GUIDA PRATICA · EDIZIONE 2026

PA CENTRALE · ENTI LOCALI · SANITÀ

LIVELLO 1 → 5

Pronti a ripartire.

I cinque livelli della cyber resilience nella Pubblica Amministrazione: come riconoscere il vostro e come salire al successivo.

Per vertici, dirigenti, responsabili IT, CISO e RTD della Pubblica Amministrazione

HTDI | Commvault

PROLOGO · UNO SCENARIO, DUE FINALI

Stesso attacco.

Due enti, due storie.

Lunedì, ore 06:40. Due enti pubblici delle stesse dimensioni vengono colpiti dallo stesso ransomware, entrato con la stessa credenziale rubata.

ENTE A

06:40
I file server iniziano a cifrarsi. Nessuno se ne accorge.

08:00
Sportelli fermi. Si prova a ripartire: **anche le copie di sicurezza sono cifrate**, stavano sulla stessa rete.

Giorno 3
Si ricostruisce da zero. Nessuno sa quale servizio riaprire per primo.

Settimana 3
Servizi ancora parziali. La notifica all'ACN è fatta di stime.

ENTE B

06:52
Un allarme segnala cifrature anomale sui dati. Il reperibile isola i sistemi.

08:00
Sportelli in modalità ridotta. **Le copie isolate sono intatte** e verificate.

Ore 14:00
Identità e anagrafe ripartono in un ambiente pulito, nell'ordine deciso mesi prima.

Giorno 2
Servizi essenziali attivi. Notifica completa con dati reali, non stime.

> La differenza non l'hanno fatta il budget o la fortuna. L'ha fatta il livello di maturità a cui erano arrivati **prima** dell'attacco.

Scenario illustrativo, costruito su dinamiche ricorrenti negli incidenti alla PA.

PERCHÉ ORA

Gli attacchi puntano alla capacità di ripartire.

1.140

eventi cyber contro la Pubblica Amministrazione nel 2025. Erano 756 un anno prima: **+51%**.

ACN, Relazione annuale 2025

99%

degli attacchi a enti governativi e locali ha provato a colpire anche le copie di sicurezza.

Sophos, 2024

8×

più alti i costi di ripartenza quando le copie vengono compromesse.

Sophos, 2024

53%

è tornato pienamente operativo entro una settimana. Gli altri no.

Sophos, State of Ransomware 2025

> Non basta più proteggere i dati. Conta se l'ente **resiste all'attacco, riparte pulito e sa dimostrarlo**.

CAPITOLO 1 · IL CONCETTO

Che cos'è davvero la cyber resilience.

È la capacità di un'organizzazione di **anticipare, resistere, ripristinare e adattarsi** di fronte ad attacchi e compromissioni dei propri sistemi (NIST SP 800-160 Vol. 2). In una frase: continuare a servire i cittadini anche nel giorno peggiore.

1

Anticipare

Sapere cosa è critico, dove sono i dati, chi decide. Prima che serva.

2

Resistere

Copie che un attaccante non può cancellare. Allarmi che scattano presto.

3

Ripristinare

Ripartire da copie pulite, nell'ordine giusto, in tempi misurati.

4

Adattarsi

Imparare da ogni test e da ogni incidente. E dimostrarlo.

IERI · PROTEZIONE DEI DATI

«Abbiamo una copia dei dati?»

→

OGGI · CYBER RESILIENCE

«Quanto ci mettiamo a riaprire i servizi, e possiamo dimostrarlo?»

La legge non la chiama così. Ma la chiede.

NIS2 e ACN parlano di cybersicurezza. Dentro, però, ci sono proprio i mattoni della resilienza.

Direttiva NIS2, art. 21

Tra le misure minime: **continuità operativa, gestione del backup, disaster recovery e gestione delle crisi.**

Direttiva NIS2, art. 23

Incidenti significativi: **preallarme entro 24 ore, notifica entro 72, relazione finale entro un mese.** In Italia dal 15 gennaio 2026.

D.Lgs. 138/2024 e Determinazione ACN 379907/2025

Le misure di base, entro ottobre 2026: **116 requisiti** per i soggetti essenziali, **87** per gli importanti. Poi partono le verifiche.

