

CL  **UD DAY 2024**

improve

Milano, Nov 20

Se può andar male, lo farà: piani e strategie di disaster recovery

Serena Sensini

Enterprise Architect @ Dedalus





Non esiste un
posto sicuro al
mondo al 100%



Svalbard Global Seed Vault





**THIS IS WHY YOU
NEED**

DISASTER RECOVERY

**UN INCIDENT È DEFINITO COME UN EVENTO
O UN INSIEME DI EVENTI CHE CAUSANO
DANNI AGLI ASSET INFORMATICI O AL
PATRIMONIO INFORMATIVO DI
UN'ORGANIZZAZIONE.**

Def. «Incident»



Anche i grandi
falliscono

«Giusto se va a fuoco...»

← Post

 **Octave Klaba** 
@olesovhcom

We have a major incident on SBG2. The fire declared in the building. Firefighters were immediately on the scene but could not control the fire in SBG2. The whole site has been isolated which impacts all services in SGB1-4. We recommend to activate your Disaster Recovery Plan.

3:42 AM · Mar 10, 2021

2,022 Reposts 1,233 Quotes 4,411 Likes 185 Bookmarks

    185 

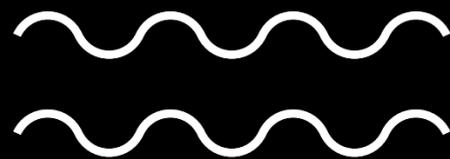
«Procedi con
l'aggiornamento,
non ci dovrebbero
essere problemi»

NEWS BREAKING

**CROWDSTRIKE
OUTAGE**

GLOBAL GLITCH

«Ma figurati se
mi rubano
l'account»

A screenshot of a mobile website interface. At the top, the 'WIRED' logo is visible, along with navigation links for 'SCIENZA' and 'ECONOMIA'. A green button with the text 'Inizia' is prominent. Below this, the article header shows the author 'GABRIELE PORRO', the category 'ECONOMIA', and the date '06.04.2021'. The main headline reads: 'Come verificare se si è tra i 533 milioni di utenti vittime dell'hacking di Facebook'. The introductory text states: 'Un set di dati personali antecedenti al 2019 è trapeato dalla piattaforma, esponendo email, numeri di telefono, nomi completi e posizioni geografiche'. An orange circle highlights the 'ECONOMIA' link in the top navigation bar.

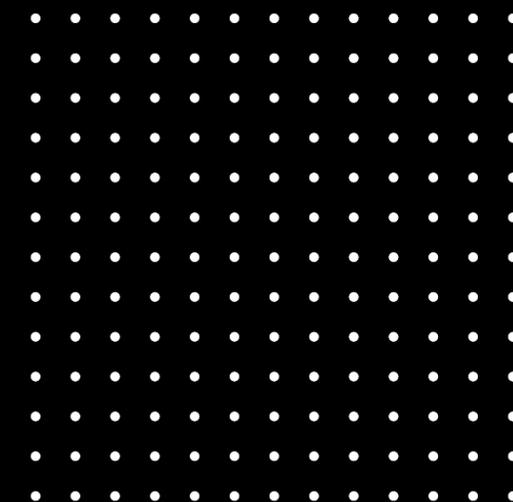
WIRED SCIENZA ECONOMIA

Inizia

GABRIELE PORRO ECONOMIA 06.04.2021

Come verificare se si è tra i 533 milioni di utenti vittime dell'hacking di Facebook

Un set di dati personali antecedenti al 2019 è trapeato dalla piattaforma, esponendo email, numeri di telefono, nomi completi e posizioni geografiche



«Tanto c'è il backup»

BS Home Latest E-Paper Markets BS at 50 Opinion Elections India News Portfolio More . . . [Subscribe](#)

Home / World News / Google Cloud accidentally deletes \$125 billion Australian pension fund Advertisement

Google Cloud accidentally deletes \$125 billion Australian pension fund

The 'unique misconfiguration' affected over half a million members who were unable to access their pension accounts for a week

Advertisement

123 notices [Manuali d'istruzione online](#) [DOWNLOAD >](#)



Latest News [view more](#)

[In this section](#) [All](#)

Gazprom stops natural gas flow to Austria on payments issue: OMV utility 

Bullet strikes Southwest Airlines plane without injuries at Dallas airport 

UN climate chief urges G20 leaders to carry out rapid cuts in emissions 

Advertisement

Esempi

- **Accesso non autorizzato**
- **Malware**
- **Data Breach**
- **Attacchi DDoS**

