ogni canale
- mantenere tali garanzie effettive nel lungo periodo
- minimizzare l'errore umano
- identificare manomissioni

Sicurezza Informatica



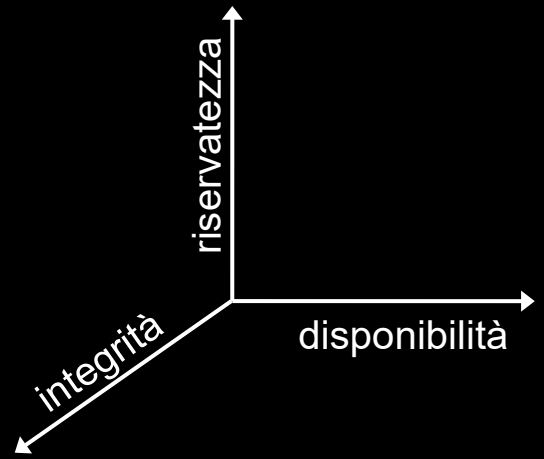
1. Classificare Dati e Canali
   - ✔ riservatezza
   - ✔ integrità
   - ✔ confidenzialità

   } esigenze da garantire

2. Proteggere i Dati

3. Minimizzare i Rischi

Minimizzare i Rischi

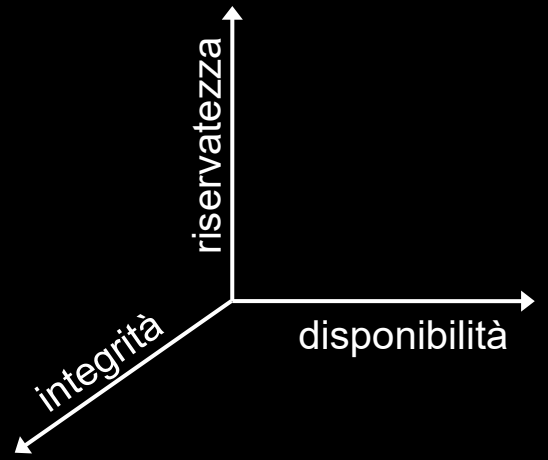


Misurare le garanzie offerte dal canale

- le garanzie dichiarate **non** impediscono incidenti
  - risarcimenti ridicoli per danni irreversibili
- le garanzie di un canale devono essere verificabili
  - dopo ogni incidente deve essere possibile e rapido identificare quali garanzie sono venute meno e perché

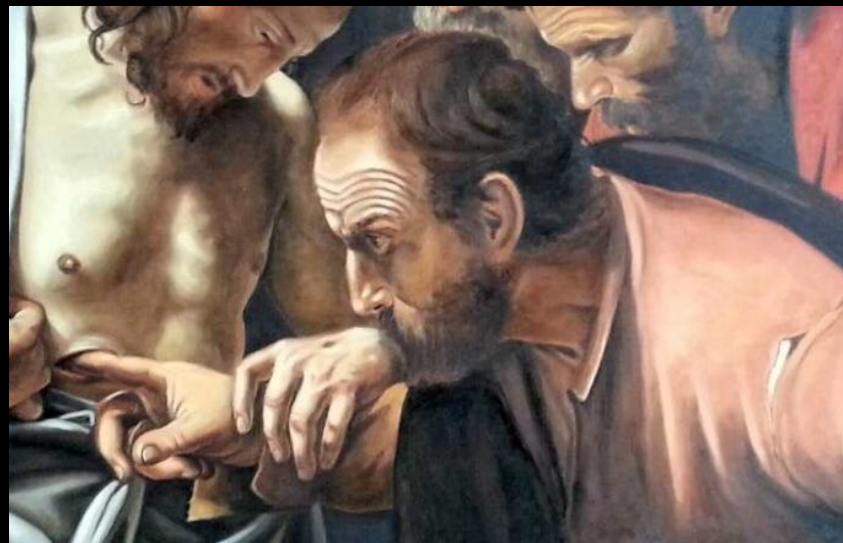
TRASPARENZA

Minimizzare i Rischi

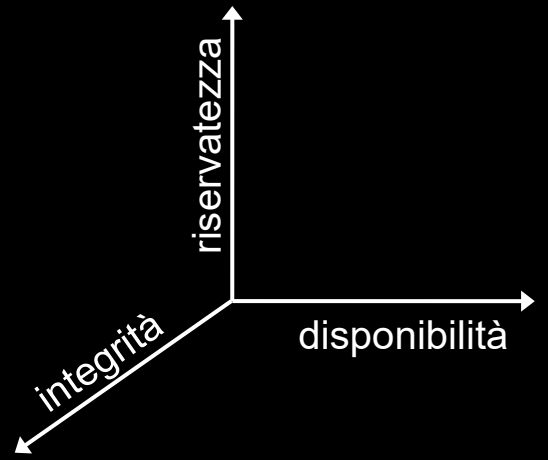


Non esiste sicurezza senza trasparenza

- la trasparenza promessa (anche contrattualmente) è una favola della buona notte per i manager
- se non potete ispezionare concretamente e completamente un canale, allora **non** è trasparente



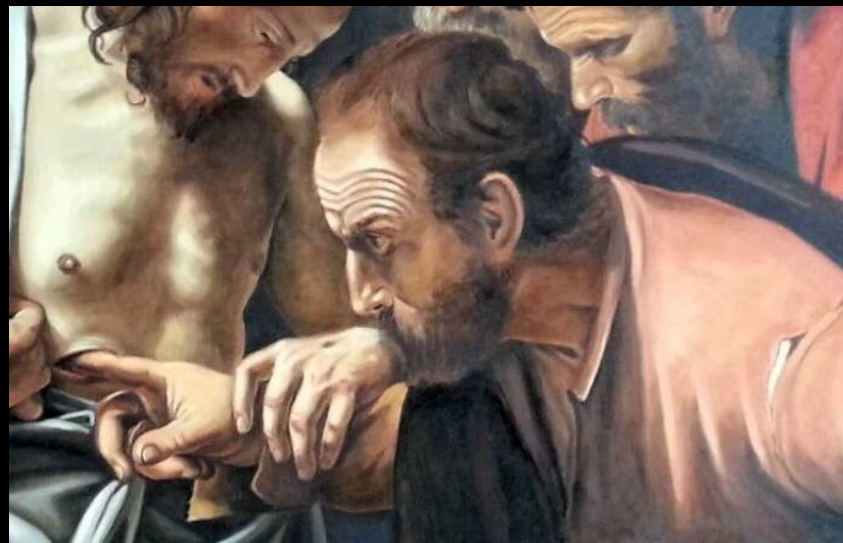
Minimizzare i Rischi



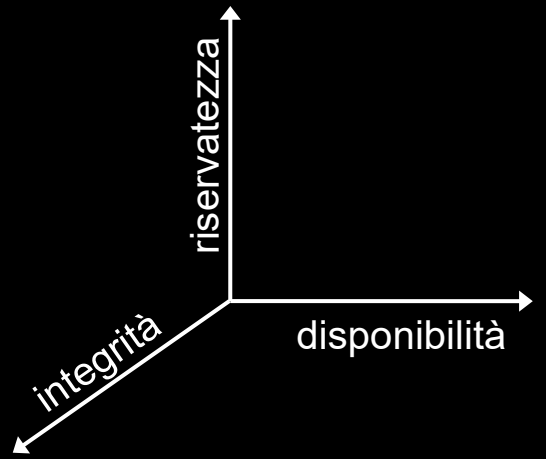
Non esiste sicurezza senza trasparenza

- la trasparenza promessa (anche contrattualmente) è una favola della buona notte per i manager
- se non potete ispezionare concretamente e completamente un canale, allora **non** è trasparente

Riservate la **fiducia** per i membri dell'organizzazione



Minimizzare i Rischi

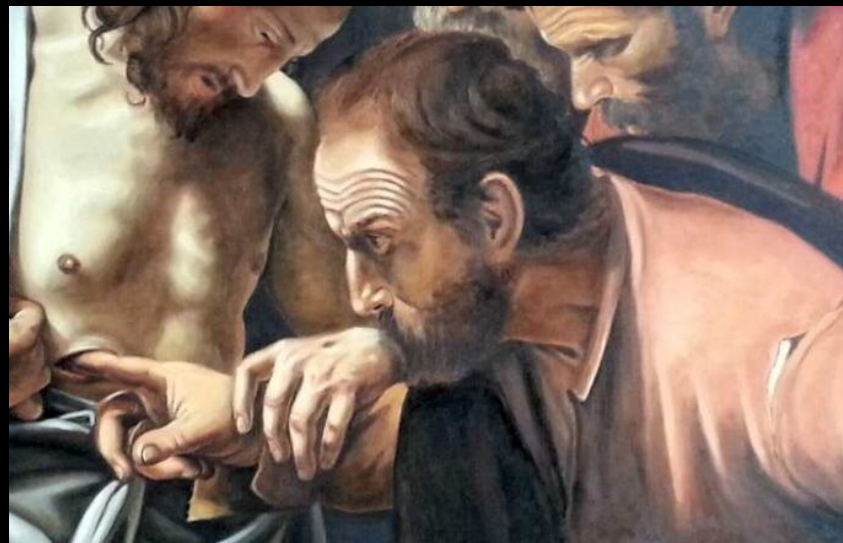


Non può essere trasparente

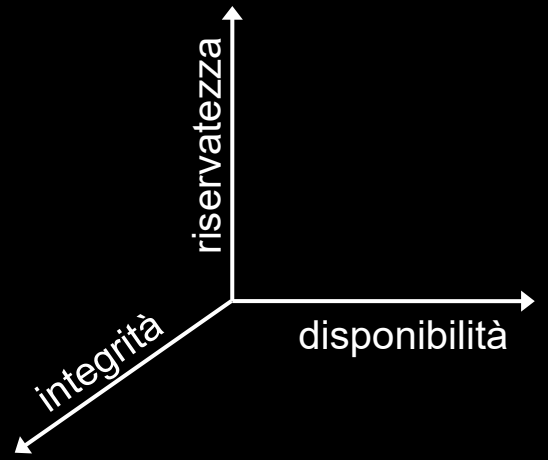
- software proprietario
- software opensource troppo complesso
- hardware non riparabile

  right to repair
- servizi “cloud” di terze parti*

* da non confondere con le tecnologie di virtualizzazione “*cloud on premise*”



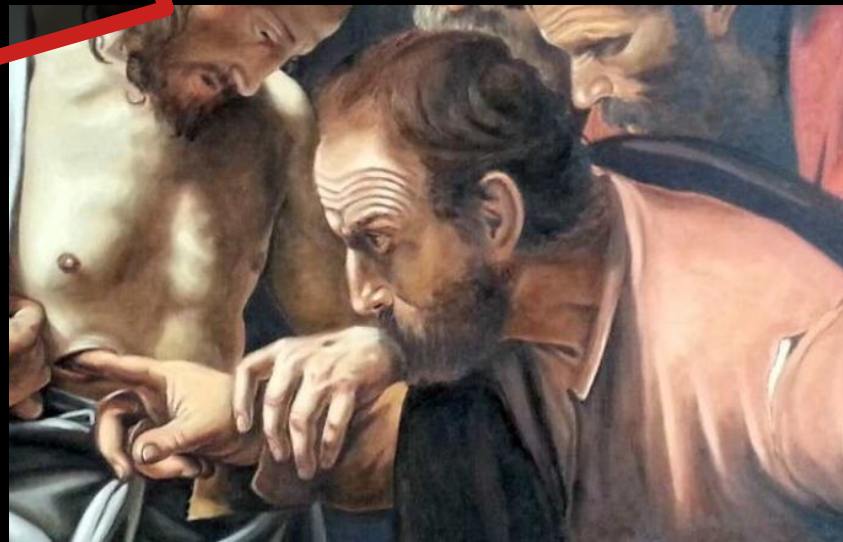
Minimizzare i Rischi



Non può essere trasparente

- software proprietario
- software opensource troppo complesso
- hardware non riparabile
  right to repair
- servizi "cloud" di terze parti*

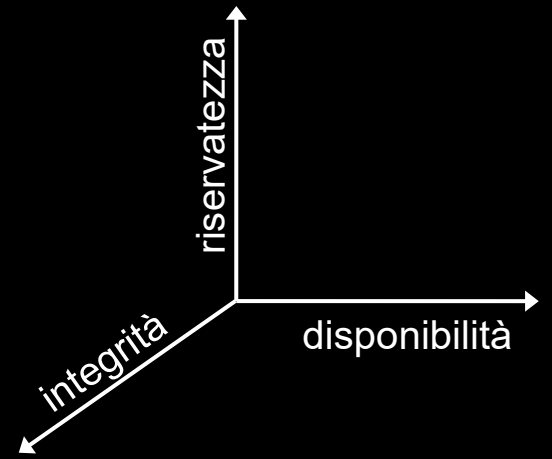
INSICURO



* da non confondere con le tecnologie di virtualizzazione "*cloud on premise*"

Minimizzare i Rischi

E se non c'è un canale adatto?



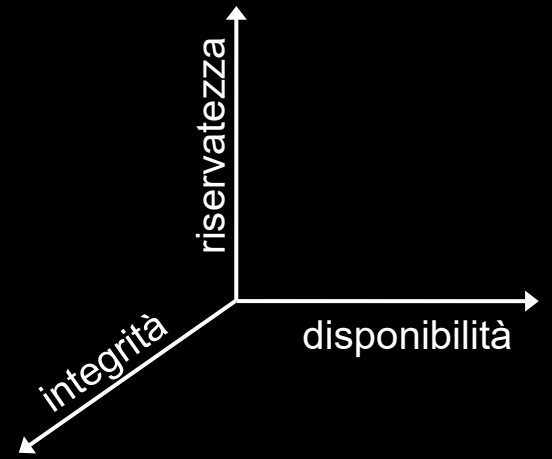
Talvolta tutti i canali disponibili forniscono garanzie insufficienti rispetto ad una o più delle esigenze necessarie alla comunicazione.

Soluzioni:

- **non** trasmettere il dato
  - informaticamente sicura... ma ciberneticamente?
- trasmetterlo ad un destinatario che possa garantire le esigenze mancanti
  - soluzione inadatta se il canale non fornisce riservatezza sufficiente
- creare un canale cifrato

Minimizzare i Rischi

E se non c'è un canale adatto?

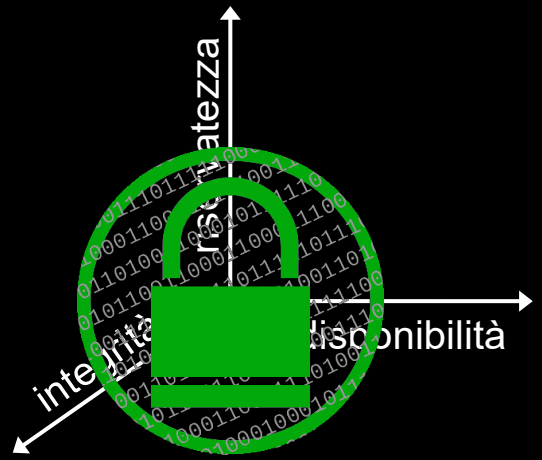


Talvolta tutti i canali disponibili forniscono garanzie insufficienti rispetto ad una o più delle esigenze necessarie alla comunicazione.

Soluzioni:

- **non** trasmettere il dato
  - informaticamente sicura... ma ciberneticamente?
- trasmetterlo ad un destinatario che possa garantire le esigenze mancanti
  - soluzione inadatta se il canale non fornisce riservatezza sufficiente
- creare un canale cifrato

Minimizzare i Rischi

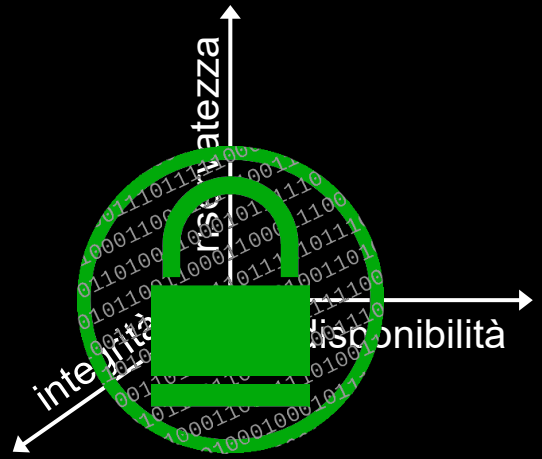


Crittografia – *kryptós graphein*

- insieme di algoritmi e protocolli
  - tipicamente codificati in software
- può fornire garanzie superiori a quelle di alcuni canali attraversati
  - **se** implementata correttamente
  - **se** applicata correttamente da **tutti** gli interlocutori
    - protezione chiavi, autenticazione etc...
- non può fornire garanzie superiori a quelle fornite dagli interlocutori
  - ...e dal loro hardware, software etc...