Responsabilità dei vertici

Gli organi di amministrazione **approvano le misure, ne seguono l'attuazione, si formano e rispondono** delle violazioni.

Da non confondere. Il *Cyber Resilience Act* (Reg. UE 2024/2847) riguarda la sicurezza dei prodotti digitali immessi sul mercato, non gli obblighi degli enti. Per la PA il riferimento è la NIS2.

Cinque livelli, cinque domande.

Ogni livello risponde a una domanda che un vertice può fare al proprio responsabile IT. Si sale un gradino alla volta: saltarne uno lascia un buco.

1 **Protetti sulla carta**
Abbiamo una copia dei dati?

2 **Copie inattaccabili**
La copia sopravvive a un attacco?

3 **Ripartenza misurata**
In quanto tempo riapriamo, e in che ordine?

4 **Ripartenza pulita**
Siamo sicuri di non reintrodurre il malware?

5 **Resilienza dimostrata**
Possiamo provarlo a un'ispezione ACN?

Nelle prossime pagine, per ogni livello: la frase che si sente dire, come riconoscerlo, il rischio e le tre azioni per salire.

1 Protetti sulla carta.

Il punto di partenza di molti enti.

> *«Le copie le facciamo tutte le notti.»*

COME LO RICONOSCETE

- Le copie finiscono su uno storage nella stessa rete dei sistemi.
- La console che gestisce le copie usa le credenziali di dominio.
- Nessuno ricorda quando è stato fatto l'ultimo ripristino completo.

IL RISCHIO

- Chi entra nel dominio arriva anche alle copie, e le cifra per prime.
- Posta, Teams e SharePoint spesso restano fuori dal perimetro.

PER SALIRE AL LIVELLO 2

1. Separare le credenziali della console delle copie e attivare l'MFA.
2. Creare almeno una copia immutabile, che nessuno possa modificare o cancellare.
3. Fare l'inventario: quali dati, quali servizi, Microsoft 365 e identità inclusi.

La domanda da portare al vertice: **«Se domani entrassero nel dominio, potrebbero cancellare anche le nostre copie?»**

2 Copie inattaccabili.

Le copie sopravvivono. Ma nessuno sa quanto ci vuole a ripartire.

> ***«Anche se ci attaccano, le copie non le toccano.»***

COME LO RICONOSCETE

- Almeno una copia è immutabile e isolata dalla rete di produzione.
- Si segue la regola 3-2-1-1-0: tre copie, due supporti, una fuori sede, una immutabile, zero errori.
- Accesso alla console protetto da MFA e ruoli separati.

IL RISCHIO

- Le copie ci sono, ma i tempi di ripristino sono una stima mai verificata.
- Si scopre durante la crisi che Active Directory non riparte, e senza identità non riparte nulla.

PER SALIRE AL LIVELLO 3

1. Definire con la dirigenza i servizi critici e i tempi massimi di fermo accettabili.
2. Fare il primo test di ripristino completo di un servizio critico, cronometrato.
3. Proteggere Active Directory ed Entra ID con copie e ripristino dedicati.

La domanda da portare al vertice: **«Quanto ci mettiamo a riaprire l'anagrafe? L'abbiamo mai provato?»**

3 Ripartenza misurata.

La resilienza diventa misurabile.

> ***«Sappiamo quanto ci vuole a riaprire l'anagrafe: l'abbiamo provato.»***

COME LO RICONOSCETE

- Test di ripristino almeno due volte l'anno sui servizi critici, con tempi misurati.
- Un ordine di ripristino dei servizi approvato dalla dirigenza.
- Le identità si possono ripristinare in modo granulare o per intero.

IL RISCHIO

- Gli attaccanti restano nella rete per settimane prima di colpire: le copie recenti possono essere già infette.
- Ripristinare in fretta sopra la produzione significa farsi cifrare una seconda volta.

PER SALIRE AL LIVELLO 4

1. Attivare il rilevamento delle anomalie sui dati protetti (cifrature, cancellazioni massive).
2. Controllare che le copie non contengano malware prima di usarle.
3. Predisporre un ambiente isolato (clean room) dove verificare e riaccendere i sistemi.