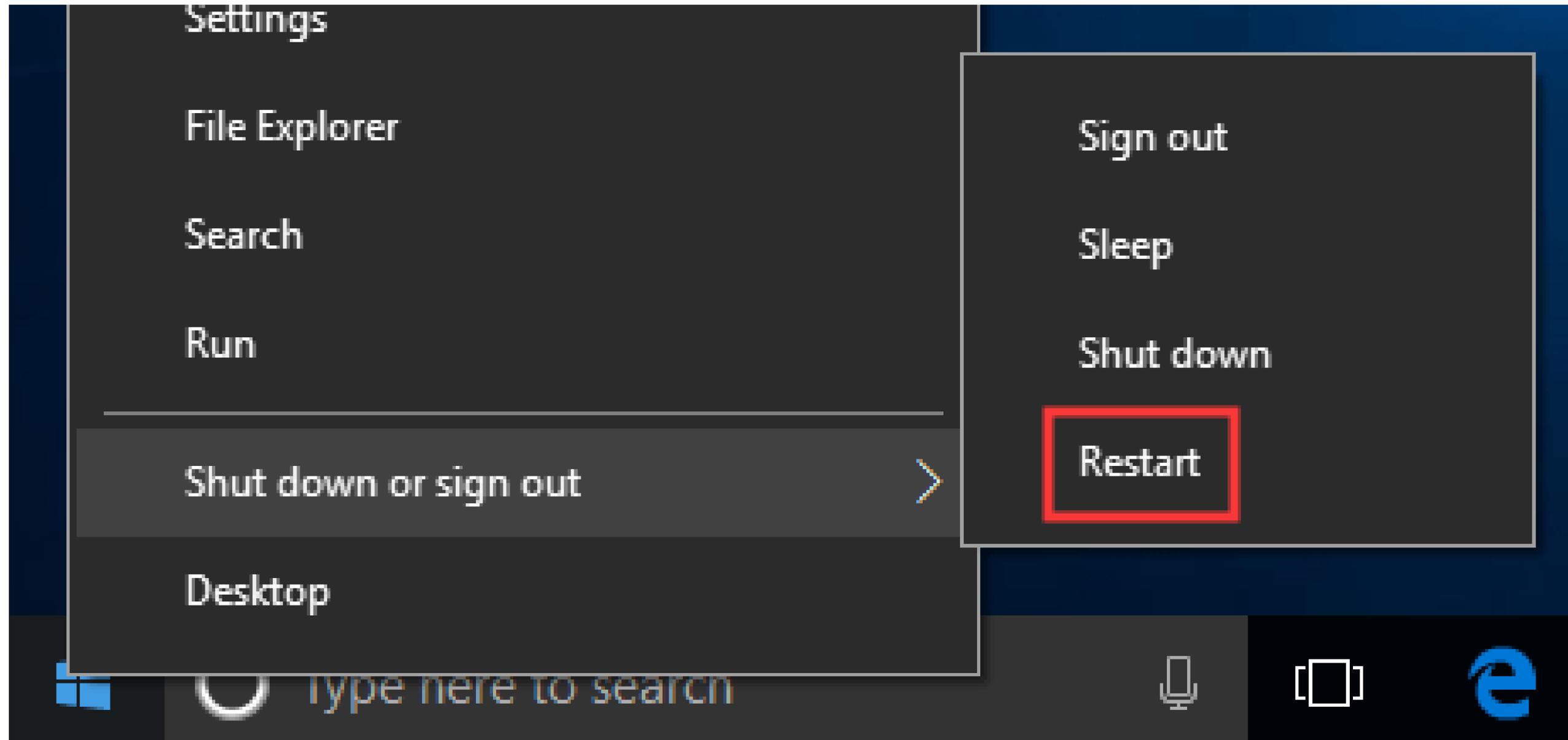
Ok, ora

*ho paura/
è successo/
voglio correre ai ripari/
[giustificazione qualsiasi]*

Che faccio?