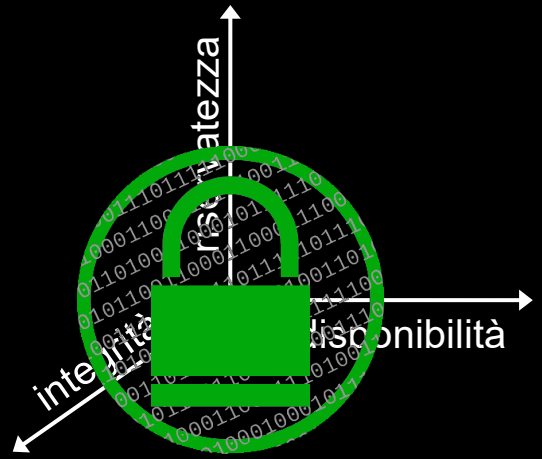
Minimizzare i Rischi

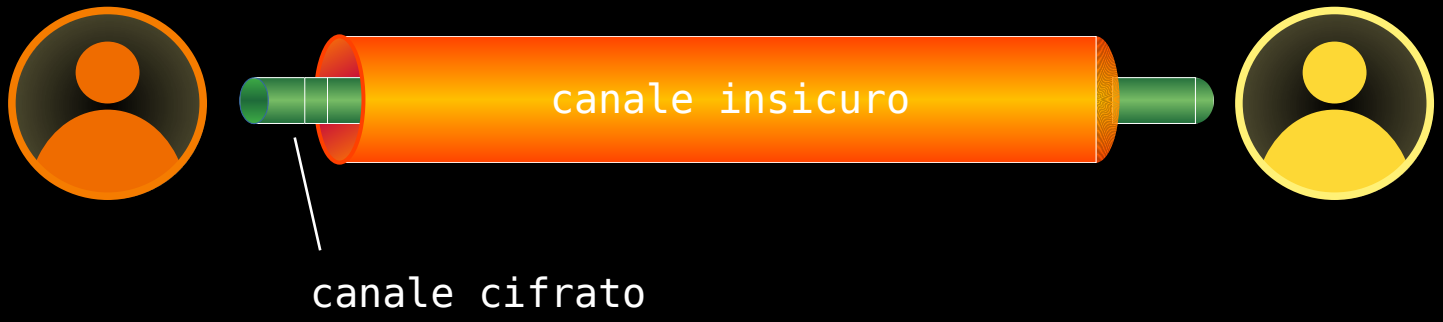
Crittografia – *kryptós graphein*



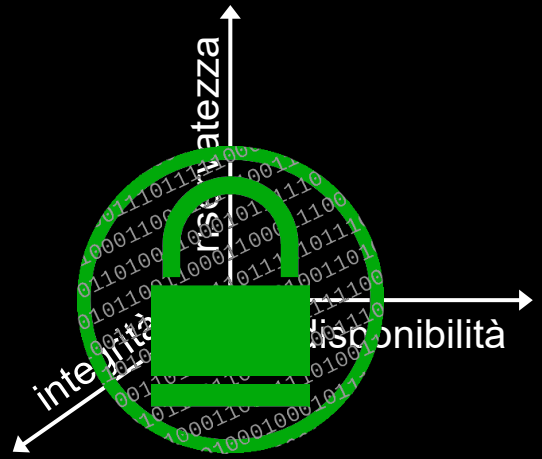
Minimizzare i Rischi

Crittografia – *kryptós graphein*





Minimizzare i Rischi



Canale cifrato

- connette due interlocutori (*peers*)
- non può proteggere alcuni metadati
  - mittente, destinatario, ora...
- quando sembra connettere più interlocutori
  - uno smista i messaggi

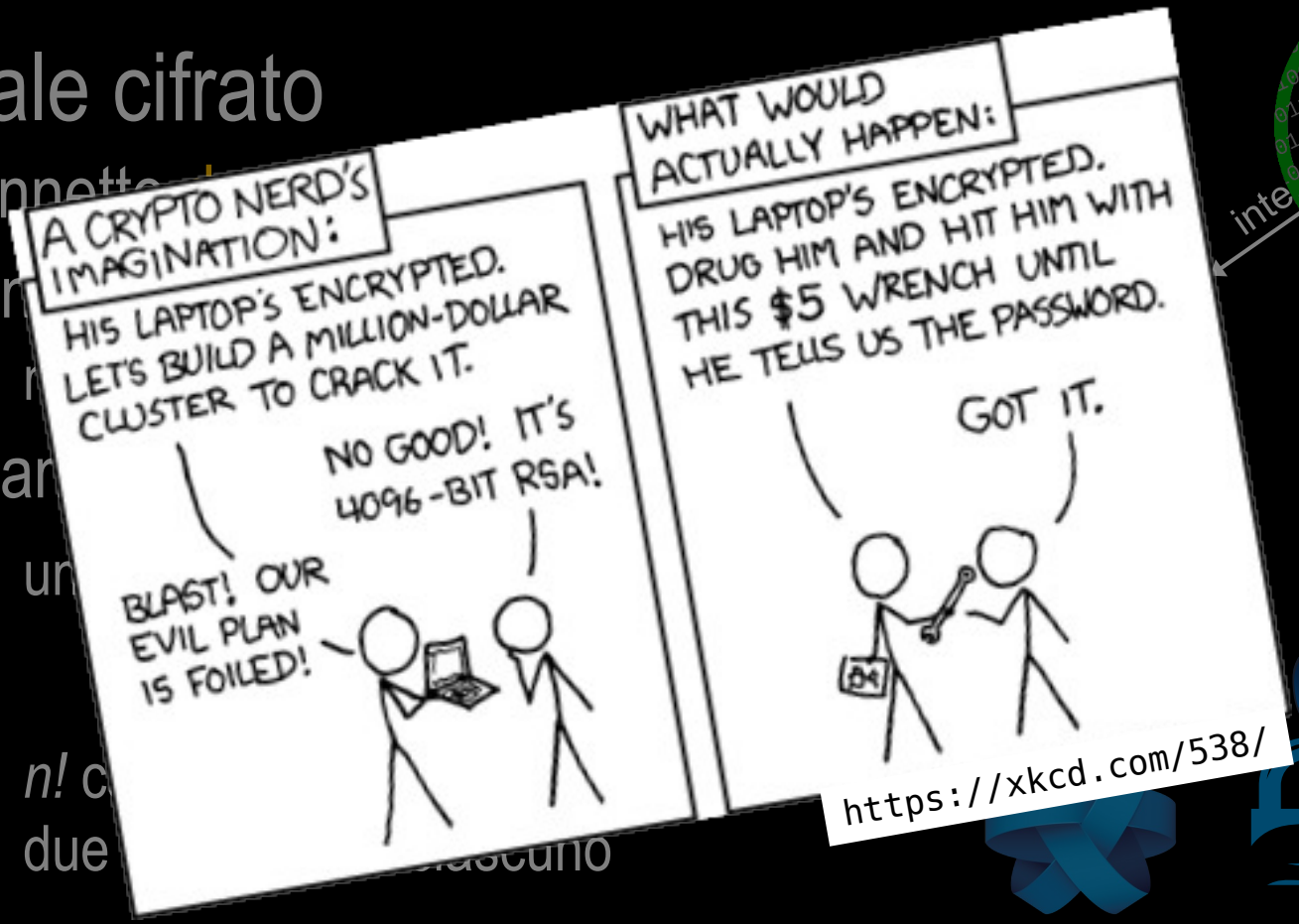
    può leggere (e talvolta alterare) i messaggi di tutti
  - *n!* canali cifrati diversi connettono due interlocutori ciascuno

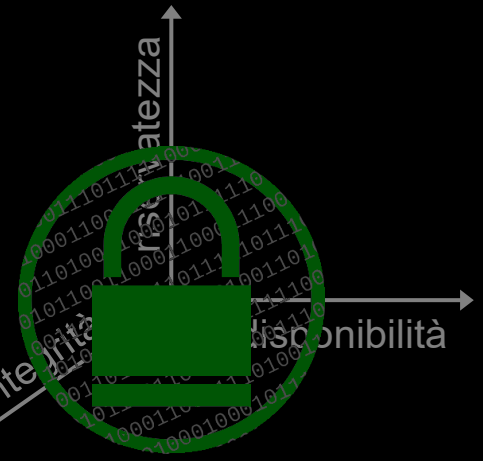
GnuPG

Minimizzare i Rischi

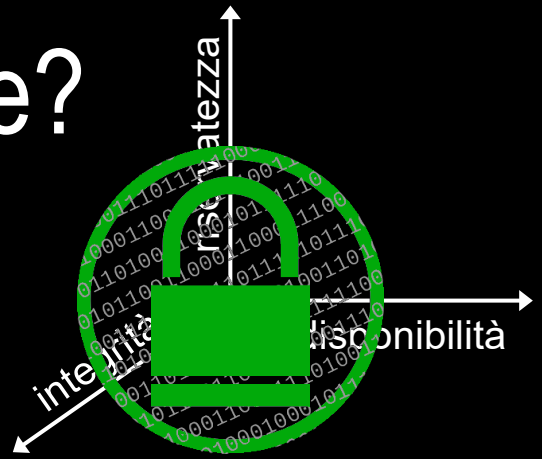
Canale cifrato

- connett
- nor
  - r
- quar
  - ur
  - *n!* c
    due





Sicurezza Informatica: domande?



1. Classificare Dati e Canali
   - ✔ riservatezza
   - ✔ integrità
   - ✔ confidenzialità

   } esigenze da garantire

2. Proteggere i Dati
3. Minimizzare i Rischi

Sicurezza

"*sine cura*" – senza preoccupazione

Definiamo "sicuro" un sistema progettato in modo tale che la sua evoluzione non può produrre effetti indesiderati.

Sicurezza Cibernetica

"*sine cura*" – senza preoccupazione

Definiamo "sicuro" un sistema cibernetico stabile la cui evoluzione non può procurare danni ai propri membri.

Sicurezza Cibernetica

"*sine cura*" – senza preoccupazione

Definiamo "sicuro" un sistema cibernetico stabile la cui evoluzione non può procurare danni ai propri membri.

Resiliente

continua a svolgere le
funzioni per cui è progettato
anche a fronte di imprevisti

Sicurezza Cibernetica

"*sine cura*" – senza preoccupazione

Definiamo "sicuro" un sistema cibernetico stabile la cui evoluzione non può procurare danni ai propri membri.

Resiliente

continua a svolgere le funzioni per cui è progettato anche a fronte di imprevisti

Protetto

non **può** danneggiare persone ed automatismi coinvolti

Sicurezza Cibernetica

"*sine cura*" – senza preoccupazione

Definiamo "sicuro" un sistema cibernetico stabile la cui evoluzione non può procurare danni ai propri membri.

Prevedibile

l'evoluzione del sistema può essere prevista e pianificata in modo da evitare i pericoli

Trasparente

lo stato del sistema è sempre e completamente ispezionabile, comprensibile e verificabile

Sicurezza Cibernetica

Insieme di procedure atte a garantire la stabilità operativa di un’organizzazione cibernetica

Sicurezza Cibernetica

Insieme di procedure atte a garantire la stabilità operativa di un'organizzazione cibernetica

- protezione fisica di spazi e hardware
- monitoraggio degli automatismi
- protezione e formazione delle persone
- protezione dei canali di comunicazione
- …

Sicurezza Cibernetica

Insieme di procedure atte a garantire la stabilità operativa di un'organizzazione cibernetica

- protezione fisica di spazi e hardware
- monitoraggio degli automatismi
- protezione e formazione delle persone
- protezione dei canali di comunicazione
- …

LUNGO PERIODO

Sicurezza Cibernetica

Perimetro di Sicurezza

confine ideale che separa i membri di un'organizzazione e gli automatismi sotto il loro pieno controllo dagli agenti autonomi ed automatici che non lo sono.

Sicurezza Cibernetica

Perimetro di Sicurezza

confine ideale che separa i membri di un'organizzazione e gli automatismi sotto il loro pieno controllo dagli agenti autonomi ed automatici che non lo sono.

Superficie di Attacco

insieme dei canali di comunicazione che connettono i membri di un'organizzazione cibernetica (automatismi o autonomie) con agenti esterni all'organizzazione.

Sicurezza Cibernetica

Superficie di Attacco

insieme dei canali di comunicazione che connettono i membri di un'organizzazione cibernetica (automatismi o autonomie) con agenti esterni all'organizzazione.

- email
- browser
- aggiornamenti software
  - smartphone
  - laptop
  - server
- spazzatura
- assistenti vocali
- "internet of things"
- social network e chat
- smartphone
- chiavette USB

} per **ogni** membro!

Sicurezza Cibernetica

Superficie di Attacco

insieme dei canali di comunicazione che connettono i membri di un'organizzazione cibernetica (automatismi o autonomie) con agenti esterni all'organizzazione.

La superficie di attacco cresce rapidamente al crescere di una organizzazione cibernetica: ogni membro può estenderla.

Per proteggerla è necessario:

- compartimentare, differenziare, minimizzare i rischi
- diffondere una piena cittadinanza cibernetica

Sicurezza Cibernetica

Superficie di Attacco

insieme dei canali di comunicazione che connettono i membri di un'organizzazione cibernetica (automatismi o autonomie) con agenti esterni all'organizzazione.

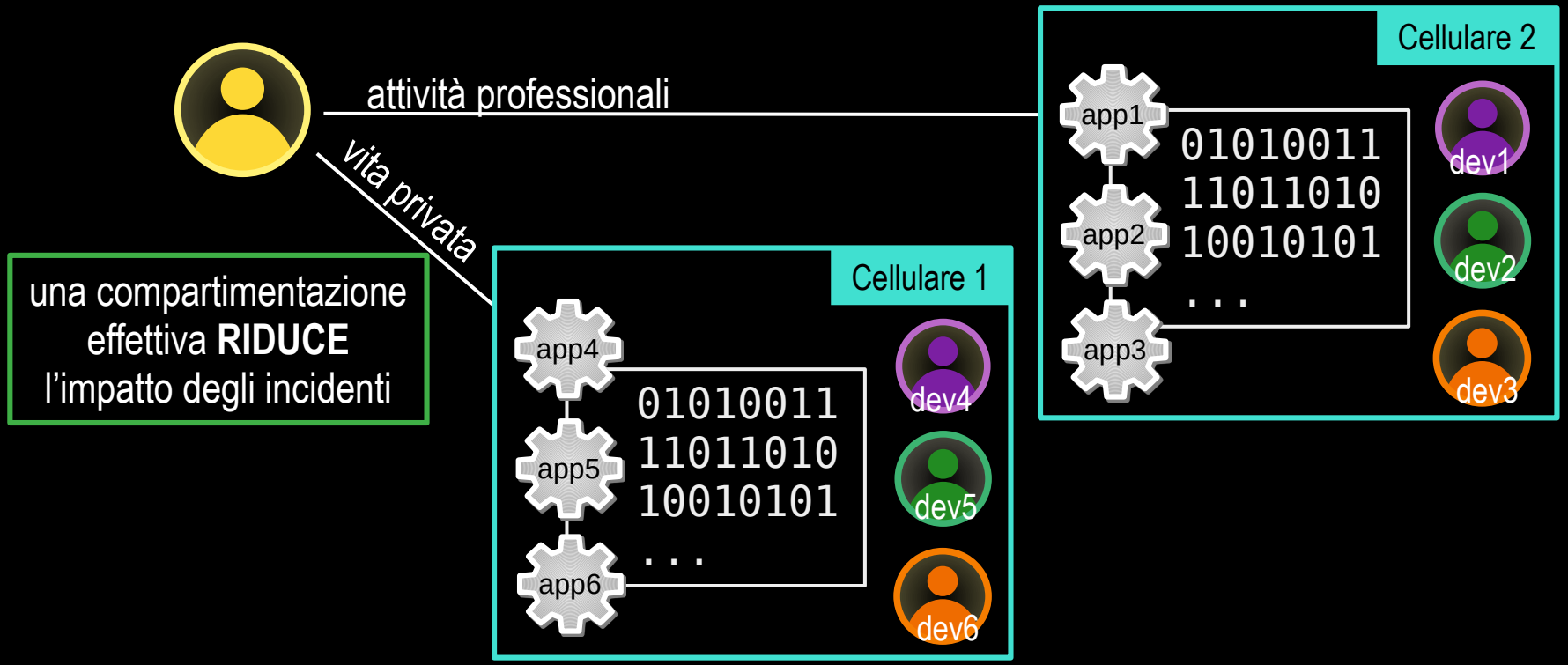
La superficie di attacco cresce rapidamente al crescere di una organizzazione cibernetica: ogni membro può estenderla.

