

EFESTO · ANALISI DI RETE E PENETRATION TEST

Analisi di rete su sette livelli e penetration test

Sede centrale su sei piani con doppio accesso a Internet, centro dati unico e agenzie collegate in VPN: dal kick-off di progetto alla verifica dopo trenta giorni.

CLIENTE

Voltaria Distribuzione S.p.A. (esempio)

SETTORE

Distribuzione all'ingrosso di materiale elettrico e illuminazione

CALENDARIO

Kick-off 28 aprile 2026 · test dall'11 al 26 maggio 2026 (12 giornate)

VERSIONE

1.0 · documento completo

RIFERIMENTI

Mandato VD-2026-031 · nasce dallo studio di fattibilità SF-2026-014 (31 marzo 2026)

SERVIZIO

Efesto — livello Avanzato

CONSEGNA E VERIFICA

Relazione 8 giugno 2026 · handover 10 giugno · verifica successiva 8 luglio 2026

REDATTO DA

BoNet™ — un progetto di Euro Buchberger

Documento dimostrativo. Ragione sociale, persone, fornitori di connettività, indirizzi, numeri e rilievi descritti in questa relazione sono inventati a scopo illustrativo e non si riferiscono ad alcun cliente reale. BoNet™ la pubblica come esempio del metodo, del livello di dettaglio e dell'organizzazione di un incarico di analisi di rete e di penetration test su una rete complessa. La relazione ha un documento gemello, lo studio di fattibilità, che la precede. L'hardware e il software indicati rappresentano il pool scelto per questa prova simulata: in un incarico reale vengono progettati di volta in volta.

Come leggere questo documento

CAPITOLO 1 · CONVENZIONE DEI COLORI E DEI SIMBOLI

In tutto il documento i colori hanno un significato fisso. Chi li impara una volta può leggere qualsiasi pagina senza bisogno della legenda: gravità dei rilievi, zone di rete, tipi di collegamento e riquadri di attenzione usano famiglie di colori diverse e non si confondono tra loro. Ogni colore è sempre accompagnato da un testo o da una sigla, così il documento resta leggibile anche in bianco e nero.

1.1 Gravità dei rilievi

La gravità misura quanto un rilievo può incidere sulla continuità del servizio e sulla protezione dei dati. Usa colori caldi, dal bordeaux al verde: **questi colori compaiono solo nei rilievi** e mai negli schemi di rete.

Gravità	Significato	Tempi indicativi di intervento
CRITICO	Può causare fermo totale, perdita di dati o accesso completo a persone non autorizzate, con sforzo contenuto.	Misure contenitive subito (entro 72 ore); correzione definitiva entro 30 giorni
ALTO	Impatto serio su servizi o dati, realizzabile con competenze correnti.	Correzione entro 30 giorni
MEDIO	Impatto limitato, oppure realizzabile solo in condizioni particolari.	Correzione entro 90 giorni
BASSO	Impatto minimo o condizioni difficili da realizzare.	Al prossimo intervento programmato
INFORMATIVO	Osservazione o buona pratica: nessun rischio diretto.	Nessuna azione richiesta
✓ PUNTO DI FORZA	Scelta progettuale ben riuscita, da mantenere nel tempo.	—

Gli stessi colori caldi indicano anche il **rischio operativo** di una giornata di test (capitolo 6) e il livello dei rischi di progetto dello studio di fattibilità. Gli **esiti** della matrice di consegna (capitolo 23) usano i blu e i viola: **✓ SODDISFATTA** **⚠ CON RISERVA** **? DA VERIFICARE**.

1.2 Zone di rete (schemi)

Negli schemi ogni zona ha un proprio colore, preso dalla famiglia dei blu, dei viola, dei rosa e dei marroni. Gli stessi colori tornano nelle tabelle quando si parla di quella zona.