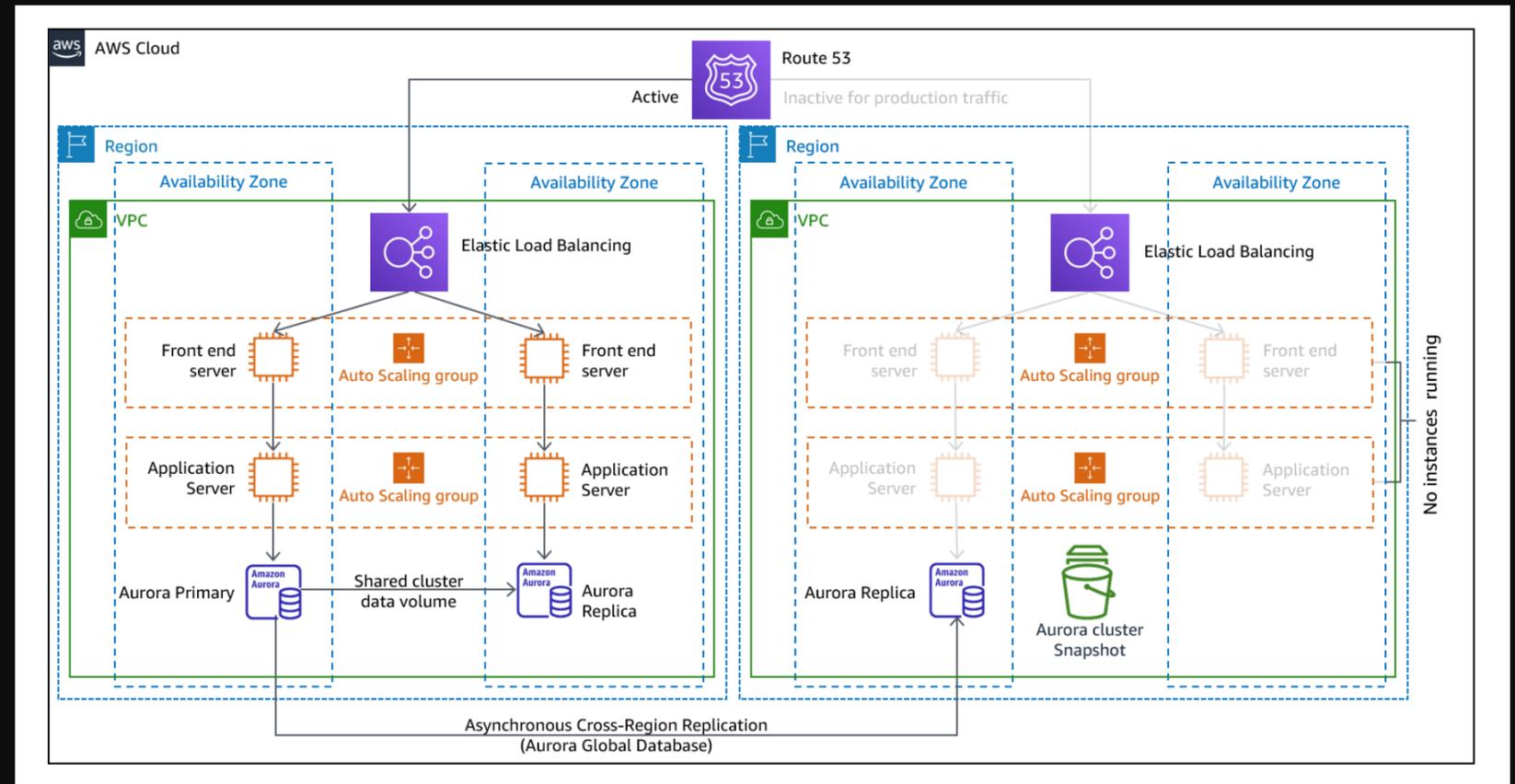
Strategie

Spegni e riaccendi



Pilot light

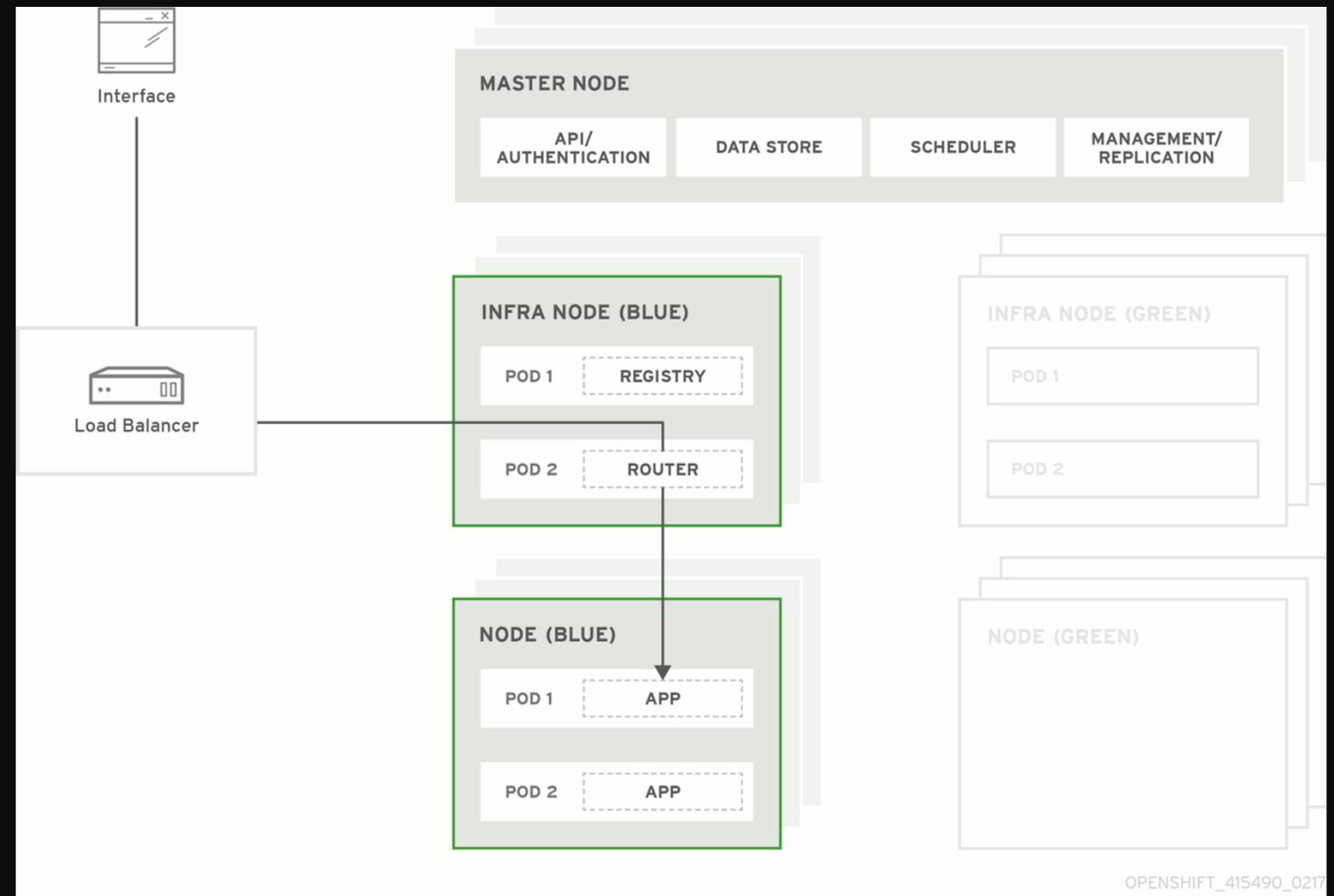
- Mantenere una versione ridotta e sempre attiva dell'infrastruttura necessaria per il ripristino dei servizi in caso di emergenze



<https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html#pilot-light>

Blue-green deployment

- Utilizzare due ambienti e impostare il nuovo ambiente quando è pronto ed è stato verificato lo stato di integrità



https://docs.openshift.com/container-platform/3.11/upgrading/blue_green_deployments.html

Documentazione

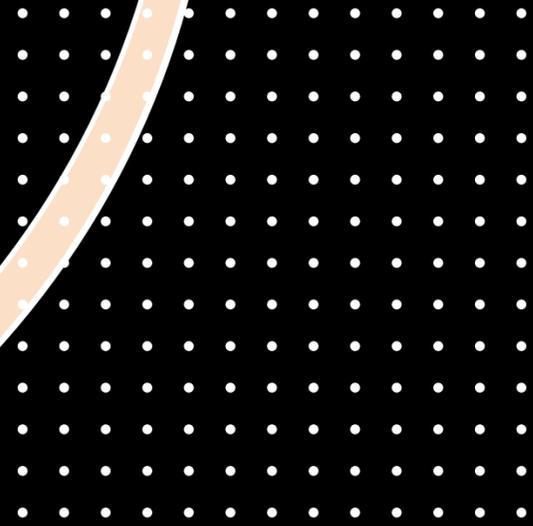
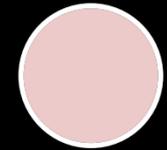


- **Risk Assessment (prima)**
 - scoprire e identificare quali sono i threats potrebbero verificarsi e come mitigarli o minimizzarne l'impatto.
- **Business continuity plan (prima)**
 - assicura che le funzioni critiche rimangano in esecuzione anche durante un disaster
- **Business Impact Analysis (prima)**
 - Descrive le conseguenze di eventuali incident che potrebbero verificarsi e quali processi prioritizzare
- **Incident report (dopo)**
 - Un rapporto sugli incidenti IT è un documento formale che descrive in dettaglio un'interruzione o una potenziale interruzione dei sistemi IT.