Per proteggerla è necessario:

- compartimentare, differenziare, minimizzare i rischi
- diffondere una piena cittadinanza cibernetica

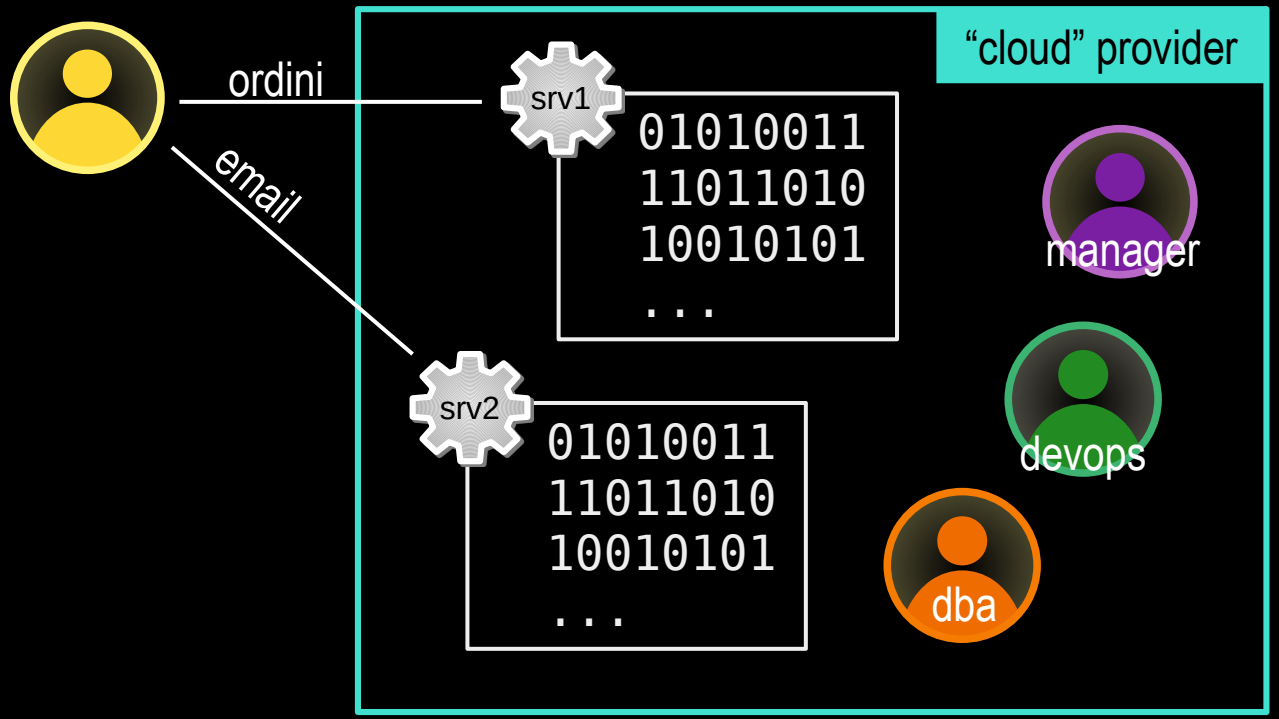
Sicurezza Cibernetica

Compartimentare i Dati



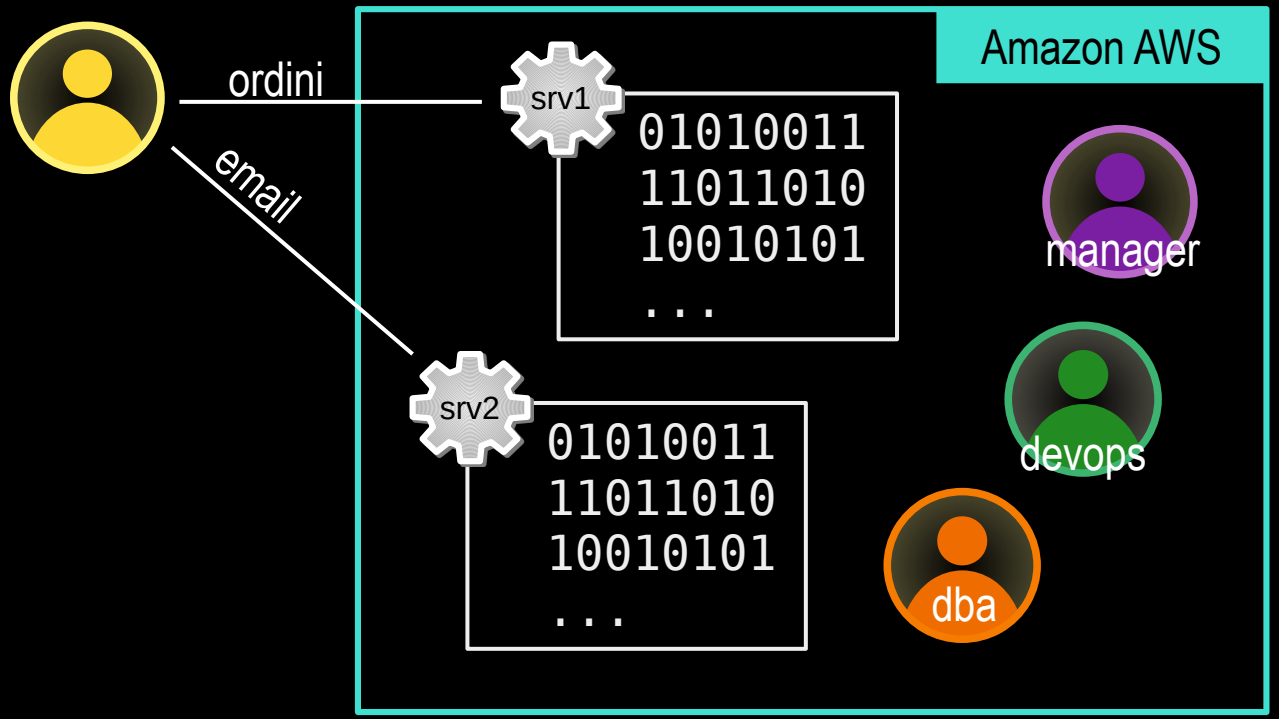
Sicurezza Cibernetica

Compartimentare i Dati



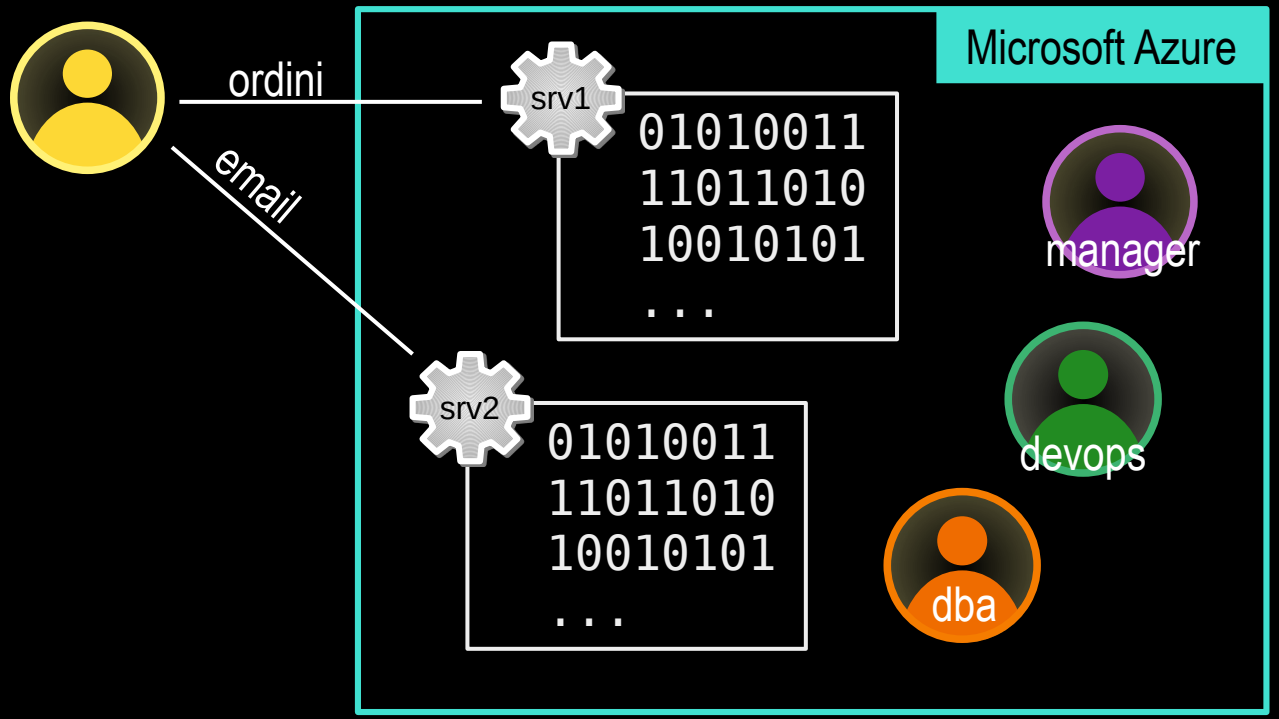
Sicurezza Cibernetica

Compartimentare i Dati



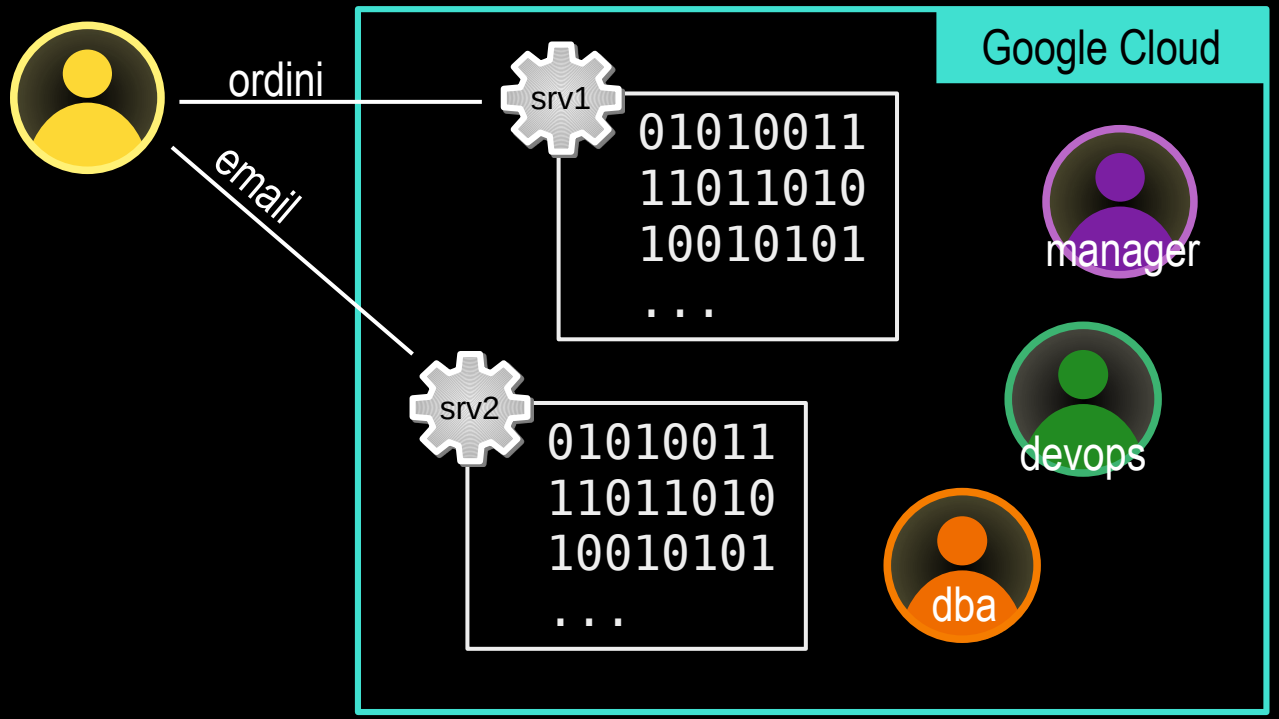
Sicurezza Cibernetica

Compartimentare i Dati



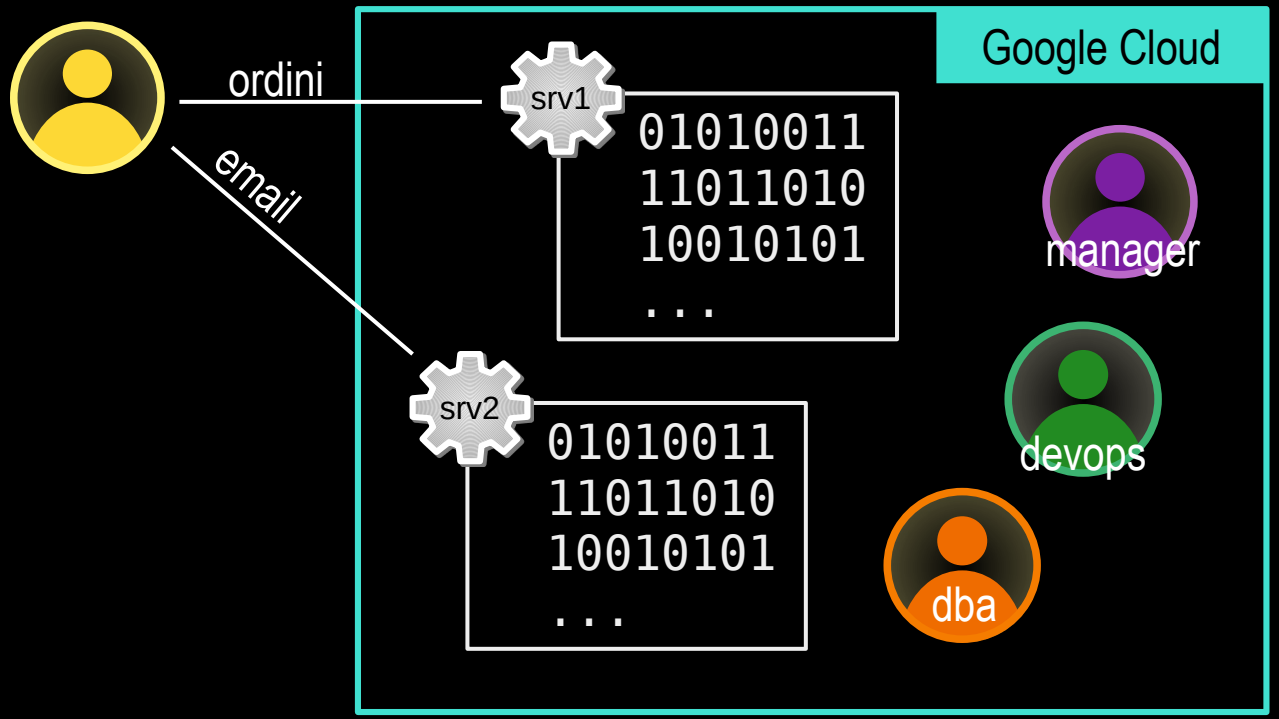
Sicurezza Cibernetica

Compartimentare i Dati



Sicurezza Cibernetica

Compartimentare i Dati



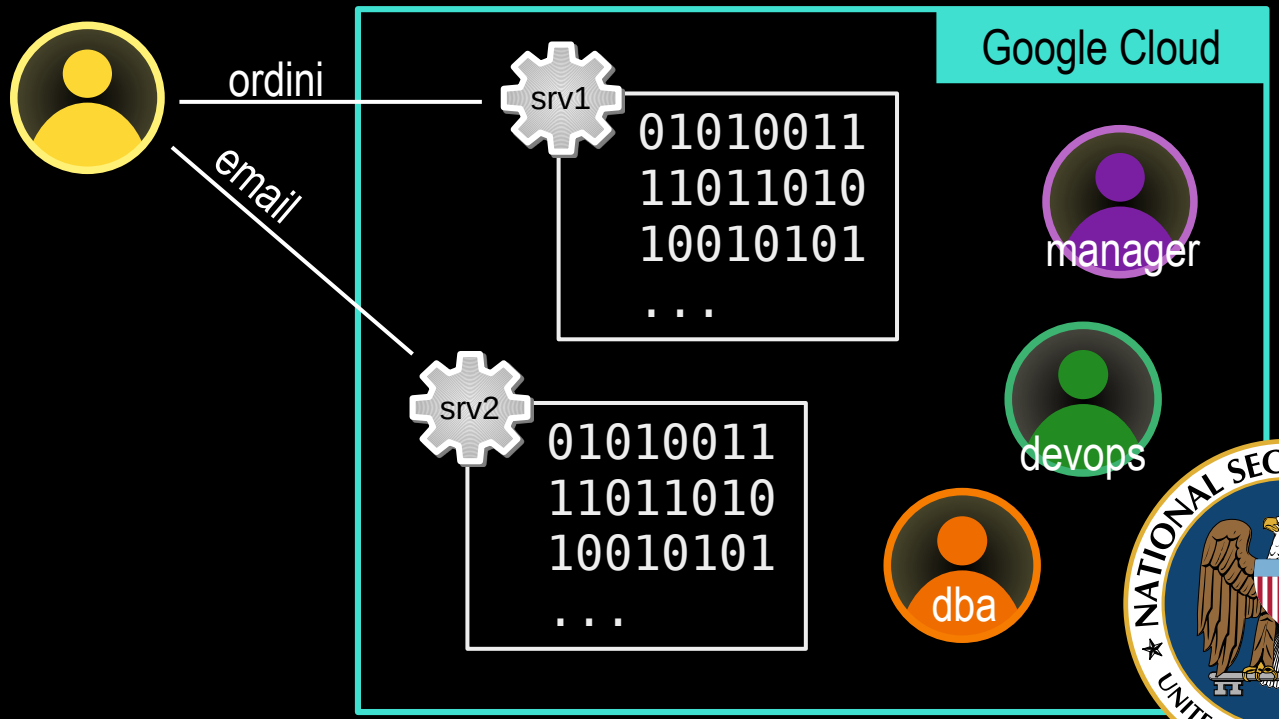
mettere
tutte le uova
in un paniere

produce
lock-in

facilita
- frittate

Sicurezza Cibernetica

Compartimentare i Dati



mettere
tutte le uova
in un paniere

produce
lock-in

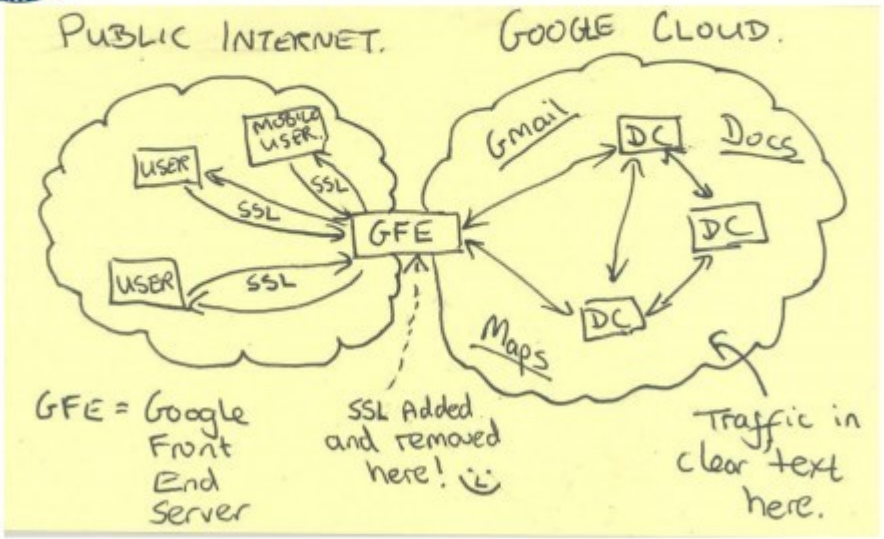
facilita
- frittate
- volpi

Sicurezza Cibernetica

Comp

TOP SECRET//SI//NOFORN

Current Efforts - Google



TOP SECRET//SI//NOFORN

. . .

