GUIDA PRATICA · EDIZIONE 2026

PA CENTRALE · ENTI LOCALI · SANITÀ

72:00:00

Le prime 72 ore

Cosa succede davvero dopo un attacco informatico a un ente pubblico, cosa chiedono NIS2 e ACN, e come tornare operativi senza pagare riscatti.

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

HTDI | Commvault

UNO SCENARIO CHE L'ACN VEDE OGNI SETTIMANA

Martedì, ore 03:12.

03:12 Il sistema di monitoraggio segnala cifrature anomale sul file server. Nessuno è in servizio.

07:40 Gli sportelli aprono. **Anagrafe, protocollo e pagamenti non rispondono.** La PEC è ferma.

08:15 Sui monitor compare una richiesta di riscatto. I dati dei cittadini sono stati copiati prima di essere cifrati.

09:30 Il responsabile IT prova a ripristinare. **Anche le copie di sicurezza sono state cifrate:** stavano sulla stessa rete, con le stesse credenziali.

03:12
+24h

Scade il termine per il preallarme al CSIRT Italia. La domanda non è più tecnica: **chi firma, cosa si dichiara, quando si riapre?**

> Questa guida parte da qui. Da quello che succede nelle ore in cui ogni decisione conta.

NON È UNA QUESTIONE DI "SE"

La PA italiana è diventata il bersaglio principale.

1.140

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

ACN, Relazione annuale 2025

28%

degli incidenti gravi in Italia colpisce governo e PA: il primo settore.

Rapporto Clusit 2026

84%

degli incidenti in Italia ha impatto alto o critico.

Rapporto Clusit 2026

94%

delle organizzazioni colpite da ransomware ha visto attaccare anche le copie di sicurezza.

Sophos, State of Ransomware 2024

> Gli attaccanti lo sanno: **se colpiscono le copie, colpiscono la capacità di ripartire.** Per questo non basta ripristinare: bisogna prepararsi a ripartire.

COSA TROVI NELLE PROSSIME PAGINE

Una guida da tenere sulla scrivania, non in archivio.

05 **Ripristinare non basta**
I quattro tempi della cyber resilience, spiegati per chi deve decidere.

06 **NIS2 e ACN, senza giuridichese**
Chi è dentro, le scadenze, cosa verifica l'Agenzia dopo il 31 ottobre 2026.

08 **Le prime 72 ore, ora per ora**
La sequenza che separa un incidente da un fermo di settimane.

10 **Tre capitoli, tre realtà**
PA centrale, comuni e regioni, aziende sanitarie: rischi e priorità di ognuno.

13 **I sei mattoni della cyber resilience**
Dalla copia dei dati al ripristino pulito: cosa serve davvero per ripartire.

14 **Un ripristino mai testato è un'ipotesi**
Il test di ripristino in quattro passi, da mettere per iscritto.

15 **La checklist in 20 domande**
In dieci minuti sapete quanto siete pronti. Con il punteggio.

CHECKLIST DI AUTOVALUTAZIONE · ANTEPRIMA

01 Abbiamo almeno una copia dei dati non modificabile e isolata dalla rete di produzione?

02 Abbiamo provato un ripristino completo negli ultimi sei mesi?

03 [illegible]

🔒 **Sblocca la guida completa · 15 pagine**

Ripristinare non basta.

Una copia dei dati risponde a una sola domanda: *posso recuperarli?* La cyber resilience ne pone quattro, e un ente deve saper rispondere a tutte. Non limitarsi a ripristinare: prepararsi a ripartire.

1

Prevenire

Ridurre la superficie d'attacco: patch, accessi, identità protette, copie immutabili.

2

Resistere

Accorgersi presto. Rilevare cifrature e comportamenti anomali prima che si propaghino.

3

Rispondere

Isolare, capire cosa è stato colpito, notificare nei tempi. Con ruoli già decisi.

4

Ripristinare

Tornare operativi da copie pulite e verificate, nell'ordine giusto, senza reintrodurre il malware.