**AH, LA
DOCUMENTAZIONE,
QUESTA
SCONOSCIUTA...**



https://www.linkedin.com/posts/serena-sensini_ah-la-documentazione-questa-sconosciuta-activity-7165249904649474048-U8_X



Obiettivi di recovery chiari

- Definire un'analisi dell'impatto aziendale (BIA)
- Identificare i requisiti normativi e legali
- Valutare le capacità operative
- Aggiornare gli obiettivi regolarmente
- Definire RTO e RPO

Metrische

- Recovery Time Objective (RTO)
 - Recovery Point Objective (RPO)
-

Ogni metrica «dipende» dal contesto

Due scenari diversi, ma uguali

- **Contesto:** un'azienda di vendita al dettaglio online fa molto affidamento sul suo sito Web per le vendite e le interazioni con i clienti.
 - **RTO:** l'azienda imposta un RTO di 1 ora. Ciò significa che in caso di guasto del sistema, deve ripristinare il sito Web entro un'ora per evitare perdite significative di fatturato e insoddisfazione dei clienti.
 - **RPO:** l'RPO è impostato su 30 minuti. Ciò indica che l'azienda può tollerare la perdita di dati sulle transazioni pari a 30 minuti. Pertanto, esegue backup ogni 30 minuti per garantire una perdita minima di dati.
- **Contesto:** un'organizzazione sanitaria gestisce cartelle cliniche e sistemi medici critici che richiedono elevata disponibilità.
 - **RTO:** il fornitore di servizi sanitari stabilisce un RTO di 2 ore. Ciò significa che qualsiasi periodo di inattività per i sistemi critici deve essere risolto entro due ore per garantire che l'assistenza ai pazienti non venga compromessa e che venga mantenuta la conformità normativa.
 - **RPO:** l'RPO è impostato su 15 minuti. Ciò indica che l'organizzazione può permettersi di perdere solo fino a 15 minuti di dati dei pazienti. Di conseguenza, implementano la replica dei dati in tempo reale per garantire che i backup siano il più aggiornati possibile.

Testing regolare

- Controlli regolari e testing sulle applicazioni permettono di prevenire, anziché curare
- È possibile identificare e mitigare le vulnerabilità, in linea con le migliori pratiche di test continui e aggiornamenti dei piani di disaster recovery



Piani di comunicazione efficaci

(e non)

email addresses of all Okta customer support system users.)

Okta pointed out to The Stack that the attacker began targeting Cloudflare's systems "almost a month after Okta shared guidance to customers to rotate credentials on October 19 when "we notified customers, shared guidance to rotate credentials, and provided indicators of compromise (IoCs) related to the October security incident. We can't comment on our customers' security remediations."

It was not immediately clear why Cloudflare had "mistakenly believed" the tokens in question were unused, as it admitted.

See also: [Not HAR HAR as Okta breach escalates](#)

Cloudflare said it embarked on a huge security hygiene overhaul after the incident, even returning hardware to manufacturers when the attackers tried (unsuccessfully) to "access a console server in our new, and not yet in production, data center in São Paulo... The immediate "Code Red" effort ended on January 5, but work continues across the company around credential management, software hardening, vulnerability management, additional alerting, and more" its leadership concluded.