dba

mettere
tutte le uova
in un paniere

produce
lock-in

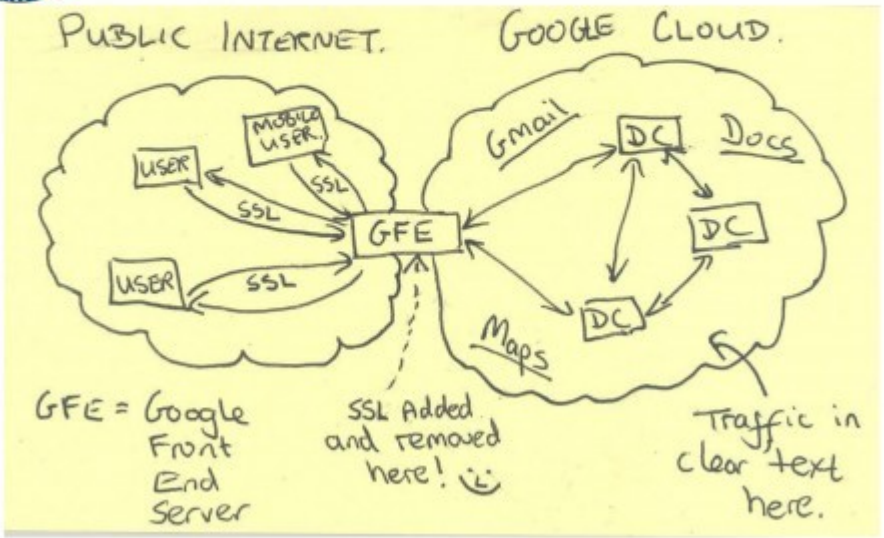
facilita
- frittate
- volpi

Sicurezza Cibernetica

Comp

TOP SECRET//SI//NOFORN

Current Efforts - Google



TOP SECRET//SI//NOFORN

produce
lock-in

facilita
- frittate
- volpi

dba

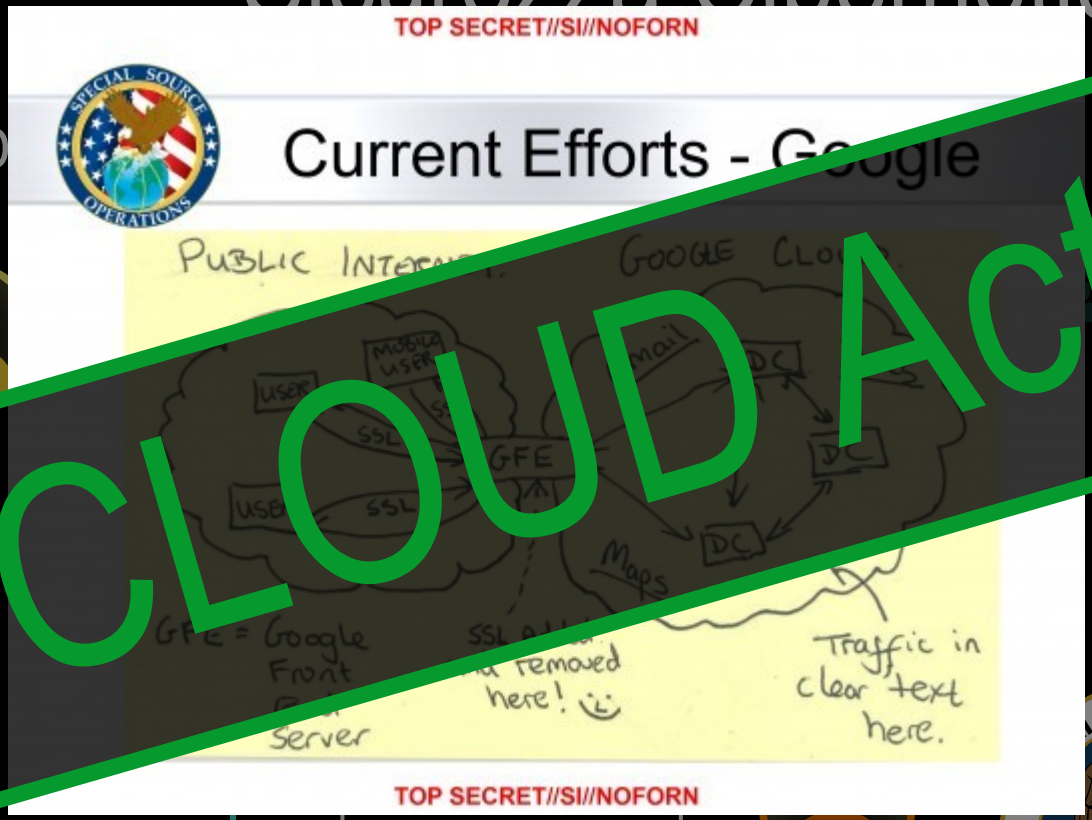
. . .

Sicurezza Cibernetica

Comp

produce
lock-in

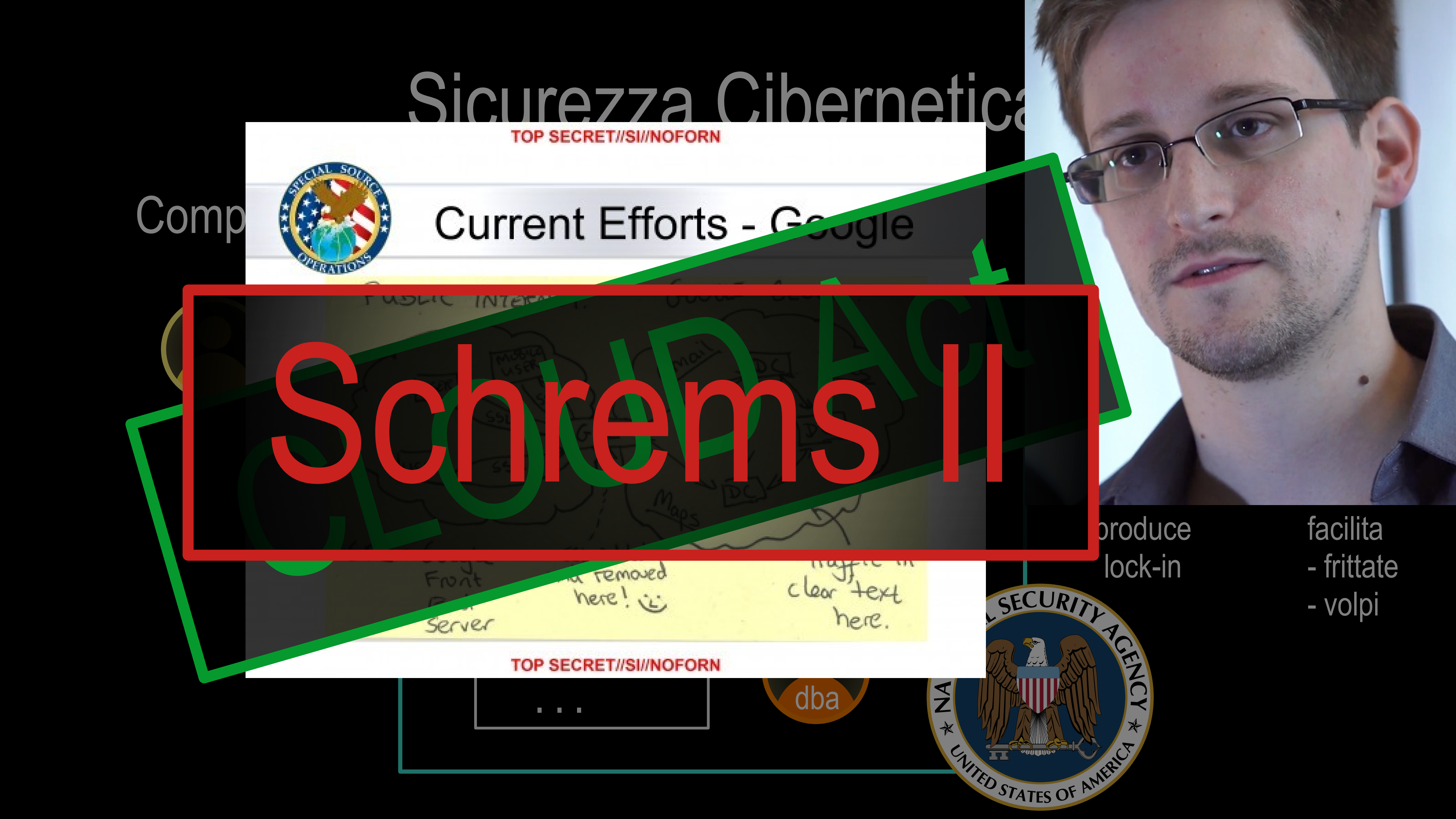
facilita
- frittate
- volpi



CLOUD Act

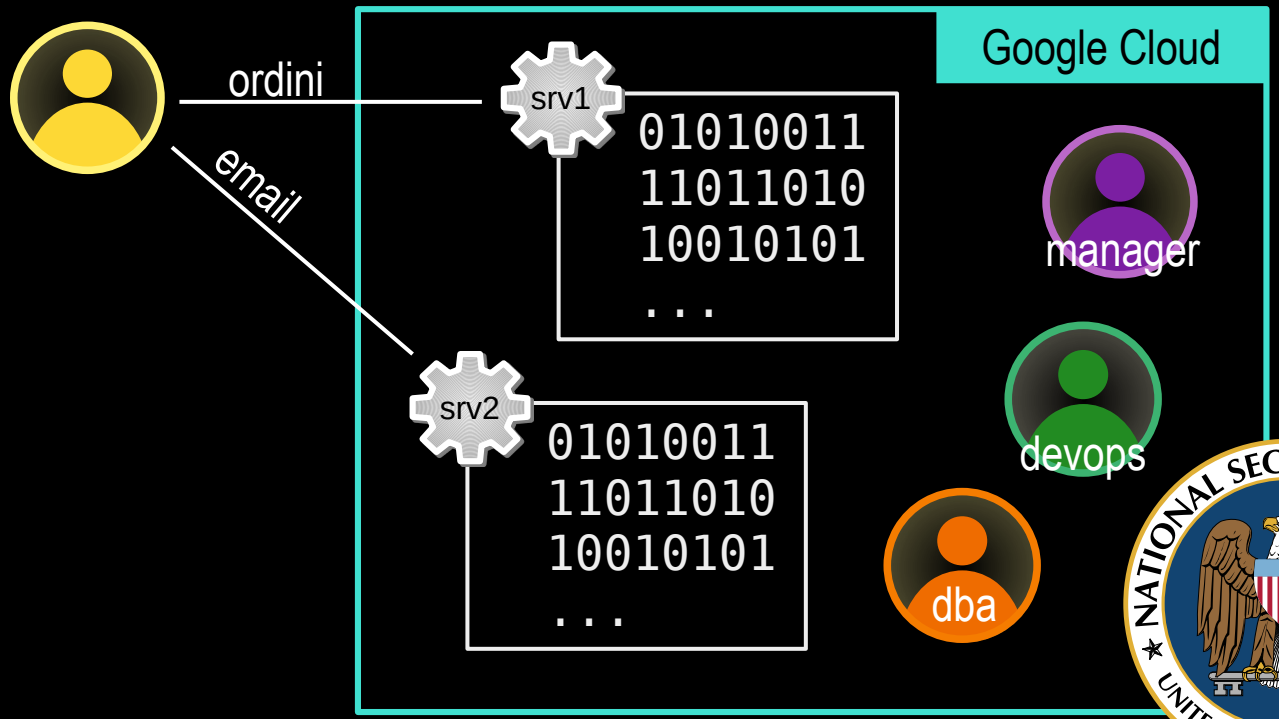
dba

. . .


Sicurezza Cibernetica
Comp
TOP SECRET//SI//NOFORN
Current Efforts - Google
Schrems II
CLOUD Act
produce
lock-in
facilita
- frittate
- volpi
dba
clear text
here.
TOP SECRET//SI//NOFORN