> *L'obiettivo non è recuperare i dati persi. È continuare a erogare i servizi essenziali anche durante la crisi, e tornare rapidamente alla piena operatività.*

NIS2 e ACN: chi è dentro.

Il D.Lgs. 138/2024 recepisce la direttiva NIS2. Per la Pubblica Amministrazione il perimetro è ampio e, per molti enti, automatico.

Amministrazioni centrali
Ministeri, agenzie, autorità indipendenti

Regioni e Province autonome
Incluse le loro amministrazioni

Enti locali
Città metropolitane, comuni sopra 100.000 abitanti, capoluoghi di regione

Sanità
Aziende sanitarie locali

Altri soggetti pubblici
Enti di ricerca, istituti zooprofilattici, enti di regolazione

Su designazione ACN
Società in house, partecipate, TPL, istituti con attività di ricerca

Responsabilità in capo ai vertici. Gli organi di amministrazione approvano le misure, ne sovrintendono l'attuazione, seguono una formazione specifica e rispondono delle violazioni (art. 23).

Il calendario che conta.

15 gen 2026

Obbligo di notifica degli incidenti

Preallarme al CSIRT Italia entro 24 ore, notifica entro 72, relazione finale entro un mese.

31 ott 2026

Misure di sicurezza di base

Vanno adottate dai soggetti inseriti nell'elenco NIS 2025. Da qui l'ACN avvia la fase di verifica e ispezione.

Sempre

Aggiornamento e revisione

Dati sulla piattaforma ACN entro 14 giorni da ogni variazione, revisione periodica dell'efficacia delle misure, formazione continua.

116
requisiti per i soggetti essenziali

87
requisiti per i soggetti importanti

Determinazione ACN n. 379907/2025. Tra gli ambiti: gestione degli incidenti, **continuità operativa e disaster recovery**, controllo degli accessi, autenticazione a più fattori, catena di approvvigionamento.

CAPITOLO 3

Le prime 72 ore, ora per ora.

Ogni incidente è diverso. La sequenza delle decisioni no: prepararla prima è ciò che rende l'ente resiliente.

0 – 1 h

Contenere

Isolare i sistemi colpiti. Non spegnere tutto alla cieca: si perdono le tracce utili all'analisi.

1 – 6 h

Capire

Quali servizi, quali dati, da quando. Verificare subito se le copie di sicurezza sono integre e raggiungibili.

entro 24 h

Preallarme

Comunicazione al CSIRT Italia. Serve sapere cosa dichiarare: l'inventario e i log fanno la differenza.

24 – 48 h

Ripristinare pulito

Ripartire in un ambiente isolato, da copie verificate. Prima identità e servizi critici, poi il resto.

entro 72 h

Notifica completa

Impatto, cause presunte, misure adottate. Con dati concreti, non stime.

entro 1 mese

Relazione finale

Cosa è successo, perché, cosa cambia. È anche la base per l'audit ACN.

I cinque errori che trasformano un incidente in un fermo di settimane

1. **Copie sulla stessa rete** e con le stesse credenziali di produzione.
2. **Ripristino mai provato**: si scopre il giorno dell'attacco che non funziona.
3. **Active Directory non protetta**: senza identità non riparte nulla.
4. **Ripristinare sistemi ancora infetti** e farsi cifrare una seconda volta.
5. **Nessun ordine di ripristino** concordato tra IT e dirigenza.

01 PA centrale

Ministeri, agenzie, autorità indipendenti. Soggetti essenziali per definizione.

COSA RISCHIATE

- Interruzione di servizi nazionali a cittadini e imprese, con effetti a catena sugli enti collegati.
- Compromissione delle identità: un dominio violato apre tutti i sistemi.
- Esposizione pubblica e verifiche ACN sui 116 requisiti.

LE PRIORITÀ

- **Proteggere Active Directory ed Entra ID** con ripristino automatizzato della foresta.
- **Una sola piattaforma** per on-premise, cloud e Microsoft 365: meno strumenti, meno punti ciechi.
- **Test di ripristino documentati**, da mostrare in sede di audit.

