WORKSHOP GARR 2026

NET MAKERS

NIS2

Dalla conformità alla sicurezza dimostrabile

La norma come occasione per cambiare ciò che conta:

responsabilità, dipendenze e capacità di risposta

Gianluca Mazzini

Università di Ferrara

Non «fare NIS2». Usare la NIS2.

Il vincolo normativo può finalmente mettere in moto decisioni rimaste in sospeso.

01 / VINCOLO

Dover rendere conto di rischi e continuità

→

02 / SCELTA

Decidere priorità, responsabilità e risorse

→

03 / CAPACITÀ

Saper prevenire, reagire e ripartire

L'adempimento è il punto di partenza. La capacità operativa è il risultato.

Un servizio è una rete di dipendenze

La disponibilità per l'utente dipende da elementi tecnici, organizzativi e umani.



Ciò che non conosciamo non possiamo governarlo, proteggerlo né ripristinarlo.

Dalla carta alle scelte

Politiche e piani sono necessari. Il loro valore si misura nelle azioni che producono.

DOCUMENTO	DECISIONE O PROVA
Politica di sicurezza	Obiettivi, responsabilità e priorità chiare
Piano di gestione dei rischi	Rischi accettati, risorse e tempi decisi
Piano di continuità	Ripristino realmente provato sul campo

Un documento è utile quando rende possibile una decisione o una verifica.

Il rischio residuo è una decisione

La responsabilità di accettare un rischio non può essere delegata a un allegato.

01

CHI ANALIZZA

Rileva minacce e vulnerabilità; misura e propone

02

CHI DIRIGE

Integra impatti e alternative; coordina interventi e risorse

03

CHI GOVERNA

Approva priorità e trattamento; assume il rischio residuo

REVISIONE INDIPENDENTE Rende più comprensibili rischi, limiti ed evidenze: aiuta a decidere.

Responsabilità distinte, decisioni esplicite e tracciabili.

Il ripristino è una sequenza, non una lista

L'ordine dipende dai prerequisiti tecnici e dallo scenario, non solo dalla visibilità del guasto.

CONNETTIVITÀ
raggiungere

→

IDENTITÀ / DNS
accedere

→

PIATTAFORME
eseguire

→

SERVIZI
erogare

Sequenza esemplificativa: le dipendenze cambiano secondo l'incidente.

PER RENDERE IL RIPRISTINO REALE

OBIETTIVI
RTO / RPO coerenti
con i servizi critici

ISTRUZIONI
Runbook, reperibili
e sostituti

EVIDENZE
Prove di failover, backup
e tempi misurati

24/7

non è una casella di posta elettronica.

Un presidio esiste solo se qualcuno riceve, valuta, decide e interviene.

- PERSONE
- SOSTITUTI
- ESCALATION
- AUTORITÀ
- RISORSE

La continuità è una scelta organizzativa da finanziare e verificare.

Due prospettive, una sola realtà

La disponibilità dei singoli componenti non garantisce il funzionamento del servizio.

COMPONENTI

CPU · rete · storage · processi

TUTTO APPARENTEMENTE VERDE

SERVIZIO EROGATO

Accesso · risposta · disponibilità

L'UTENTE VEDE L'INTERRUZIONE

Misurare l'esperienza dell'utente rende visibili i problemi trasversali.

Controllo indipendente ≠ sfiducia

Un controllo utile rende leggibili le criticità e migliora la qualità delle decisioni.

01 OPERARE

Raccogliere dati
e conoscere i dettagli

→

02 VERIFICARE

Mettere alla prova
coerenza, piani e risultati

→

03 GOVERNARE

Scegliere priorità
con rischi più chiari

Una buona revisione non aggiunge un timbro: migliora una decisione.

La difesa isolata parte svantaggiata.

Chi attacca può riutilizzare strumenti. Chi difende deve costruire, presidiare e aggiornare.

SEGNALI

Condividere allarmi e indicatori per riconoscere prima

COMPETENZE

Unire analisi e capacità di risposta agli incidenti

LEZIONI

Diffondere errori e soluzioni per non ripeterli

La cooperazione non è un accessorio: è parte della capacità di difesa.

Un incidente deve lasciare conoscenza

La risposta non termina al ripristino: si chiude quando correggiamo e riproviamo.



Test, esercitazioni e lezioni apprese non sono la coda del processo: sono il processo.

Quattro impegni che lasciano un segno

Poche priorità operative, ciascuna sostenuta da responsabilità, risorse e prove.

01 CONOSCERE

Mappare servizi critici, dipendenze e punti unici di fragilità.

02 DECIDERE

Dare un proprietario a rischi residui, priorità e risorse.

03 PROVARE

Esercitare escalation, ripristini, continuità e comunicazione.

04 CONDIVIDERE

Mettere in comune segnali, competenze e lezioni apprese.

Per ciascuno: un responsabile, una scadenza e una prova.

Fra dodici mesi, che cosa sapremo dimostrare?

La differenza tra conformità e miglioramento si vede nelle risposte verificabili.

1. **Quali servizi critici sappiamo ripristinare, e da cosa dipendono?**
2. **Chi decide, e in quanto tempo, quando un servizio si interrompe?**
3. **Quale ripristino abbiamo provato davvero, con tempi misurati?**
4. **Che cosa abbiamo cambiato dopo un test o un incidente?**

Non serve moltiplicare gli indicatori: servono risposte affidabili.

WORKSHOP GARR 2026

NET MAKERS

La NIS2 sarà utile se, dopo la NIS2, saremo diversi.

Più conoscenza, decisioni, prove e cooperazione.
Meno sicurezza dichiarata. Più sicurezza dimostrabile.

Gianluca Mazzini · Workshop GARR 2026