Zona	Che cosa comprende
INTERNET E FORNITORI	Le linee dei due fornitori (Fibra Marmolada e Rete Lavaredo) e i loro modem, di proprietà dei fornitori.
BORDO CLIENTE	I due router del cliente, subito dopo i modem, che dialogano in BGP con i fornitori.
FIREWALL	La coppia di firewall in alta affidabilità e le VPN verso le agenzie.
DMZ	La zona intermedia con i servizi raggiungibili da Internet: posta, sito, concentratore VPN.
CORE - CED	I due core in failover, i server, il backup: tutto nel centro dati unico.
UTENTI (DATI)	La rete dei computer dei dipendenti, sui sei piani.
TELEFONIA IP	Un telefono IP per utente, su rete dedicata alla voce.
STAMPANTI	Dieci stampanti per piano, su rete dedicata.
TELECAMERE	Le telecamere e il registratore video, su reti dedicate.
OSPITI WI-FI	Il Wi-Fi per gli ospiti, solo nella sala d'attesa al piano terra, isolato dal resto.
STRUMENTI BONET	L'hardware di test, i suoi collegamenti e i punti sotto test (T1-T6). L'oro è riservato a BoNet™.

1.3 Collegamenti

I collegamenti si distinguono per il tipo di linea, non per il colore.

	Fibra ottica — dorsali verticali, linee dei fornitori, collegamenti dei router di bordo.
	Rame Cat6 — cablaggio orizzontale e collegamenti nel CED.
	VPN — tunnel cifrati tra le agenzie e il firewall.
	Failover / alta affidabilità — coppie di apparati che si sostituiscono a vicenda.
	Collegamento di test BoNet — temporaneo, solo per la durata dell'incarico.

1.4 Riquadri e sigle

NOTA

Chiarimenti e definizioni di termini tecnici.

ATTENZIONE

Un punto che richiede cura, senza essere un divieto.

STOP · LIMITE INVALIDICABILE

Ciò che non si fa mai, o la condizione in cui ci si ferma subito.
Il rosso vivo è riservato a questo uso.

RECOVERY

Che cosa si fa per tornare alla normalità, e chi lo fa.

DA DECIDERE AL KICK-OFF

Un punto che il cliente e BoNet™ stabiliscono insieme prima di iniziare.

✓ PUNTO DI FORZA

Una scelta ben riuscita dell'infrastruttura del cliente.

STRUMENTI E ATTIVITÀ BONET

Che cosa installa e che cosa fa BoNet™.

Sigle. T1-T6: punti sotto test (switch di piano scelti dal cliente) · G1-G12: giornate di test · R6-01: rilievo dell'analisi di livello 6 · PT-03: rilievo del penetration test · REI120: compartimento resistente al fuoco per 120 minuti · HA: alta affidabilità · CED: centro elaborazione dati.

Lo scenario: Voltaria Distribuzione S.p.A.

CAPITOLO 2 · IL CLIENTE E LA SUA RETE

Voltaria Distribuzione S.p.A. (nome di fantasia) è un distributore all'ingrosso di materiale elettrico e illuminazione con una sede centrale su sei piani e quaranta agenzie commerciali sul territorio italiano. La rete è stata progettata con cura: ridondanza dalle linee ai piani, doppia alimentazione degli apparati, due percorsi fisici per la fibra. È un buon punto di partenza, e per questo un buon banco di prova: un'analisi su sette livelli e un penetration test mostrano dove la ridondanza protegge davvero e dove restano margini di miglioramento.

DA DOVE NASCE QUESTO INCARICO

Il 9 marzo 2026 Voltaria ha formulato **undici richieste (R1-R11)**: tenuta ai guasti, esposizione da Internet, rischio dai piani e dal Wi-Fi ospiti, inventario, VPN delle agenzie, backup, attestazione per clienti e assicuratore, nessun fermo degli ordini, piano di rimedio, passaggio delle conoscenze, riservatezza. Lo **studio di fattibilità SF-2026-014** (31 marzo 2026) le ha valutate e ha proposto l'opzione C, che questa relazione documenta. Al capitolo 23 ogni richiesta riceve il suo esito.