> La domanda da portare al prossimo comitato: **«Se domani cadesse il dominio, in quante ore torniamo a firmare atti?»**

02 Regioni, città metropolitane, comuni

Regioni, città metropolitane, comuni sopra 100.000 abitanti e capoluoghi di regione.

COSA RISCHIATE

- Sportelli fermi: anagrafe, tributi, SUAP, servizi sociali, protocollo.
- Team IT piccoli e molti fornitori esterni: la catena di approvvigionamento è un punto debole.
- Dati personali di tutta la cittadinanza esposti e ricattabili.

LE PRIORITÀ

- **Copie immutabili e isolate**, che un attaccante non possa cancellare.
- **Un ordine di ripristino** per servizio, deciso con la dirigenza prima dell'emergenza.
- **Semplicità di gestione**: una console unica che anche un team di due persone possa governare.

> La domanda da portare in giunta: **«Quale servizio riapriamo per primo, e chi lo ha deciso?»**

03 Sanità

Aziende sanitarie locali e strutture collegate. Qui il fermo si misura in pazienti.

51% delle strutture sanitarie colpite da ransomware è riuscita a ripristinare dalle copie di sicurezza. Un anno prima erano il 72%.

Sophos, State of Ransomware in Healthcare 2025

COSA RISCHIATE

- Pronto soccorso, CUP, referti e laboratori fermi o in modalità cartacea.
- Estorsione sui dati sanitari, anche senza cifratura.

LE PRIORITÀ

- **Tempi di ripristino misurati** per i sistemi clinici critici.
- **Clean room recovery**: ripartire in un ambiente isolato e verificato.

CAPITOLO 5

I sei mattoni della cyber resilience.

Nessuno basta da solo. Insieme, trasformano le copie dei dati in capacità di ripartire.

Protezione dei dati

Copie di server, VM, database e cloud, immutabili e isolate.

Rilevamento delle minacce

Anomalie e cifrature individuate nei dati protetti, prima del ripristino.

Ripristino pulito

Clean room: un ambiente isolato dove verificare e riaccendere i sistemi.

Disaster recovery orchestrato

Failover e failback automatici, nell'ordine dei servizi critici.

Protezione delle identità

Active Directory ed Entra ID, con ripristino granulare e della foresta.

Cloud e SaaS

Microsoft 365, Azure, AWS, Google Cloud e Kubernetes nella stessa console.

Sono le componenti della piattaforma Commvault Cloud, disponibili per la PA nella Convenzione Consip ID 2955 · Lotto 4.

CAPITOLO 6

Un ripristino mai testato è un'ipotesi.

Solo il 53% delle organizzazioni colpite da ransomware torna pienamente operativo entro una settimana (Sophos, State of Ransomware 2025). La differenza la fa il test.

1 **Scegliete tre servizi critici**
Quelli che, se fermi, fanno notizia. Per ognuno: sistemi, dati, dipendenze.

2 **Ripristinate in un ambiente isolato**
Mai sopra la produzione. Misurate il tempo reale, non quello a preventivo.

3 **Verificate che funzionino**
Un utente vero prova il servizio: login, una pratica, un documento.

4 **Mettetelo per iscritto**
Tempi, problemi, correzioni. È la prova che l'ACN vi chiederà.

Ogni quanto? Almeno due volte l'anno sui servizi critici, e dopo ogni cambiamento importante dell'infrastruttura.

CAPITOLO 7 · AUTOVALUTAZIONE

Quanto siete pronti?

20 domande, 10 minuti.

Rispondete con onestà: un punto per ogni sì pieno. Un «più o meno» vale zero. Stampate queste pagine e compilatele con il vostro team.