> La domanda da portare al vertice: **«Se ripristiniamo la copia di ieri, siamo sicuri che sia pulita?»**

4 Ripartenza pulita.

La tecnica è matura. Manca il governo.

> ***«Sappiamo quale copia è pulita, e ripartiamo in un ambiente isolato.»***

COME LO RICONOSCETE

- Allarmi automatici su comportamenti anomali nei dati, anche fuori orario.
- Ripristino in clean room e disaster recovery orchestrato nell'ordine dei servizi.
- Cloud, SaaS e Microsoft 365 protetti come i server, nella stessa console.

IL RISCHIO

- Tutto dipende da una o due persone dell'IT: se non ci sono, il piano si ferma.
- I vertici non sono coinvolti e i test non sono documentati: per l'ACN è come se non esistessero.

PER SALIRE AL LIVELLO 5

1. Far approvare le misure di resilienza dagli organi di amministrazione.
2. Organizzare un'esercitazione congiunta IT e dirigenza su uno scenario realistico.
3. Documentare ogni test in un formato pronto per un'ispezione.

La domanda da portare al vertice: **«Se il responsabile IT fosse in ferie il giorno dell'attacco, sapremmo cosa fare?»**

5 Resilienza dimostrata.

La resilienza è un processo, non un progetto.

> ***«Ecco l'ultimo test di ripristino: firmato, con i tempi e le correzioni.»***

COME LO RICONOSCETE

- Gli organi di amministrazione approvano le misure e si formano ogni anno.
- Esercitazioni periodiche con dirigenza, IT, comunicazione e fornitori critici.
- Report dei test pronti da mostrare all'ACN, con tempi reali confrontati con gli obiettivi.

IL RISCHIO

- Fermarsi: l'infrastruttura cambia, i test invecchiano, il livello scende senza che nessuno se ne accorga.

PER RESTARE AL LIVELLO 5

1. Ripetere i test dopo ogni cambiamento importante dell'infrastruttura.
2. Portare al vertice pochi indicatori: tempi di ripristino misurati contro obiettivo, test fatti, criticità aperte.
3. Includere i fornitori critici nei test e nei contratti.

La domanda da portare al vertice: **«Qual è stato il nostro tempo di ripristino all'ultimo test, e cosa abbiamo corretto?»**

CAPITOLO 4 · TRE REALTÀ

Da dove partire,

ente per ente.

01 PA centrale

Ministeri, agenzie, autorità indipendenti

Il nodo sono **le identità**: un dominio violato apre tutto. Priorità a protezione e ripristino dedicati di Active Directory ed Entra ID, una sola piattaforma per on-premise, cloud e Microsoft 365, e test documentati per i 116 requisiti.

02 Regioni, città metropolitane, comuni

Team IT piccoli, molti fornitori esterni

Il nodo è **la semplicità**: copie immutabili, una console che due persone possano governare, e un ordine di ripristino deciso in giunta prima dell'emergenza. Anagrafe, tributi, protocollo, SUAP.

03 Sanità

Aziende sanitarie e strutture collegate

Il nodo è **il tempo**: qui il fermo si misura in pazienti. Tempi di ripristino misurati per pronto soccorso, CUP, laboratori e referti, e ripartenza in clean room per non reinfettare i sistemi clinici.

> Qualunque sia l'ente, il primo passo è lo stesso: **sapere a che livello siete oggi.**

CAPITOLO 5 · AUTOVALUTAZIONE

A che livello siete?

10 domande, 5 minuti.

LIV.	DOMANDA	SÌ	NO
L1	Facciamo copie regolari di tutti i dati e servizi critici, Microsoft 365 incluso?	☐	☐
L1	Sappiamo dove sono le copie e chi può accedervi?	☐	☐
L2	Abbiamo almeno una copia immutabile e isolata dalla rete di produzione?	☐	☐
L2	La console delle copie ha credenziali separate dal dominio e MFA?	☐	☐
L3	Abbiamo fatto un ripristino completo di un servizio critico negli ultimi sei mesi, cronometrato?	☐	☐
L3	Esiste un ordine di ripristino dei servizi approvato dalla dirigenza?	☐	☐
L4	Riceviamo un allarme se i dati iniziano a essere cifrati o cancellati in modo anomalo?	☐	☐
L4	Possiamo ripartire in un ambiente isolato da copie verificate senza malware?	☐	☐
L5	Le misure sono approvate dagli organi di amministrazione, che si sono formati nell'ultimo anno?	☐	☐
L5	I test di ripristino sono documentati e pronti da mostrare in un'ispezione ACN?	☐	☐