2.1 La rete in numeri

Elemento	Descrizione nell'esempio
Accesso a Internet	4 linee in fibra da 1 Gbit/s: 2 per ciascuno dei due fornitori (Fibra Marmolada e Rete Lavaredo), su due anelli terrestri diversi per fornitore. 4 modem di proprietà dei fornitori.
Bordo del cliente	2 router in coppia, fuori dalla DMZ, subito dopo i modem. Dialogano in BGP con i fornitori: Voltaria ha un proprio sistema autonomo (AS 64500) e un blocco di indirizzi pubblici proprio (203.0.113.0/24). Numeri e indirizzi sono quelli riservati alla documentazione.
Sicurezza di perimetro	2 firewall in alta affidabilità (coppia attivo/passivo), una DMZ con posta, sito e concentratore VPN, e 40 VPN verso le agenzie.
Centro dati (CED)	Un solo locale, al piano interrato: 2 core in failover, 3 server di virtualizzazione con 14 macchine virtuali (file, posta, gestionali, directory), sistema di backup e registratore video. Tutti gli apparati hanno doppio alimentatore.
Edificio	6 piani (piano terra e piani 1-5), 2 switch per piano : ciascuno collegato a un core diverso e tra loro collegati, così che la caduta di un core non isoli i dispositivi collegati. 12 switch in tutto.
Utenti e dispositivi	Da 65 a 80 utenti per piano (433 in totale), un telefono IP per utente (433), 10 stampanti per piano (60). 56 telecamere su reti dedicate.
Cablaggio	Dorsali verticali in fibra su due cavedi diversi, entrambi REI120 ; cablaggio orizzontale in rame Cat6.
Wi-Fi	Solo per gli ospiti, nella sala d'attesa del piano terra, su rete isolata.

✓ PUNTI DI FORZA

Quattro linee su due fornitori e due anelli; BGP sul bordo; firewall e core in coppia; doppio alimentatore ovunque; due cavedi REI120 per la fibra; reti separate per voce, stampanti, telecamere e ospiti; Wi-Fi limitato allo stretto necessario.