Sicurezza Cibernetica

Compartimentare i Dati



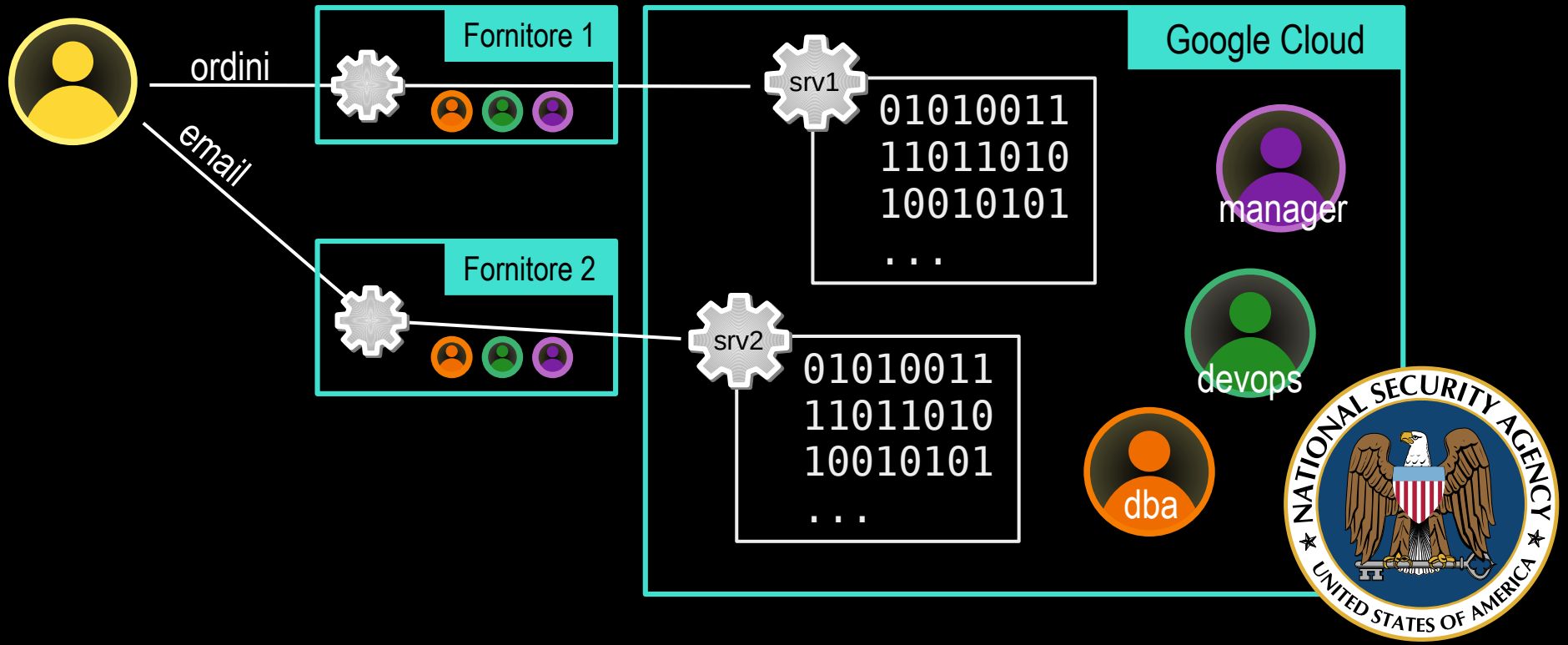
mettere
tutte le uova
in un paniere

produce
lock-in

facilita
- frittate
- volpi

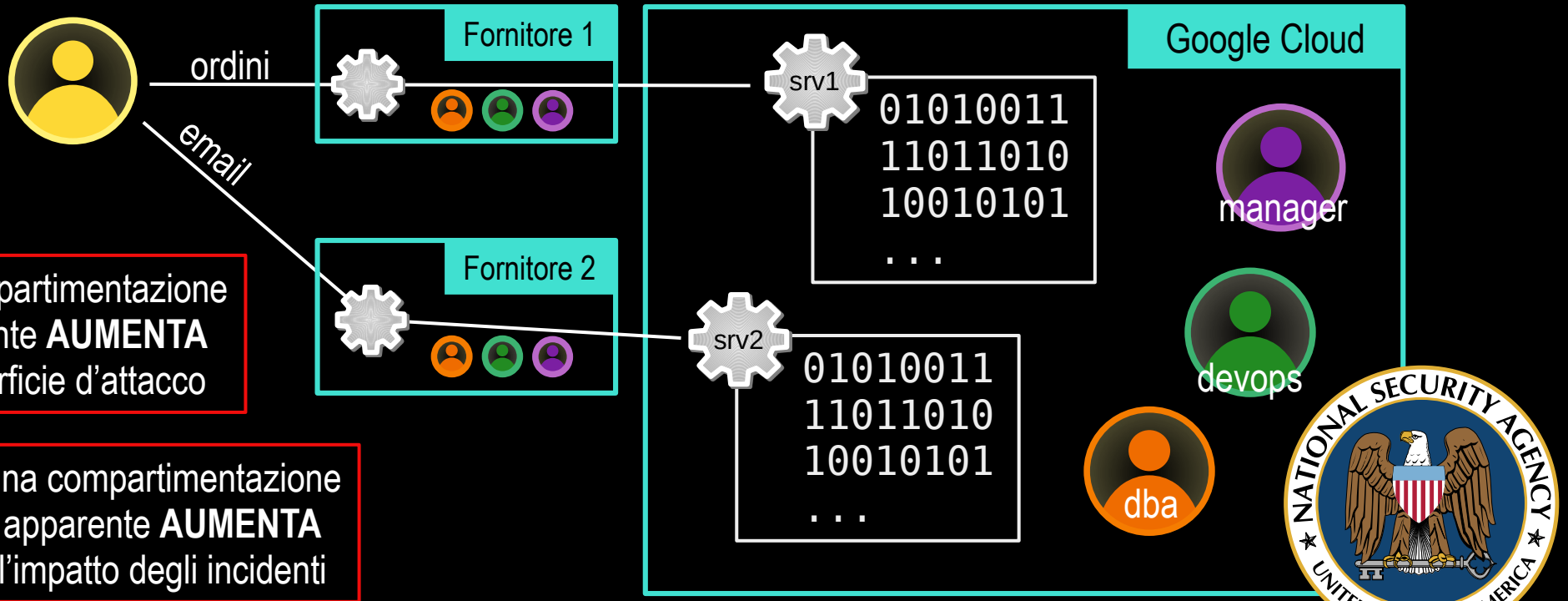
Sicurezza Cibernetica

Compartimentare i Dati



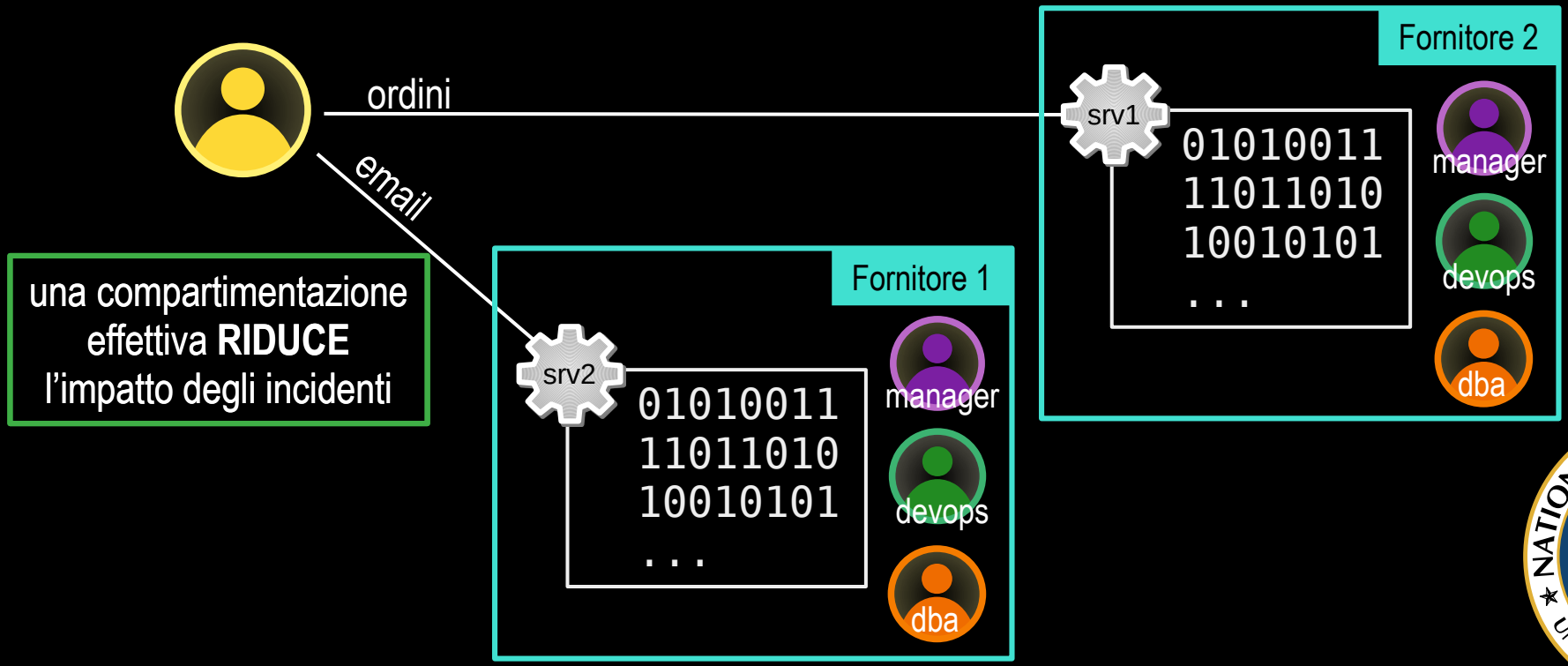
Sicurezza Cibernetica

Compartimentare i Dati



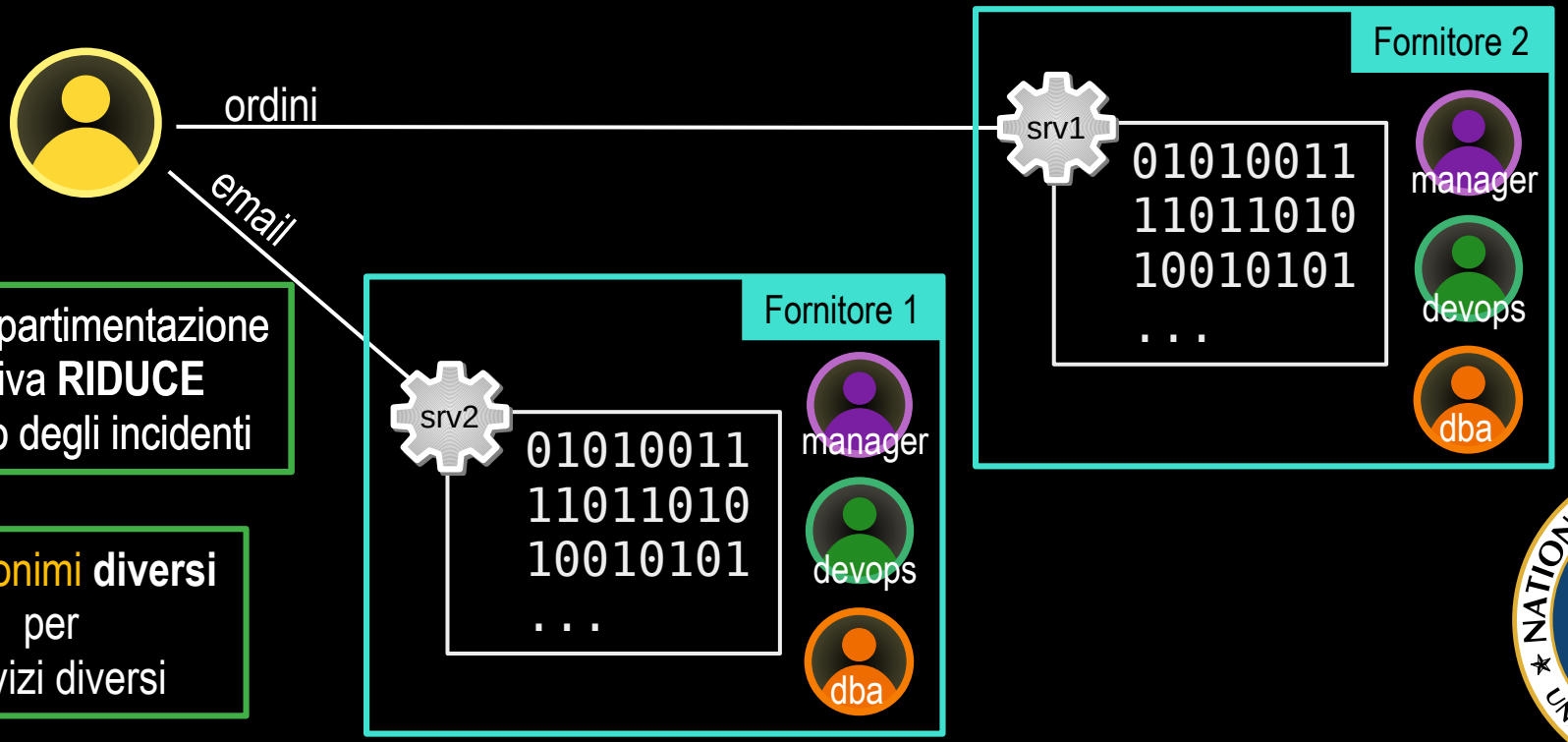
Sicurezza Cibernetica

Compartimentare i Dati



Sicurezza Cibernetica

Compartimentare i Dati, gli Identificativi

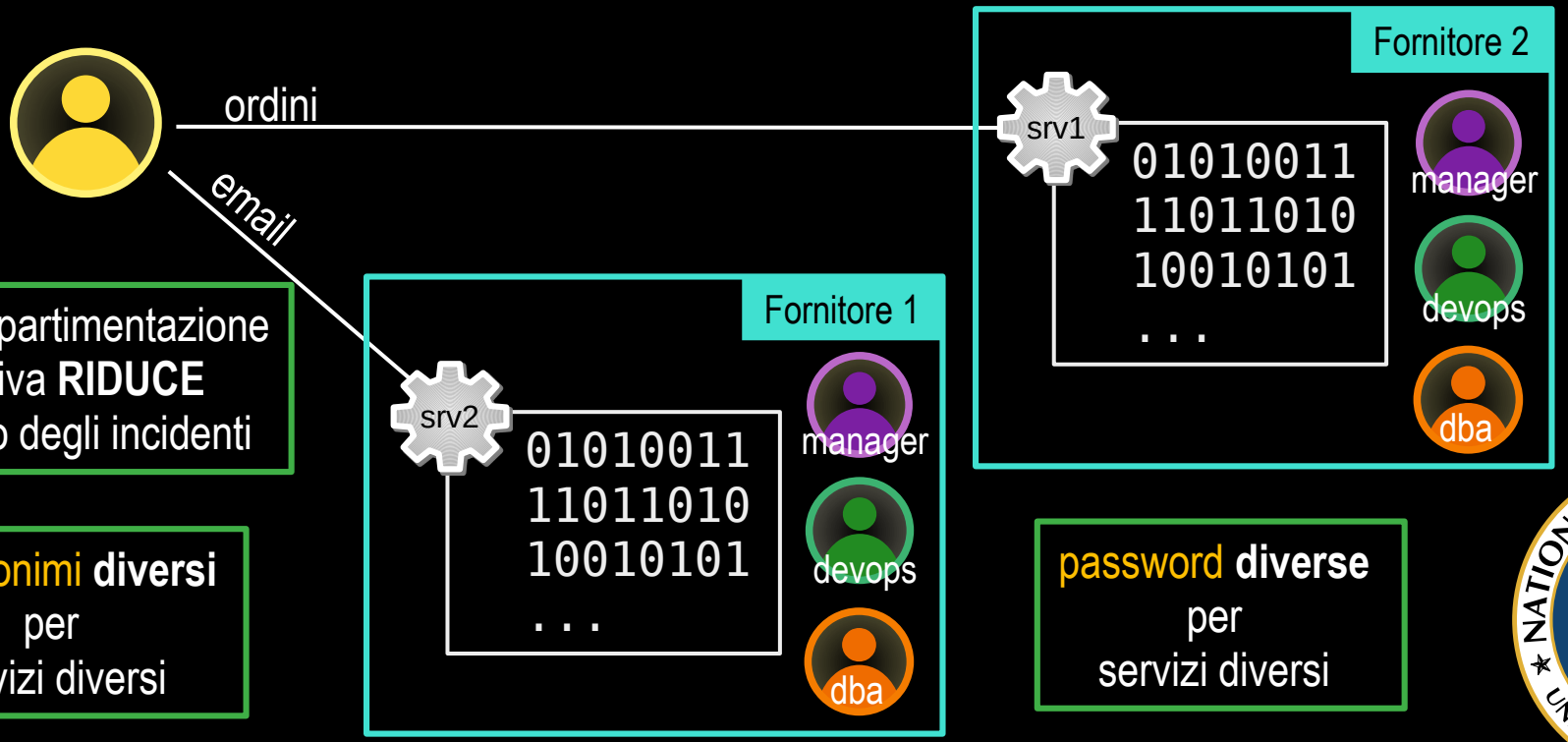


una compartimentazione effettiva **RIDUCE** l'impatto degli incidenti

pseudonimi **diversi** per servizi diversi

Sicurezza Cibernetica

Compartimentare i Dati, gli Identificativi e le Password



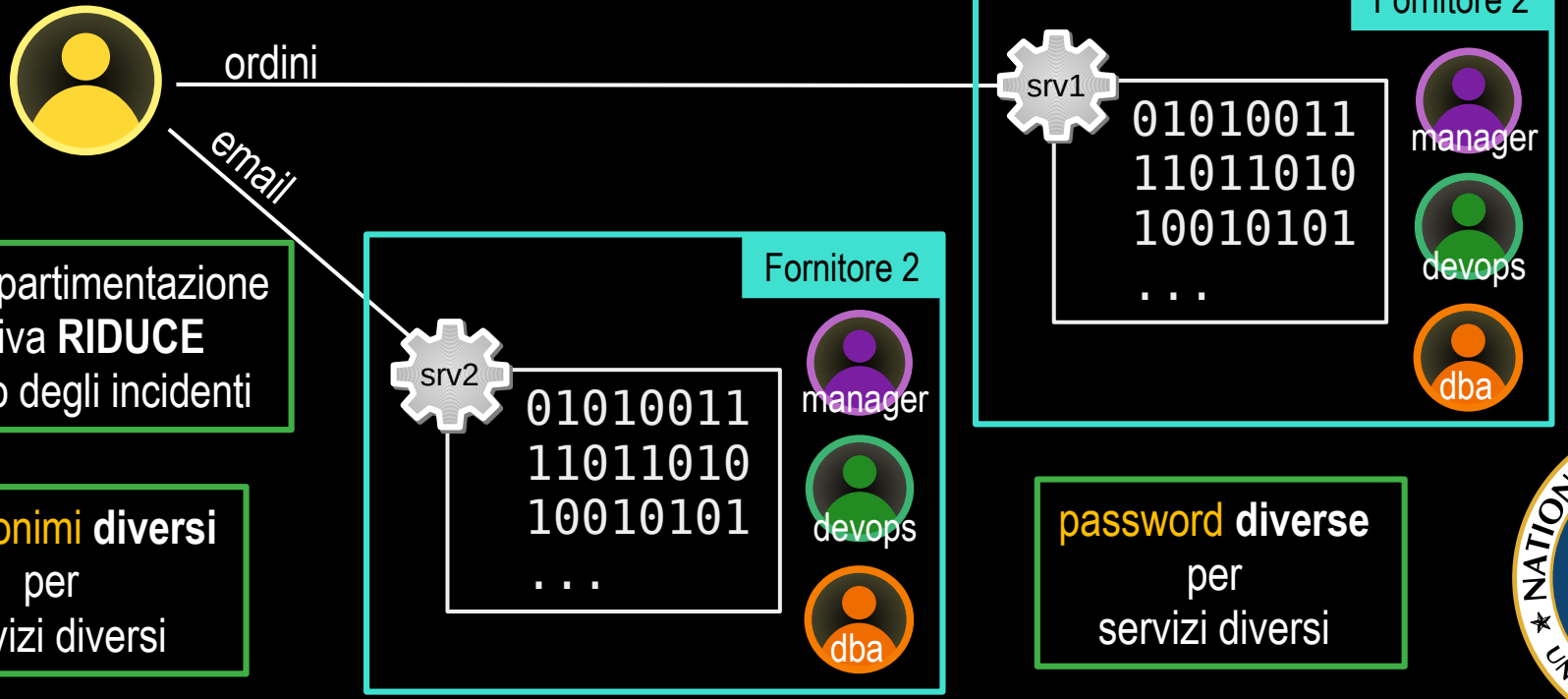
una compartimentazione effettiva **RIDUCE** l'impatto degli incidenti