Come leggere il risultato. Partite dal livello 1 e salite: il vostro livello è **l'ultimo in cui avete risposto sì a entrambe le domande**. Un no al livello 2 vi lascia al livello 1, anche con tutti sì al livello 4. È il gradino mancante a fermarvi durante un attacco.

CAPITOLO 6 · IL PIANO

Un livello in più

in 90 giorni.

Salire di un gradino non richiede un progetto di anni. Richiede tre mesi, poche decisioni chiare e una persona che ne risponda.

GIORNI 1 – 30

Fotografare

- Autovalutazione con IT e dirigenza.
- Inventario di servizi critici, dati e dipendenze.
- Credenziali separate e MFA sulla console delle copie: si fa in giorni, non mesi.

RISULTATO

Sapete a che livello siete e cosa manca.

GIORNI 31 – 60

Proteggere e provare

- Almeno una copia immutabile e isolata.
- Protezione dedicata delle identità.
- Primo test di ripristino di un servizio critico, cronometrato.

RISULTATO

Le copie sopravvivono a un attacco e conoscete un tempo reale.

GIORNI 61 – 90

Decidere e documentare

- Ordine di ripristino approvato dal vertice.
- Report del test in formato ispezione.
- Obiettivo e data per il livello successivo.

RISULTATO

Un livello in più, documentato e approvato.

CHI COINVOLGERE

Vertice o direzione generale · Responsabile IT o CISO · RTD · DPO · Fornitori critici

CAPITOLO 7 · GLI STRUMENTI

Una piattaforma di cyber resilience, in convenzione.

2	**Dati e identità inattaccabili**: copie immutabili e isolate per on-premise, cloud, Microsoft 365, Active Directory ed Entra ID.
3	**Recovery orchestrato**: i servizi ripartono nell'ordine deciso, in tempi misurati, anche su larga scala.
4	**Rilevamento delle minacce e Cleanroom Recovery**: individuare le anomalie e ripartire in un ambiente isolato e verificato.
5	**Resilienza misurabile**: test di recovery ripetibili e report pronti per le verifiche ACN.

Commvault Cloud copre i livelli dal 2 al 5 in un'unica piattaforma. Il livello 1 è il punto da cui si parte.

CONVENZIONE CONSIP

ID 2955 · Lotto 4

Prodotti Commvault, rinnovo della manutenzione per le licenze in uso e servizi connessi. Acquistabili con ordinativo diretto su Acquisti in Rete della PA, **senza una gara propria**.

Fornitore aggiudicatario: **HTDI** · supporto tecnico Commvault

IL PROSSIMO PASSO

Il vostro livello, in 30 minuti.

Un mini audit gratuito con gli specialisti HTDI: rivediamo insieme l'autovalutazione, i tempi di ripristino reali e il piano per salire al livello successivo, in vista delle verifiche ACN.

MINI AUDIT · 30 MINUTI

lotto4.htdi.it

commvault26_lotto4@htdi.it

WEBINAR · MARTEDÌ 20 OTTOBRE, 11:00

Il backup c'è. E il ripristino?

Online e gratuito, con gli specialisti di HTDI e Commvault

Fonti. ACN, Relazione annuale al Parlamento 2025 · Sophos, The impact of compromised backups on ransomware outcomes (2024) · Sophos, State of Ransomware 2025 · NIST SP 800-160 Vol. 2 Rev. 1 · Direttiva (UE) 2022/2555 (NIS2), artt. 21 e 23 · D.Lgs. 138/2024 · Determinazione ACN n. 379907/2025 · Regolamento (UE) 2024/2847. Dati aggiornati a settembre 2026. Questa guida ha scopo informativo e non costituisce consulenza legale.