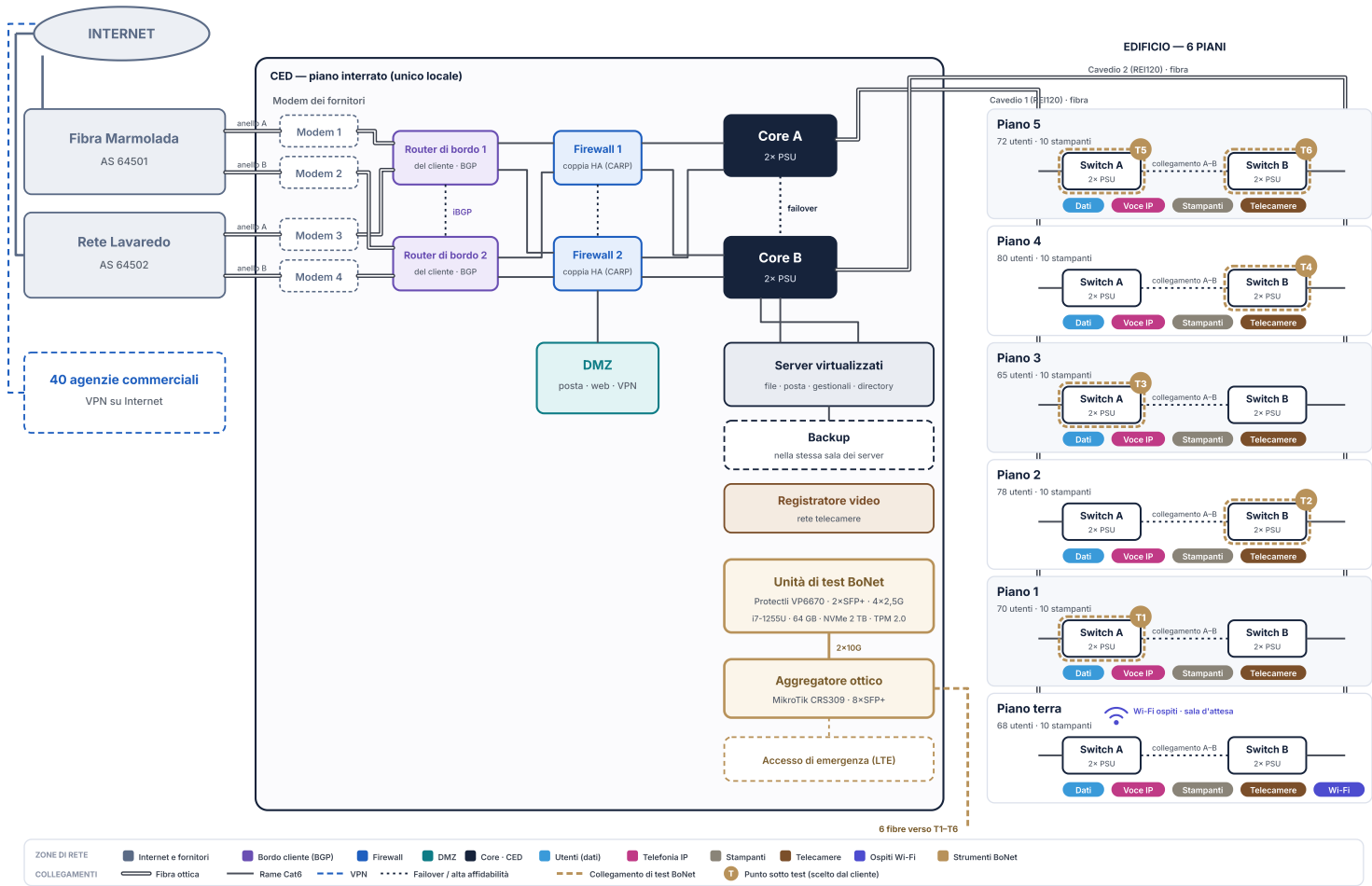
2.2 Come è organizzato il documento

Il documento si compone di tre parti e di quattro appendici. Per leggerlo in ordine seguire i capitoli; per cercare un tema, usare la tabella.

Cap.	Contenuto
Parte A — Il progetto (parte dallo studio di fattibilità SF-2026-014)	
1	Come leggere questo documento: convenzione dei colori
2–3	Lo scenario e lo schema generale della rete
4	Il kick-off di progetto: ruoli, limiti, condizioni di stop, recovery
5	Hardware e software di test, con licenze
6–7	Le giornate di test; il cablaggio ai piani (tre opzioni)
Parte B — Le sette analisi di rete	
8–14	Rilevamento e inventario · Topologia e instradamento · Prestazioni e capacità · Sicurezza e segmentazione · Configurazioni e aggiornamenti · Affidabilità e continuità · Piano di intervento
Parte C — Il penetration test (Efesto, livello Avanzato)	
15–19	Perimetro esterno · Rete interna e piani · Wi-Fi ospiti, telecamere, stampanti · Servizi e backup · Sfruttamento controllato e verifica dell'impatto
20–22	Rilievi per gravità · Pulizia e ripristino · Piano di rimedio
23	Handover: consegna e passaggio, con la matrice di tracciabilità delle richieste dello studio
24	Verifica successiva a 30 giorni
Appendici	
A–D	Licenze degli strumenti · Registro delle prove · Glossario · Aspetti legali

CAPITOLO 3 · SCHEMA GENERALE DELLA RETE

Dalle quattro linee ai dodici switch di piano



Lo schema mostra la rete di Voltaria e, in oro, gli strumenti BoNet™ installati per l'incarico: l'unità di test nel CED, l'aggregatore ottico con sei fibre verso i punti sotto test T1-T6 (uno ai piani 1-4, due al piano 5) e l'accesso di emergenza. I colori seguono la convenzione del capitolo 1.

Il kick-off di progetto

CAPITOLO 4 · PRIMA DI OGNI CAVO E DI OGNI TEST

Un penetration test con hardware installato nel centro dati è un'attività **invasiva** e, se non governata, **pericolosa** per la continuità del servizio. Il kick-off è la riunione — e il verbale firmato che ne deriva — in cui si stabilisce **chi fa che cosa, quando e perché**, quali sono i limiti che non si superano mai e che cosa si fa se qualcosa va storto. Senza un kick-off concluso e firmato non si installa nulla e non si esegue alcun test.

Il **punto di partenza è lo studio di fattibilità SF-2026-014**, consegnato il 31 marzo 2026: ne riprende le richieste, le ipotesi, le condizioni e i rischi, e li trasforma in decisioni firmate. È il primo punto all'ordine del giorno.