pseudonimi **diversi** per servizi diversi

password **diverse** per servizi diversi

Sicurezza Cibernetica

Compartimentare i Dati, gli Identificativi e le Password



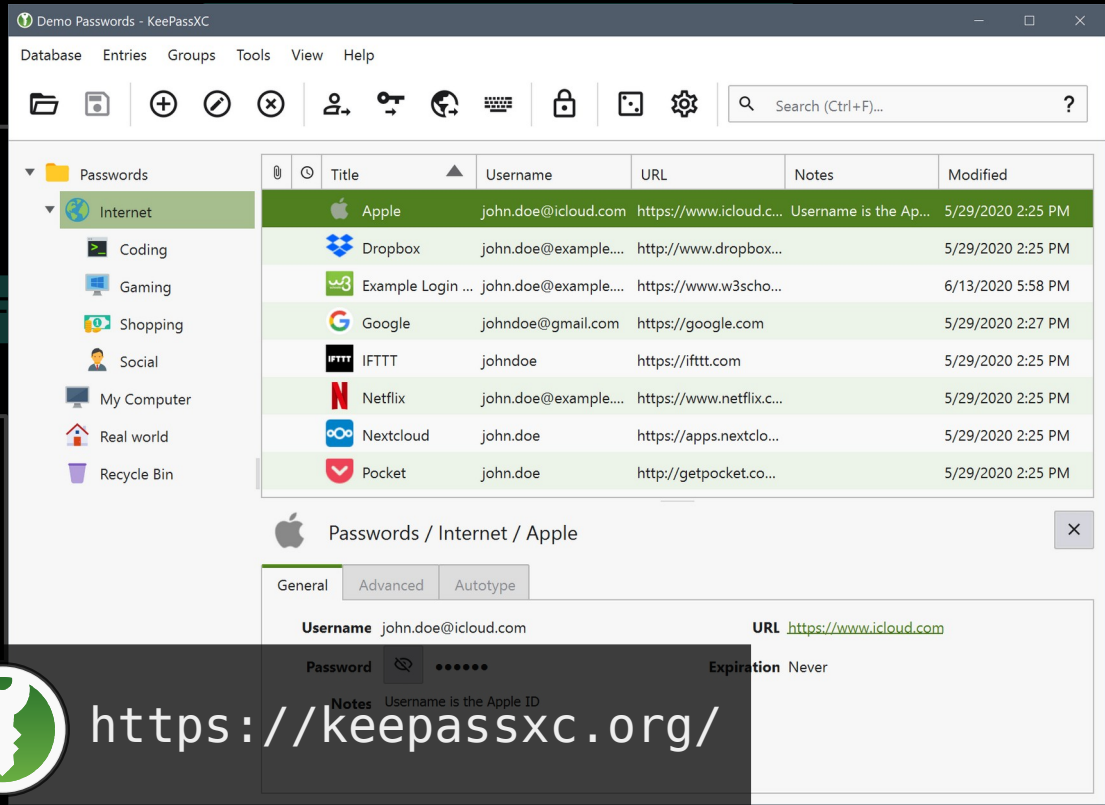
una compartimentazione effettiva **RIDUCE** l'impatto degli incidenti

pseudonimi **diversi** per servizi diversi

password **diverse** per servizi diversi

Sicurezza Cibernetica

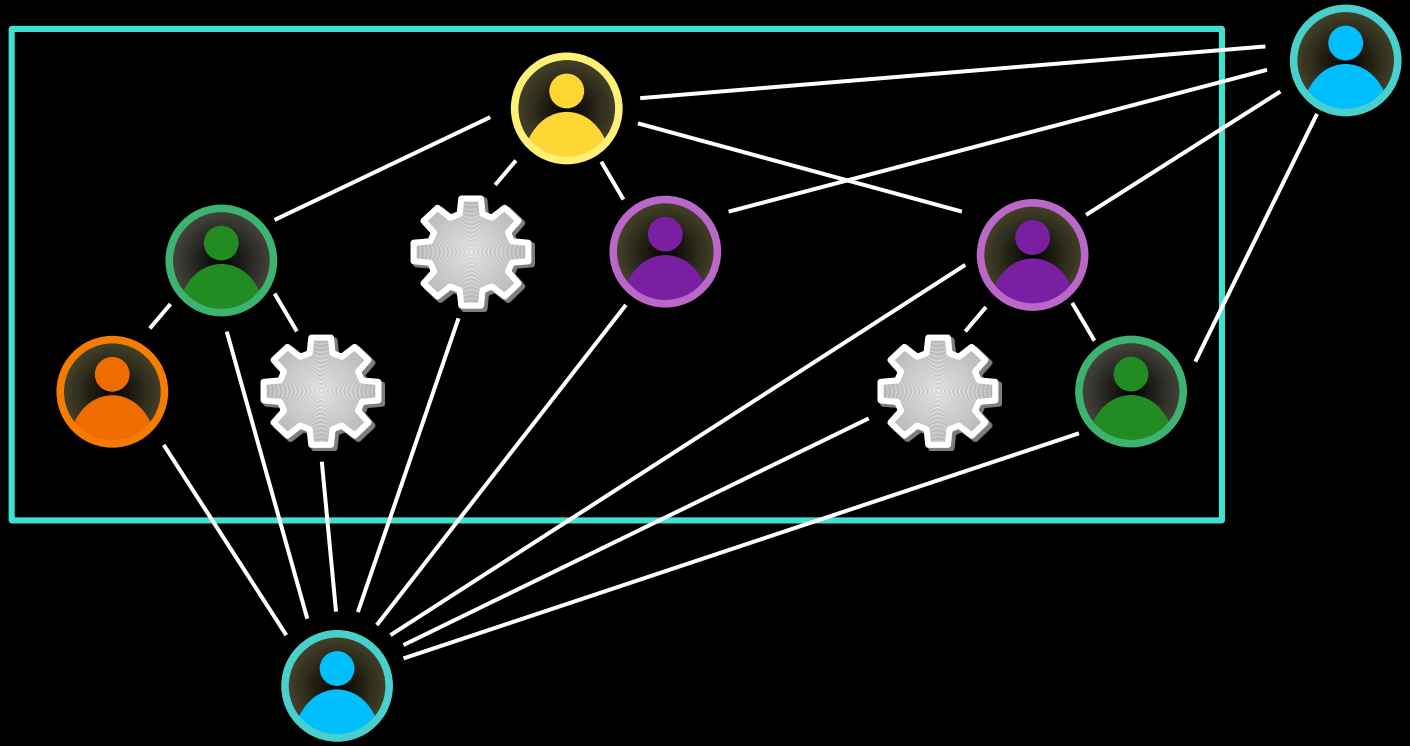
Compartimentare i Dati, gli Identificativi e le Password



https://keepassxc.org/

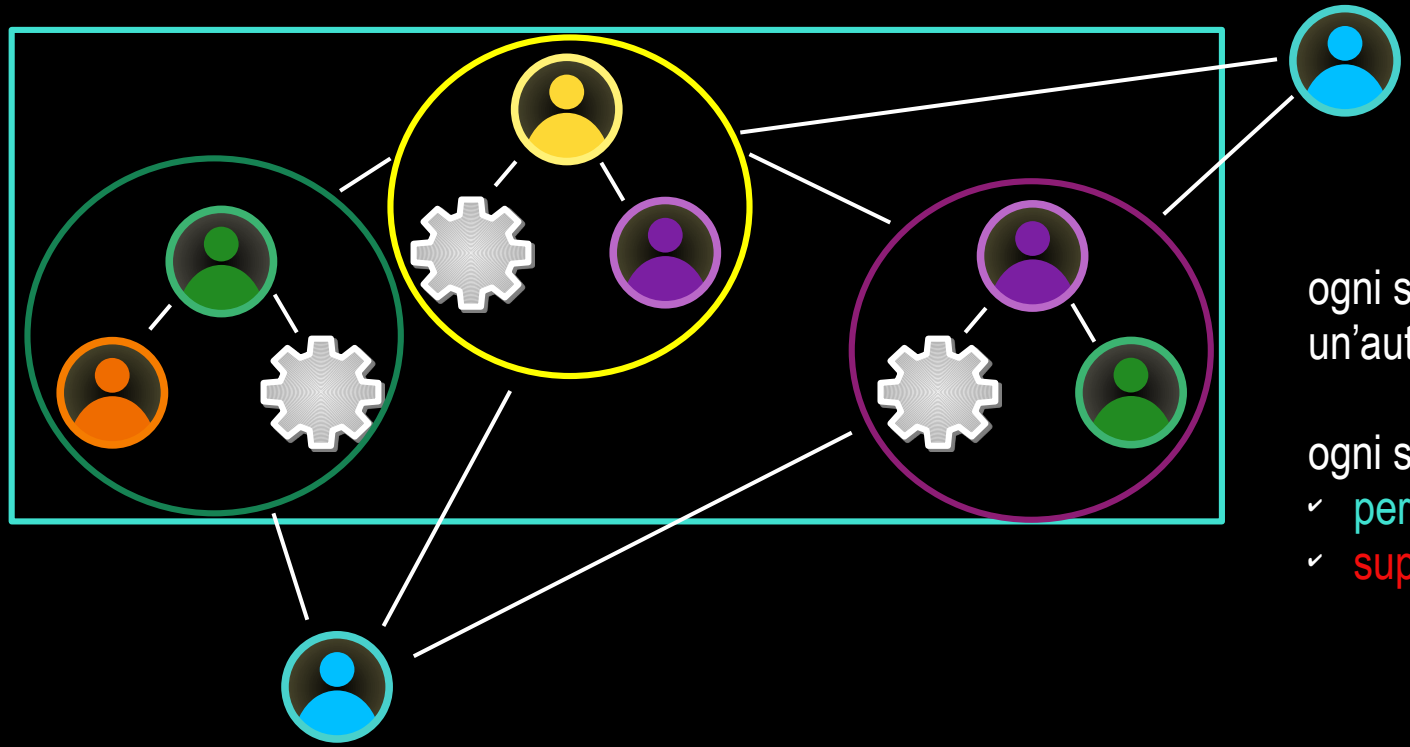
Sicurezza Cibernetica

Compartimentare l’organizzazione



Sicurezza Cibernetica

Compartimentare l'organizzazione riduce la superficie d'attacco



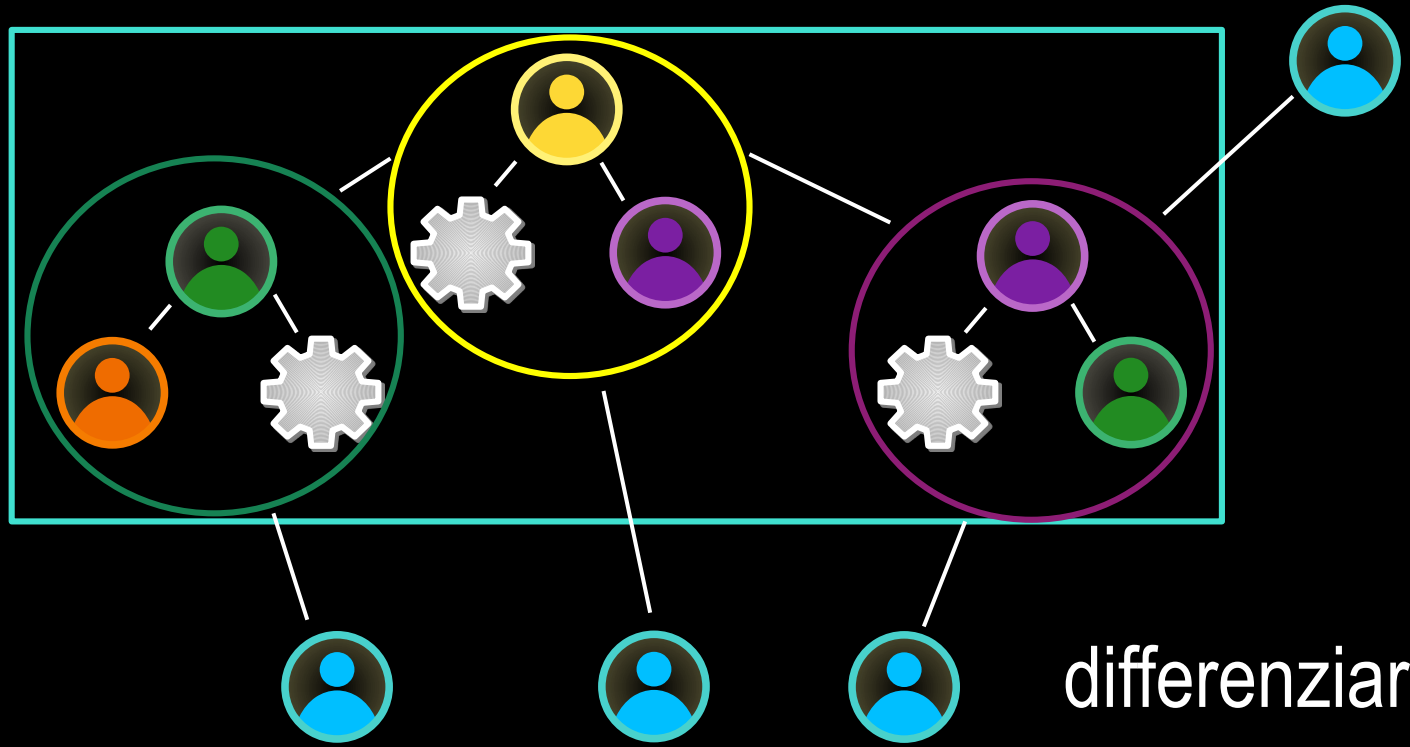
ogni sottogruppo costituisce un'autonomia a sé stante

ogni sottogruppo determina

- ✔ perimetro di sicurezza
- ✔ superficie di attacco

Sicurezza Cibernetica

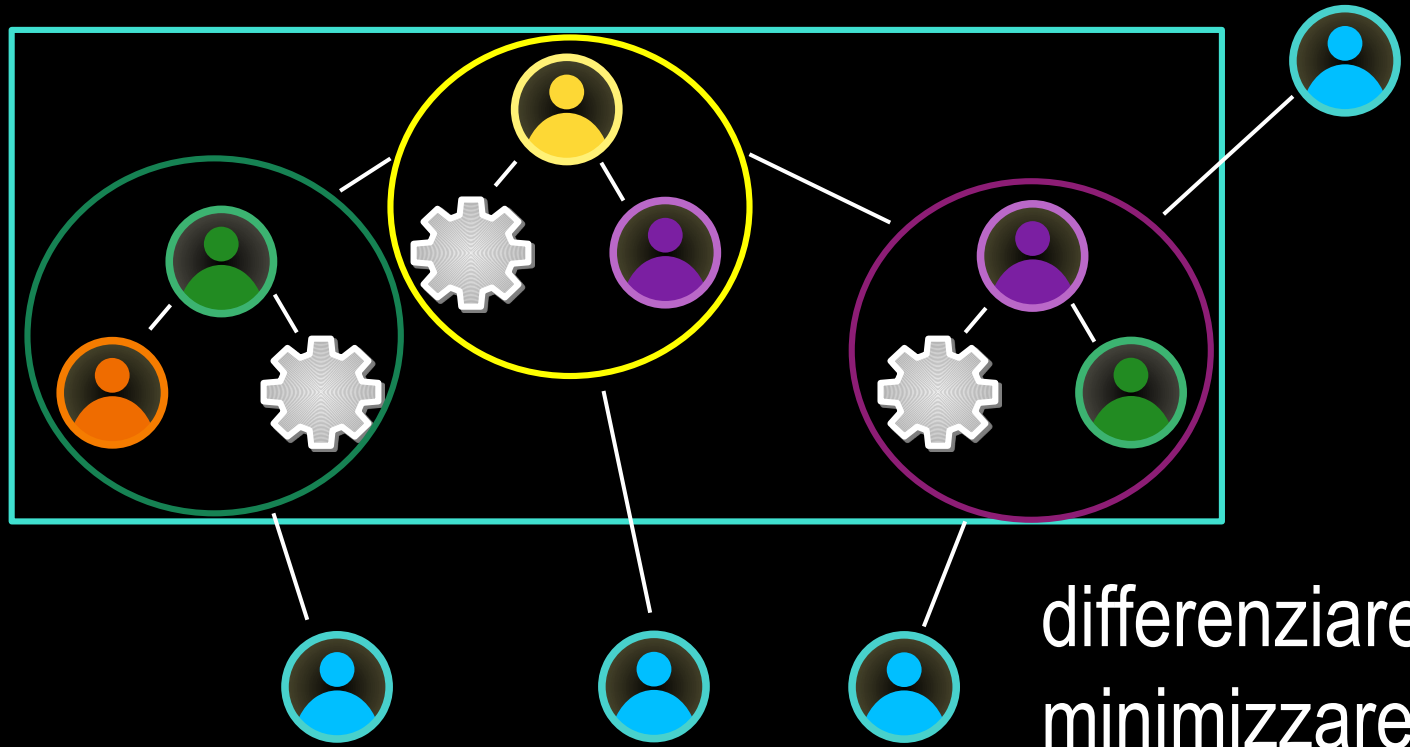
Compartimentare l'organizzazione riduce la superficie d'attacco