PROTEZIONE

01	Abbiamo almeno una copia dei dati non modificabile e isolata dalla rete di produzione?	☐
02	Le credenziali della console delle copie sono separate da quelle di dominio e protette da MFA?	☐
03	Proteggiamo anche Microsoft 365 (posta, Teams, SharePoint, OneDrive), non solo i server?	☐
04	Active Directory ed Entra ID hanno una protezione dedicata e ripristinabile?	☐
05	Sappiamo quali dati personali e sanitari custodiamo e dove si trovano?	☐

RILEVAMENTO

06	Riceviamo un allarme se i dati iniziano a essere cifrati in modo anomalo?	☐
07	Controlliamo che le copie non contengano malware prima di usarle?	☐
08	Qualcuno è reperibile fuori orario per un allarme critico?	☐

RISPOSTA

- [ ] 09 Esiste una procedura scritta per le prime 24 ore, con nomi e numeri?
- [ ] 10 Sappiamo chi invia il preallarme al CSIRT Italia e con quali informazioni?
- [ ] 11 La dirigenza sa quali decisioni le spettano durante un incidente?
- [ ] 12 Abbiamo i contatti dei fornitori critici e sappiamo cosa aspettarci da loro?

RIPRISTINO

- [ ] 13 Abbiamo provato un ripristino completo negli ultimi sei mesi?
- [ ] 14 Conosciamo il tempo reale di ripristino dei tre servizi più critici?
- [ ] 15 Esiste un ordine di ripristino dei servizi approvato dalla dirigenza?
- [ ] 16 Possiamo ripartire in un ambiente isolato, senza reintrodurre il malware?
- [ ] 17 Abbiamo copie in una seconda sede o in cloud, fuori dal perimetro principale?

GOVERNO

18	Le misure di sicurezza sono state approvate dagli organi di amministrazione?	☐
19	Dirigenti e personale hanno seguito una formazione sulla sicurezza nell'ultimo anno?	☐
20	I test di ripristino sono documentati e pronti da mostrare in un'ispezione?	☐

Il vostro punteggio: ___ / 20

0 – 9 **Esposti.** Un attacco oggi vi fermerebbe per settimane. Partite dal ripristino testato e dalle copie isolate.

10 – 15 **Sulla strada.** Le basi ci sono, mancano prove e procedure. Concentratevi su test e ordine di ripristino.

16 – 20 **Resilienti.** Documentate tutto e ripetete i test: è ciò che l'ACN verificherà.

Qualunque sia il risultato, le risposte «no» sono la vostra lista di priorità. Nel mini audit gratuito le rivediamo insieme.

COME SI ACQUISTA

Commvault per la PA, in convenzione.

Le soluzioni di questa guida sono acquistabili in **Convenzione Consip**, senza una gara propria: tempi più brevi e condizioni già negoziate.

CONVENZIONE

ID 2955 · Lotto 4

Prodotti software on premise · Prodotti Commvault, rinnovo della manutenzione per le licenze in uso e servizi connessi

Fornitore aggiudicatario:

HTDI

1 **Verifica del fabbisogno** con HTDI: cosa proteggere, con quali tempi di ripristino.

2 **Ordinativo di fornitura** sul portale Acquisti in Rete della PA.

3 **Attivazione e servizi** di configurazione, con il supporto tecnico di HTDI e Commvault.

IL PROSSIMO PASSO

Trenta minuti per sapere dove siete.

Un mini audit gratuito con gli specialisti HTDI: rivediamo insieme la vostra checklist, i tempi di ripristino reali e le priorità in vista delle verifiche ACN.

MINI AUDIT · 30 MINUTI

lotto4.htdi.it

commvault26_lotto4@htdi.it

WEBINAR GRATUITO · GIOVEDÌ 19 NOVEMBRE, 11:00

Un attacco blocca il tuo ente. Chi ne risponde?

Con l'Avv. Matia Campo (CMS) e gli esperti Commvault · lotto4.htdi.it/talk-01

Fonti. ACN, Relazione annuale al Parlamento 2025 · Rapporto Clusit 2026 · D.Lgs. 138/2024 e Determinazione ACN n. 379907/2025 · Sophos, State of Ransomware 2025 e State of Ransomware in Healthcare 2025 · Sophos, State of Ransomware 2024 e The impact of compromised backups on ransomware outcomes (2024). Dati aggiornati a ottobre 2026. Questa guida ha scopo informativo e non costituisce consulenza legale.