REGOLA D'INGAGGIO

Nessuna attività parte senza il verbale di kick-off firmato dallo sponsor e dal referente tecnico del cliente. Qualsiasi persona coinvolta, di Voltaria o di BoNet™, può chiedere lo **stop** in qualunque momento, senza doverne spiegare il motivo.

4.1 Chi partecipa e che cosa decide

Ruolo	Nell'esempio	Decide e fa	Presenza
Sponsor	Direttore generale di Voltaria	Firma l'incarico e le autorizzazioni; accetta il rischio residuo.	Kick-off e chiusura
Referente tecnico	Responsabile sistemi informativi	Approva piano, finestre orarie e punti di test; può fermare i test; è il primo contatto per ogni anomalia.	Tutte le giornate, reperibile
Sicurezza e protezione dati	Referente privacy (DPO)	Valuta i dati personali coinvolti; riceve le segnalazioni di incidente; gestisce le notifiche di legge, che spettano al titolare.	Kick-off; reperibile
Responsabile impianti	Facility manager	Alimentazione, raffreddamento e accessi del CED; passaggi nei cavedi REI120.	G1, G12 e su richiesta
Elettricista abilitato	Ditta di fiducia di Voltaria	Verifica e fornisce l'alimentazione dedicata; interviene in caso di emergenza elettrica.	G1 e G12 in loco; altri giorni reperibile entro 2 ore
Cablatore certificato	Ditta di fiducia di Voltaria	Tiri di cavo, certificazione delle tratte, ripristino della tenuta al fuoco dei passaggi.	G1 e G12 in loco; altri giorni reperibile entro 2 ore
Fornitori di connettività	Fibra Marmolada, Rete Lavaredo	Consenso scritto ai controlli sul perimetro esterno; riferimento tecnico per le anomalie sulle linee.	Numero di assistenza dedicato
Responsabile di progetto BoNet™	BoNet™	Conduce i test; è presente in loco durante tutte le attività a rischio e per ogni emergenza o recovery ; decide l'arresto.	Tutte le giornate
Tecnico di supporto BoNet™	BoNet™	Affianca nei test; custodisce le evidenze e il registro delle prove.	Giornate di test

4.2 Che cosa si decide al kick-off

#	Decisione	Perché è importante
1	Studio di fattibilità	Si confermano o si correggono le richieste R1-R11, le ipotesi e le cinque condizioni dello studio SF-2026-014; l'esito entra nel verbale.
2	Perimetro e obiettivi	Che cosa si testa, da dove e perché; che cosa resta fuori. Ciò che non è scritto non si tocca.
3	Calendario e finestre orarie	Le prove ad alto rischio si fanno fuori orario o nei giorni di minore attività; i giorni lavorativi si riservano alle attività non invasive.
4	Limiti operativi	L'elenco di ciò che non si fa mai (riquadro in questo capitolo).
5	Installazione nel CED	Spazio nel rack, alimentazione e raffreddamento (riquadro dedicato più avanti).
6	Cablaggio ai piani	Quale delle tre opzioni si usa (capitolo 7): tratte spare esistenti, tiri dedicati o unità mobile.
7	I sei switch sotto test	Li sceglie il cliente: uno ai piani 1-4 e due al piano 5. Per ognuno si fissano finestra, porta e responsabile.

#	Decisione	Perché è importante
8	Autorizzazioni di terzi	Consenso scritto dei fornitori di connettività e, se serve, del proprietario dell'edificio e del manutentore degli impianti. Voltaria conferma di aver informato il proprio assicuratore (l'assicurazione è a suo carico, come da mandato).
9	Prerequisiti di sicurezza	Backup recente con prova di ripristino riuscita; configurazioni degli apparati salvate; elenco dei servizi critici e dei loro orari.
10	Comunicazioni e reperibilità	Rubrica di emergenza, canale di comunicazione, tempi di risposta, chi informa chi.
11	Licenze e riservatezza	Elenco degli strumenti con le rispettive licenze (capitolo 5, appendice A); accordo di riservatezza; trattamento e distruzione delle evidenze.