differenziare il rischio

Sicurezza Cibernetica

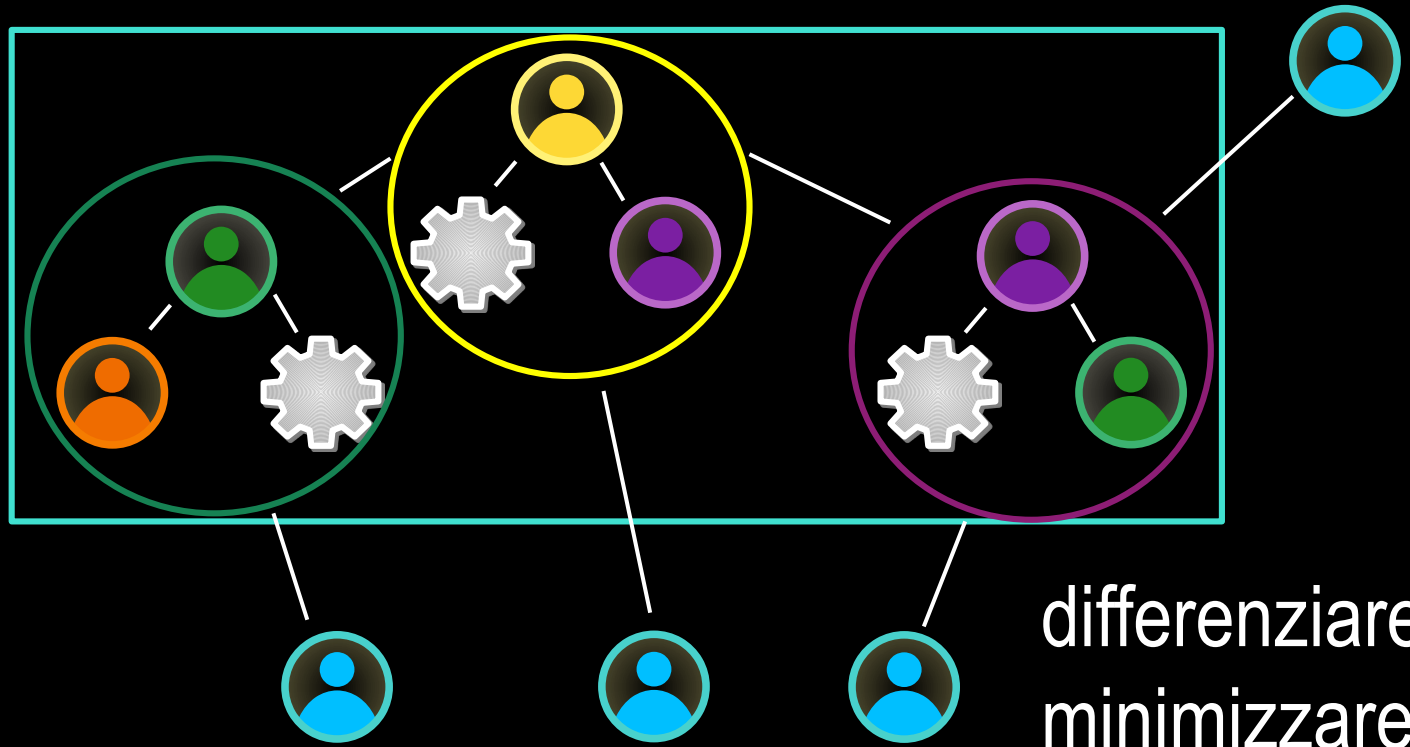
Compartimentare l'organizzazione riduce la superficie d'attacco



differenziare
minimizzare
il rischio

Sicurezza Cibernetica

Compartimentare l'organizzazione riduce la superficie d'attacco



differenziare
minimizzare
il rischio

Rischio Cibernetico

ISO 31000 → strategie di gestione del rischio:

1. evitare il rischio, evitando le attività che lo introducono
2. accettare il rischio per sfruttare un'opportunità
3. rimuovere la sorgente del rischio
4. ridurre la probabilità del rischio
5. ridurre l'impatto del rischio
6. condividere il rischio con altri
7. mantenere il rischio accettando le conseguenze

Rischio Cibernetico

ISO 31000 → strategie di gestione del rischio:

1. evitare il rischio, evitando le attività che lo introducono
2. accettare il rischio per sfruttare un'opportunità
3. rimuovere la sorgente del rischio
4. ridurre la probabilità del rischio
5. ridurre l'impatto del rischio
6. condividere il rischio con altri
7. mantenere il rischio accettando le conseguenze

Rischio Cibernetico

ISO 31000 → strategie di gestione del rischio:

1. evitare il rischio, evitando le attività che lo introducono
2. accettare il rischio per sfruttare un'opportunità
3. rimuovere la sorgente del rischio
4. ridurre la probabilità del rischio
5. ridurre l'impatto del rischio
6. condividere il rischio con altri
7. mantenere il rischio accettando le conseguenze

Rischio Cibernetico

Rischio = Vulnerabilità $\times$ Minaccia $\times$ Impatto

Ogni rischio è caratterizzato da una vulnerabilità
che una minaccia può sfruttare producendo un impatto

Rischio Cibernetico

Rischio = Vulnerabilità $\times$ Minaccia $\times$ Impatto

Ogni rischio è caratterizzato da una vulnerabilità
che una minaccia può sfruttare producendo un impatto

- quando questa condizione si verifica $\longrightarrow$ danno
  - responsabilità + incident analysis $\longrightarrow$ riduzione rischi futuri
  - scaricabarile $\longrightarrow$ immobilità $\longrightarrow$ aumento rischi futuri

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

Ogni rischio è caratterizzato da una vulnerabilità
che una minaccia può sfruttare producendo un impatto

- quando questa condizione si verifica ⟶ danno
  - responsabilità + incident analysis ⟶ riduzione rischi futuri
  - scaricabarile ⟶ immobilità ⟶ aumento rischi futuri
- per ridurre il rischio è necessario intervenire su questi 3 fattori

Rischio Cibernetico

Rischio = Vulnerabilità $\times$ Minaccia $\times$ Impatto

Si definisce “minaccia” ogni fenomeno fuori dal controllo e/o fuori dalla consapevolezza dell’organizzazione cibernetica che costituisce un pericolo per l’organizzazione stessa o i suoi membri

Rischio Cibernetico

Se conosci il nemico e te stesso, la tua vittoria è sicura.

Se conosci te stesso ma non il nemico,
potrai vincere o perdere in egual misura.

Se non conosci né il nemico né te stesso, perderai sempre.

Sun Tsu – L'arte della Guerra

Rischio Cibernetico

Rischio = Vulnerabilità $\times$ Minaccia $\times$ Impatto

Si definisce “minaccia” ogni fenomeno fuori dal controllo e/o fuori dalla consapevolezza dell’organizzazione cibernetica che costituisce un pericolo per l’organizzazione stessa o i suoi membri

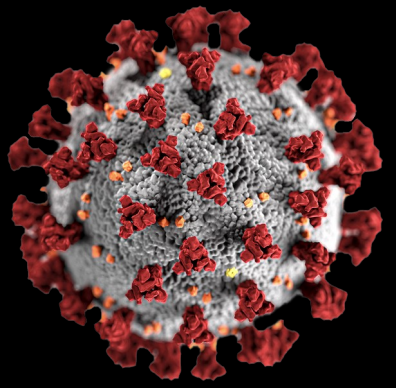
- non è possibile eliminarla

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

Si definisce “minaccia” ogni fenomeno fuori dal controllo e/o fuori dalla consapevolezza dell’organizzazione cibernetica che costituisce un pericolo per l’organizzazione stessa o i suoi membri

- non è possibile eliminarla
- può essere ignota ed imprevista

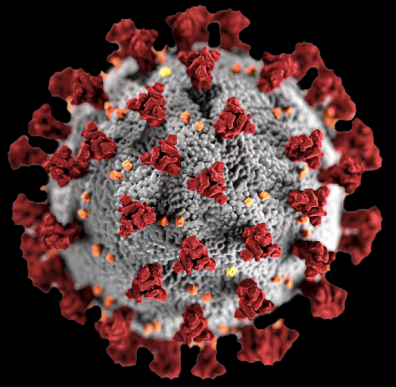


Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

Si definisce “minaccia” ogni fenomeno fuori dal controllo e/o fuori dalla consapevolezza dell’organizzazione cibernetica che costituisce un pericolo per l’organizzazione stessa o i suoi membri

- non è possibile eliminarla
- può essere ignota ed imprevista
- proteggersi dalle minacce note può ostacolare quelle ignote



Rischio Cibernetico

Rischio = Vulnerabilità $\times$ Minaccia $\times$ Impatto

Threat Modeling

processo di identificazione e studio delle minacce,
delle mitigazioni possibili e delle loro priorità

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

Threat Modeling

processo di identificazione e studio delle minacce,
delle mitigazioni possibili e delle loro priorità

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

Threat Modeling

processo di identificazione e studio delle minacce, delle mitigazioni possibili e delle loro priorità

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

Threat Modeling

processo di identificazione e studio delle minacce,
delle mitigazioni possibili e delle loro priorità

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

Threat Modeling

processo di identificazione e studio delle minacce,
delle mitigazioni possibili e delle loro priorità

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

Threat Modeling

processo di identificazione e studio delle minacce, delle mitigazioni possibili e delle loro priorità

- esistono molte metodologie diverse
- tutte necessitano di profonda comprensione delle dinamiche cibernetiche e delle specificità dell'organizzazione

Rischio Cibernetico

Rischio = Vulnerabilità $\times$ Minaccia $\times$ Impatto

Threat Modeling $\longrightarrow$ conosci i tuoi nemici

- competenze tecniche
- motivazioni
- opportunità
- numerosità / dimensione

Rischio Cibernetico

Rischio = Vulnerabilità $\times$ Minaccia $\times$ Impatto

Threat Modeling: Competenze Tecniche

- nessuna competenza tecnica
- competenze superficiali
- “utente” avanzato
- programmatore / amministratore di sistema
- esperto nella “penetrazione” dei sistemi

Rischio Cibernetico

Rischio = Vulnerabilità $\times$ Minaccia $\times$ Impatto

Threat Modeling: Motivazione all'Attacco

- nulla: l'attaccante non può trarre alcun vantaggio
- probabile: l'attaccante può trarre qualche vantaggio
- elevata: l'attaccante otterrà un vantaggio notevole

Rischio Cibernetico

Rischio = Vulnerabilità $\times$ Minaccia $\times$ Impatto

Threat Modeling: Opportunità

- l'attacco richiede accesso completo o strumenti molto costosi
- l'attacco richiede accesso riservato o strumenti particolari
- l'attacco richiede un qualsiasi tipo di accesso
- l'attacco non richiede accesso alla vittima

Rischio Cibernetico

Rischio = Vulnerabilità $\times$ Minaccia $\times$ Impatto

Threat Modeling: Numerosità / Dimensione

- sviluppatori o sistemisti dell'organizzazione
- membri dell'organizzazione
- partner, fornitori, clienti...
- agenti anonimi su Internet

Rischio Cibernetico

Rischio = Vulnerabilità $\times$ Minaccia $\times$ Impatto

Threat Modeling $\longrightarrow$ conosci i tuoi nemici

- competenze tecniche
- motivazioni
- opportunità
- numerosità / dimensione

Rischio Cibe

Rischio = Vulnerabilità ×

Threat Modeling ⟶ conosc

- competenze tecniche
- motivazioni
- opportunità
- numerosità / dimensione

Rischio Cibe

SIENA

Università, scritte fasciste e omofobe nell'ufficio di una delegata Cgil

antifascismo | siena

15/04/2022 - 11:39

Ait Cronaca

Attaccata la sede della Cgil a Roma, Landini: 'Squadrismo fascista'

Redazione ANSA

ROMA

10 ottobre 2021 09:22 NEWS

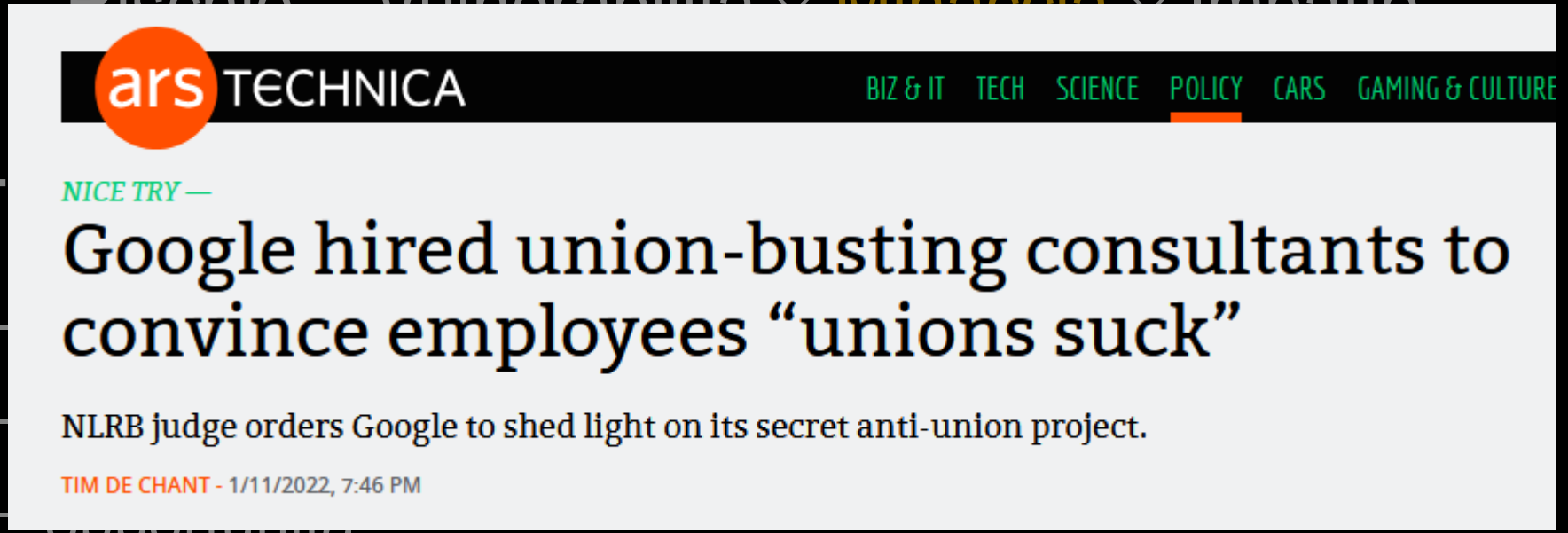
FORZA NUOVA

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

T

- opportunità
- numerosità / dimensione



ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

NICE TRY —

Google hired union-busting consultants to convince employees “unions suck”

NLRB judge orders Google to shed light on its secret anti-union project.

TIM DE CHANT - 1/11/2022, 7:46 PM

ernetico

× Minaccia × Impatto

Threat Modeling ⟶ conosci i tuoi nemici

- competenze tecniche
- motivazioni
- opportunità
- numerosità / dimensione

ernetico

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

NICE TRY —

Google hired union-busting consultants to

FACEBOOK PITCHED NEW TOOL ALLOWING EMPLOYERS TO SUPPRESS WORDS LIKE "UNIONIZE" IN WORKPLACE CHAT PRODUCT

Facebook Workplace is used by employers as large as Walmart. The new tool would allow "content control" to prevent certain topics from trending internally.

Lee Fang

June 12 2020, 4:04 a.m.

– numerosità / dimensione

ernetico


ars TECHNICA

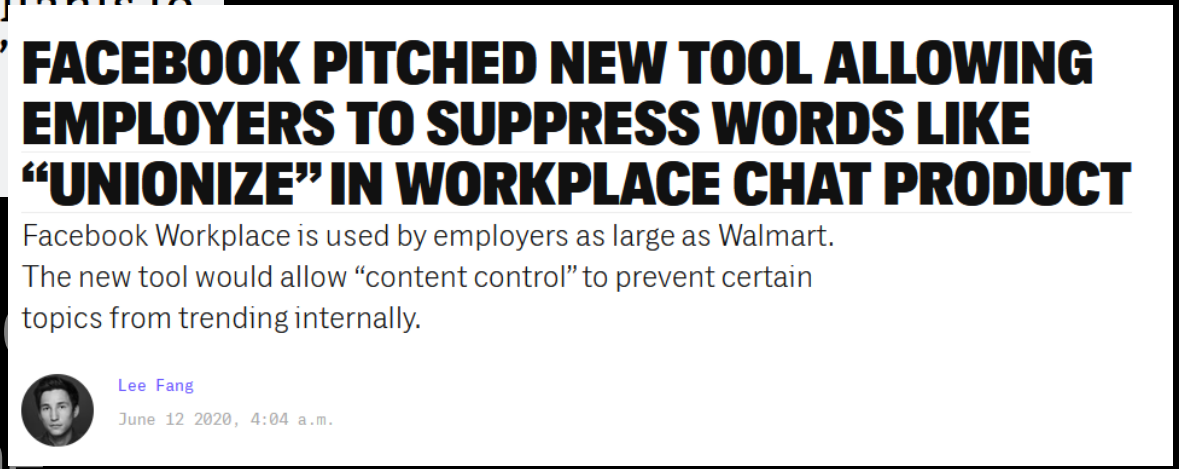
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

NICE TRY —

Google hired union-busting consultants to convince employees "unions suck"

NLRB judge orders Google to shed light on its secret anti-union project.

TIM DE CHANT - 1/11/2022, 7:46 PM


FACEBOOK PITCHED NEW TOOL ALLOWING EMPLOYERS TO SUPPRESS WORDS LIKE "UNIONIZE" IN WORKPLACE CHAT PRODUCT

Facebook Workplace is used by employers as large as Walmart. The new tool would allow "content control" to prevent certain topics from trending internally.

Lee Fang

June 12 2020, 4:04 a.m.

Threat Modeling ⟶

- competenze tecniche
- motivazioni
- opportunità
- numerosità / dimensione

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

NICE TRY —

Google hired union-busting consultants to convince employees "unions suck"

NLRB judge orders Google to shed light on its secret anti-union project.