"A large part of our "Code Red" effort was understanding what the threat

 Subscribe

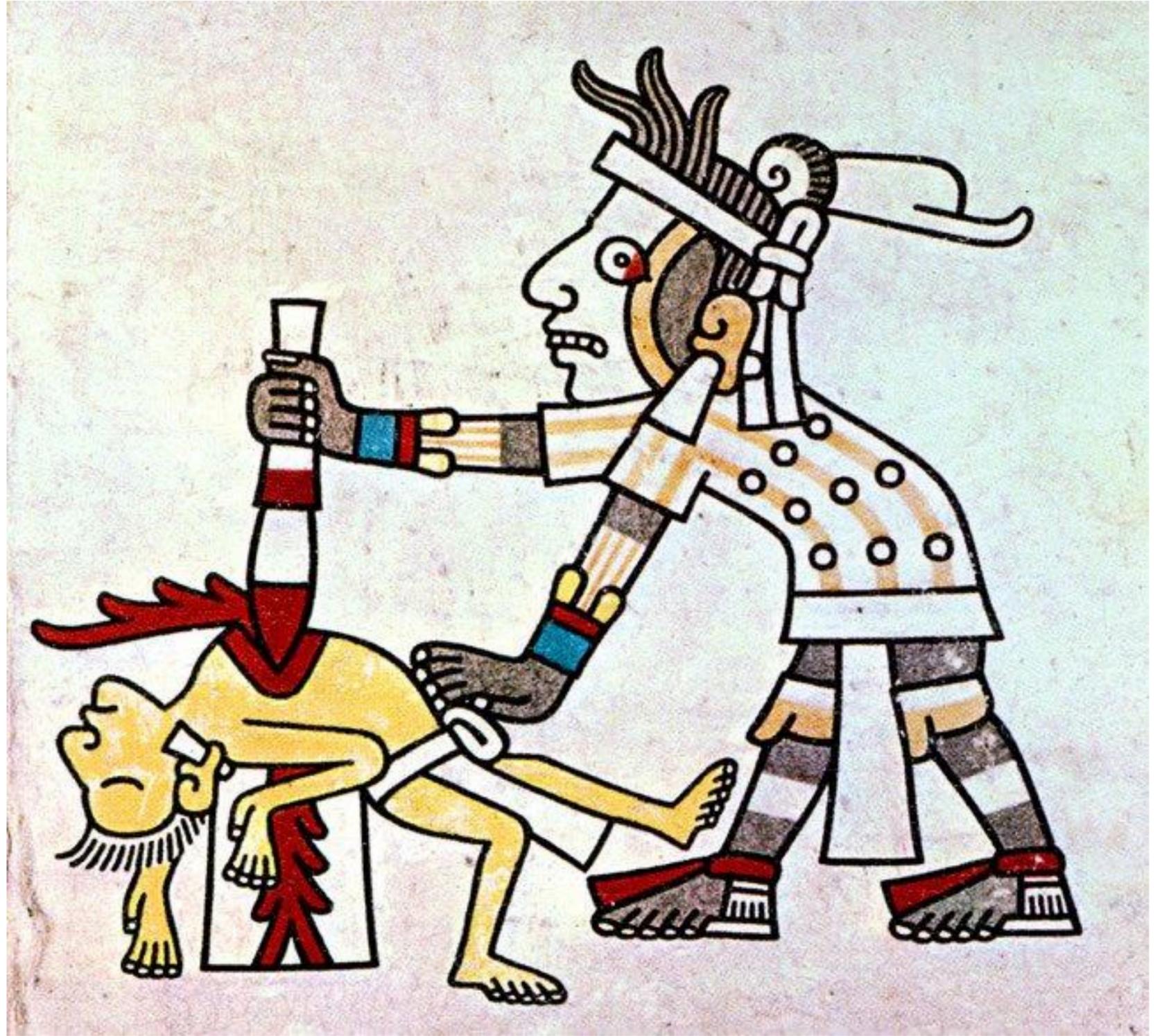
Backup dei dati

- Tipologie
 - Off-site
 - On-site
 - Cloud-based or hybrid
- Esempi
 - Commvault Cloud
 - Veeam Data Platform
 - AWS, Azure e Google Cloud Backup

Training

- Formazione continua
- Esercitazioni regolari
- Responsabilizzazione

Trovare i
responsabili e
sacrificarli



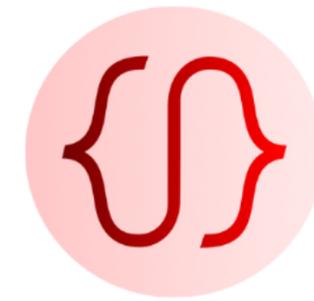
Cassetta degli attrezzi

- **Risk Assessment e Business Continuity Plan**
- **Obiettivi di Recovery strategici**
- **Strategie di Backup**
- **Testing Regolare**
- **Piani di comunicazione mirati**
- **Formazione continua**

Ego slide

Serena Sensini

Enterprise Architect @ Dedalus spa
Founder @ TheRedCode.it
Author of 5 tech books



theRedCode



Il mondo #tech a piccoli #bit

Kudos

CL[▶]UD DAY 2024

improve

Milano, Nov 20



Thanks!



Il mondo #tech a piccoli #bit

CL  UD DAY 2024

improve 

Milano, Nov 20