TIM DE CHANT - 1/11/2022, 7:46 PM

ernetico

Thr

FACEBOOK PITCHED NEW TOOL ALLOWING EMPLOYERS TO SUPPRESS WORDS LIKE "UNIONIZE" IN WORKPLACE CHAT PRODUCT

Amazon says union and NLRB "suppressed and influenced" Staten Island election

It alleges the groups acted worse than it did in Bessemer

By Mitchell Clark | Apr 8, 2022, 6:50pm EDT

The objections expand upon a document the company recently submitted that signaled its intent to fight the election results — the company now says that ALU members "intimidated employees," "recorded voters in the polling place," and "distributed marijuana to employees in exchange for their support," according to an excerpt posted by *Financial Times* reporter Dave Lee.

ernetico

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

NICE TRY —

Google hired union-busting consultants to convince employees "unions suck"

NLRB judge orders Google to shed light on its secret anti-union project.

TIM DE CHANT - 1/11/2022, 7:46 PM

FACEBOOK PITCHED NEW TOOL ALLOWING EMPLOYERS TO SUPPRESS WORDS LIKE "UNIONIZE" IN WORKPLACE CHAT PRODUCT

Facebook Workplace is used by employers as large as Walmart. The new tool would allow "content control" to prevent certain topics from trending internally.

Lee Fang

June 12 2020, 4:04 a.m.

Threat Modeling ⟶

- competenze tecniche
- motivazioni
- opportunità
- numerosità / dimensione

Amazon says union and NLRB "suppressed and influenced" Staten Island election

It alleges the groups acted worse than it did in Bessemer

By Mitchell Clark | Apr 8, 2022, 6:50pm EDT

The objections expand upon a document the company recently submitted that signaled its intent to fight the election results — the company now says that ALU members "intimidated employees," "recorded voters in the polling place," and "distributed marijuana to employees in exchange for their support," according to an excerpt posted by *Financial Times* reporter Dave Lee.

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

NICE TRY —

Goo
cor

NLRB ju

TIM DE CH

ernetico

LEAKED: NEW AMAZON WORKER CHAT APP WOULD BAN WORDS LIKE "UNION," "RESTROOMS," "PAY RAISE," AND "PLANTATION"

Also: "Grievance," "slave labor," "This is dumb," "living wage," "diversity," "vaccine," and others.

Ken Klippenstein

April 4 2022, 9:27 p.m.

numerosità / dimensione

employees," "recorded voters in the polling place," and "distributed marijuana to employees in exchange for their support," according to an excerpt posted by *Financial Times* reporter Dave Lee.

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

ernetico

NICE TRY —

Google hired union-busting consultants to convince employees "unions suck"

NLRB judge orders Google to shed light on its secret anti-union project.

TIM DE CHANT - 1/11/2022, 7:46 PM

Threat Modeling →

FACEBOOK PITCHED NEW TOOL ALLOWING EMPLOYERS TO SUPPRESS WORDS LIKE "UNIONIZE" IN WORKPLACE CHAT PRODUCT

Facebook Workplace is used by employers as large as Walmart. The new tool would allow "content control" to prevent certain topics from trending internally.

LEAKED: NEW AMAZON WORKER CHAT APP WOULD BAN WORDS LIKE "UNION," "RESTROOMS," "PAY RAISE," AND "PLANTATION"

Also: "Grievance," "slave labor," "This is dumb," "living wage," "diversity," "vaccine," and others.

Ken Klippenstein

April 4 2022, 9:27 p.m.

numerosità / dimensione

Amazon says union and NLRB "suppressed and influenced" Staten Island election

It alleges the groups acted worse than it did in Bessemer

By Mitchell Clark | Apr 8, 2022, 6:50pm EDT

The objections expand upon a document the company recently submitted that signaled its intent to fight the election results — the company now says that ALU members "intimidated employees," "recorded voters in the polling place," and "distributed marijuana to employees in exchange for their support," according to an excerpt posted by *Financial Times* reporter Dave Lee.

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

NICE TRY —

Google hired uni… convince employ…

NLRB judge orders Google to shed ligh…

TIM DE CHANT - 1/11/2022, 7:46 PM

ernetico

Intelligencer THE TECH WARS | Silicon Valley's Anti-Unionism, Now With a Sid…

In fact, a form of anti-union sentiment has been baked into the tech world's culture from the very beginning. Robert Noyce, the co-founder of Intel, so-called "Mayor of Silicon Valley," and one of the inventors of the microchip, once declared that "remaining non-union is essential for survival for most of our companies. If we had the work rules that unionized companies have, we'd all go out of business." Noyce and his fellow tech pioneers saw Silicon Valley's creation as an opportunity to break free of the traditional labor model, which they viewed as helpful for building cars and mining for ore, but not for the quick-moving, always-changing world of technology creation.

OOL ALLOWING WORDS LIKE E CHAT PRODUCT

Walmart.

certain

Threat M…

LEAKED: NEW… WOULD BAN … "RESTROOMS… "PLANTATION…

Also: "Grievance," "slave labor," "This is dumb," "living wage," "diversity," "vaccine," and others.

Ken Klippenstein

April 4 2022, 9:27 p.m.

numerosità / dimensione

NLRB "suppressed and influenced" Staten Island election

It alleges the groups acted worse than it did in Bessemer

By Mitchell Clark | Apr 8, 2022, 6:50pm EDT

The objections expand upon a document the company recently submitted that signaled its intent to fight the election results — the company now says that ALU members "intimidated employees," "recorded voters in the polling place," and "distributed marijuana to employees in exchange for their support," according to an excerpt posted by *Financial Times* reporter Dave Lee.

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

Threat Modeling ⟶ conosci i tuoi nemici

- competenze tecniche
- motivazioni
- opportunità
- numerosità / dimensione

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

Threat Modeling ⟶ conosci i tuoi nemici

- competenze tecniche
- motivazioni
- opportunità
- numerosità / dimensione

hio Cibernetico

erabilità × Minaccia × Impatto

→ conosci i tuoi nemici

che

nsione

Rischio Cibernetico

Rischio = Vulnerabilità $\times$ Minaccia $\times$ Impatto

Si definisce “vulnerabilità” ogni debolezza o difetto che può essere sfruttata contro l’organizzazione cibernetica o contro i suoi membri, autonomi o automatici

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

- bug o backdoor del software
- software proprietario, remoto o black box “AI”
- aggiornamenti automatici e/o “personalizzati”
- difficoltà economiche del personale
- errori di configurazione
- fornitori infedeli
- scelta errata del canale
- clima teso, competizione interna, paraculismo...
- ...

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

- bug o backdoor del software
- software proprietario, remoto o black box “AI”
- aggiornamenti automatici e/o “personalizzati”
- difficoltà economiche del personale
- errori di configurazione
- fornitori infedeli
- scelta errata del canale
- clima teso, competizione interna, paraculismo...
- ...

Rischio Cibernetico

Rischio = Vulnerabilità $\times$ Minaccia $\times$ Impatto

Il contributo al rischio di una vulnerabilità dipende da

- facilità di individuazione
- facilità di abuso
- notorietà (presso gli attaccanti)
- tracciabilità (presso le vittime)

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

Il contributo al rischio di una vulnerabilità dipende da

- facilità di individuazione
- facilità di abuso
- notorietà (presso gli attaccanti)
- tracciabilità (presso le vittime)

Common Vulnerabilities and Exposures
https://www.cvedetails.com/
https://cve.mitre.org/

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

Il contributo al rischio di una vulnerabilità dipende da

- facilità di individuazione
- facilità di abuso
- notorietà (presso gli attaccanti)
- tracciabilità (presso le vittime)

Common Vulnerabilities and Exposures
https://www.cvedetails.com/
https://cve.mitre.org/

0-days → vulnerabilità ignota agli interessati o priva di mitigazioni

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

Si definisce “vulnerabilità” ogni debolezza o difetto che può essere sfruttata contro l’organizzazione cibernetica
o contro i suoi membri, autonomi o automatici

- variano nel tempo e nello spazio
- tanto più difficili da individuare quanto più sono strutturali
- è sempre possibile ridurre notevolmente le vulnerabilità,
  ma talvolta è impossibile eliminarle completamente

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

Si definisce “impatto” il danno prodotto dalla minaccia attraverso lo sfruttamento di una o più vulnerabilità

Perdita di

- confidenzialità
- integrità
- disponibilità
- “accountability”

Danni

- finanziari
- d’immagine
- legali
- alla privacy

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

Si definisce “impatto” il danno prodotto dalla minaccia attraverso lo sfruttamento di una o più vulnerabilità

Perdita di
- confidenzialità
- integrità
- disponibilità
- “accountability”

Danni
- finanziari
- d’immagine
- legali
- alla privacy

} per quante persone?

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

Si definisce “impatto” il danno prodotto dalla minaccia attraverso lo sfruttamento di una o più vulnerabilità

- l’impatto potenziale varia nel tempo
- è possibile minimizzarlo
  - riducendo i dati e gli asset esposti al rischio
    compartimentazione + minimizzazione dati raccolti
  - riducendo la durata dell’attacco
    monitoraggio continuo ⟶ individuazione precoce

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

Si definisce “impatto” il danno prodotto dalla minaccia attraverso lo sfruttamento di una o più vulnerabilità

- l’impatto potenziale varia nel tempo
- è possibile minimizzarlo
  - riducendo i dati e gli asset esposti al rischio
    compartimentazione + minimizzazione dati raccolti
  - riducendo la durata dell’attacco
    monitoraggio continuo ⟶ individuazione precoce

~300 giorni
Tempo medio di rilevazione di un attacco informatico avvenuto con successo

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

Per ridurre il rischio cibernetico
è possibile intervenire solo su

- Vulnerabilità
- Impatto

} variano nel tempo →

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

Per ridurre il rischio cibernetico
è possibile intervenire solo su

- Vulnerabilità
- Impatto

variano nel tempo →

Misurate !!!

Rischio Cibernetico

Rischio = Vulnerabilità × Minaccia × Impatto

È possibile stimare il rischio
con simulazioni periodiche

“Penetration” test

attacchi effettuati da esperti
di sicurezza per individuare
vulnerabilità e stimare impatti

Disaster Recovery test

simulazioni di ripristino dei
backup con verifica dei risultati

Sicurezza Cibernetica

Superficie di Attacco

insieme dei canali di comunicazione che connettono i membri di un'organizzazione cibernetica (automatismi o autonomie) con agenti esterni all'organizzazione.

La superficie di attacco cresce rapidamente al crescere di una organizzazione cibernetica: ogni membro può estenderla.

Per proteggerla è necessario:

- compartimentare, differenziare, minimizzare i rischi
- diffondere una piena cittadinanza cibernetica

Sicurezza Cibernetica

Superficie di Attacco

insieme dei canali di comunicazione che connettono i membri di un'organizzazione cibernetica (automatismi o autonomie) con agenti esterni all'organizzazione.

La superficie di attacco cresce rapidamente al crescere di una organizzazione cibernetica: ogni membro può estenderla.

Per proteggerla è necessario:

- compartimentare, differenziare, minimizzare i rischi
- diffondere una piena cittadinanza cibernetica

ogni catena è forte quanto il suo anello più debole

Sicurezza Cibernetica

Superficie di Attacco

insieme dei canali di comunicazione che connettono i membri di un'organizzazione cibernetica (automatismi o autonomie) con agenti esterni all'organizzazione.

La superficie di attacco cresce rapidamente al crescere di una organizzazione cibernetica: ogni membro può estenderla.

Per proteggerla è necessario:

- compartimentare, differenziare, minimizzare i rischi
- diffondere una piena cittadinanza cibernetica

ogni catena è forte quanto il suo anello più debole

Cittadinanza Cibernetica

Viviamo in una Società Cibernetica.

Cittadinanza Cibernetica

Viviamo in una Società Cibernetica.

- cambio di paradigma: da Economia a Informatica
  - evidente in finanza → HFT ...e criptoMENATE
  - inevitabile: il denaro è un dato (ma non viceversa)

Cittadinanza Cibernetica

Viviamo in una Società Cibernetica.

- cambio di paradigma: da Economia a Informatica
  - evidente in finanza → HFT ...e criptoMENATE
  - inevitabile: il denaro è un dato (ma non viceversa)
- nuovo conflitto di classe
  - hacker → massimizzazione della Conoscenza
  - capitalisti della Sorveglianza → potere egemonico

Cittadinanza Cibernetica

Viviamo in una Società Cibernetica.

- cambio di paradigma: da Economia a Informatica
  - evidente in finanza → HFT ...e criptoMENATE
  - inevitabile: il denaro è un dato (ma non viceversa)
- nuovo conflitto di classe
  - hacker → massimizzazione della Conoscenza
  - capitalisti della Sorveglianza → potere egemonico

le menti umane sono l'oggetto del contendere

Cittadinanza Cibernetica

Viviamo in una Società Cibernetica.
Vogliamo che sia Democratica?

Cittadinanza Cibernetica

Viviamo in una Società Cibernetica.

Vogliamo che sia Democratica?

In una società cibernetica, la cittadinanza presuppone

- totale comprensione dei meccanismi di funzionamento degli automatismi
- partecipazione alla loro progettazione
- capacità di alterarne il funzionamento

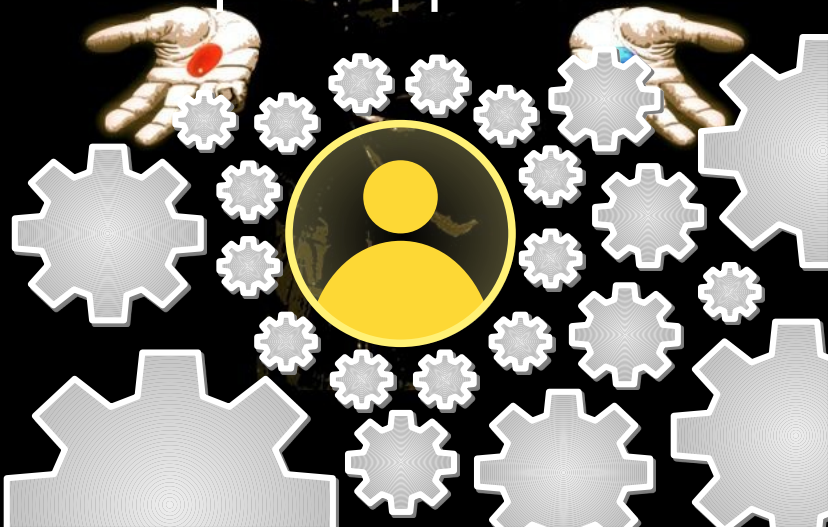
Cittadinanza Cibernetica

Viviamo in una Società Cibernetica.

Vogliamo che sia Democratica?

In una società cibernetica, la cittadinanza presuppone

- totale comprensione dei meccanismi di funzionamento degli automatismi
- partecipazione alla loro progettazione
- capacità di alterarne il funzionamento



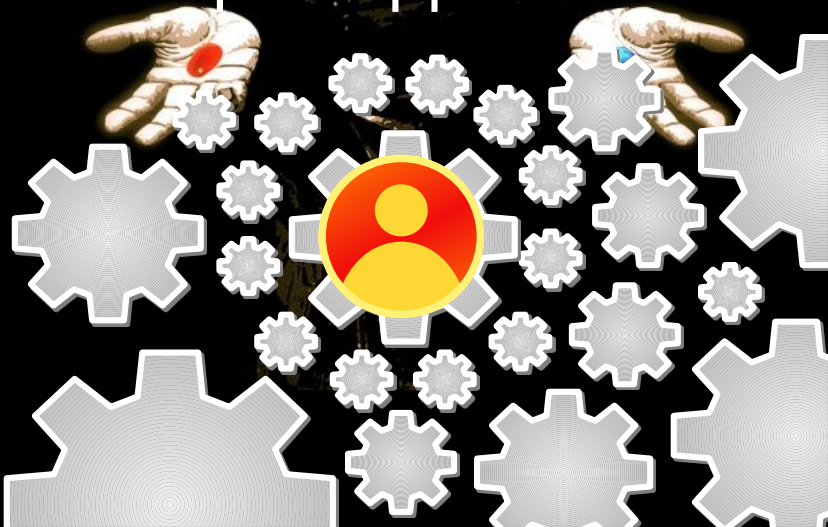
Cittadinanza Cibernetica

Viviamo in una Società Cibernetica.

Vogliamo che sia Democratica?

In una società cibernetica, la cittadinanza presuppone

- totale comprensione dei meccanismi di funzionamento degli automatismi
- partecipazione alla loro progettazione
- capacità di alterarne il funzionamento



anza Cibernetica

età Cibernetica.

mocrati

netica,

dei me

automa

oro pro

e il funz

https://c18e.it/

https://ima.circex.org/

Cittadinanza Cibernetica

Viviamo in una Società Cibernetica.
Vogliamo che sia Democratica?

Cosa può fare la CGIL?

- (in)formarsi e (in)formare
- evitare i capitalisti della sorveglianza
- dotarsi di infrastrutture autonome
- fornire servizi informatici ai lavoratori

Email, Jitsi Meet, NextCloud, PeerTube...

Cittadinanza Cibernetica

Viviamo in una Società Cibernetica.

Vogliamo che sia Democratica?

In una società cibernetica, la cittadinanza presuppone

- totale comprensione dei meccanismi di funzionamento degli automatismi
- partecipazione alla loro progettazione
- capacità di alterarne il funzionamento

Fondamenti di Cyber Security

Giacomo Tesio

http://www.tesio.it

giacomo@tesio.it