DA DECIDERE AL KICK-OFF · INSTALLAZIONE NEL CED: ALIMENTAZIONE E CALORE

L'unità di test assorbe **12 W a riposo e fino a 100 W** sotto carico (scheda del produttore); l'aggregatore ottico assorbe fino a circa 23-33 W (le fonti commerciali differiscono: il dato definitivo è quello della scheda del produttore). Il carico complessivo, con un piccolo UPS dedicato, è nell'ordine di **200 W**, ma va comunque concordato con il responsabile impianti: **(a)** linea o presa protetta da interruttore dedicato, senza collegarsi a PDU già al limite; **(b)** UPS dedicato, dimensionato per lo spegnimento ordinato; **(c)** posizione nel rack con flusso d'aria libero e pannelli ciechi per evitare ricircoli; **(d)** rilievo della temperatura dell'aria in ingresso prima e dopo l'installazione, con soglia di allerta concordata (per esempio 27 °C all'ingresso del rack) e spegnimento dell'unità BoNet™ al superamento; **(e)** nessuno scollegamento di apparati del cliente per fare spazio.

4.3 Limiti operativi e condizioni di stop

CHE COSA NON SI FA MAI

- Nessuna prova che saturi le linee o i firewall durante l'orario di lavoro; nessun test di negazione del servizio sui sistemi in produzione.
- Nessun annuncio né modifica di rotte BGP: sul bordo si fanno solo controlli di configurazione e di esposizione, in sola lettura.
- Nessuna modifica alle configurazioni di produzione del cliente: ogni modifica è del cliente, su sua decisione.
- Nessuna apertura o foratura di cavedi e compartimentazioni REI120: si usano solo passaggi già esistenti e solo il cablatore tocca i varchi.
- Nessun accesso ai dati personali oltre il minimo necessario per provare un rilievo; le prove si registrano senza copiare i dati.
- Nessuna prova fuori dal perimetro e dalle finestre approvate; nessuna prova su sistemi di terzi senza consenso scritto.

CONDIZIONI DI STOP · CI SI FERMA SUBITO SE

un servizio mostra anomalie; il cliente riceve un allarme; la temperatura nel CED supera la soglia; si perde una linea, un core o un firewall in modo imprevisto; il referente tecnico lo chiede; si individua un incidente di sicurezza reale in corso. **Dopo uno stop si riparte solo con il consenso congiunto del referente tecnico e del responsabile di progetto BoNet™.** Le decisioni si prendono entro 15 minuti.

4.4 Piano di recovery

Il piano dice che cosa si fa se una prova o un evento esterno provoca un'interruzione. È stato concordato al kick-off e viene riletto all'inizio di ogni giornata di test.

Evento	Azione immediata (entro 5 minuti)	Responsabile	Ripristino e verifica
Un core va in avaria durante un test	Stop; nessun intervento di BoNet™; si verifica che il core superstita regga il carico.	Referente tecnico + BoNet™	Ripristino secondo la procedura del cliente; prova di ritorno solo in finestra protetta.
Una linea o una sessione BGP cade	Stop; BoNet™ non agisce sul bordo; si contatta il fornitore se serve.	Referente tecnico + fornitore	Verifica delle sessioni e delle rotte; ripresa solo con consenso.
Commutazione imprevista tra i firewall	Stop; si verifica quale firewall è attivo e lo stato delle sessioni VPN.	Referente tecnico	Verifica delle VPN delle agenzie e delle regole attive.
Allarme di temperatura o sovraccarico elettrico nel CED	Spegnimento dell'unità BoNet™ con il pulsante, con l'accesso di emergenza (LTE) o dall'interruttore dedicato.	BoNet™ + elettricista	Misura di temperatura e assorbimento; ripartenza solo con l'ok del responsabile impianti.
Uno switch di piano non risponde	BoNet™ scollega la tratta di test; si verifica lo switch gemello.	BoNet™ + IT	Ripristino dalla configurazione salvata; verifica di telefoni, stampanti e postazioni del piano.

Evento	Azione immediata (entro 5 minuti)	Responsabile	Ripristino e verifica
Un servizio applicativo rallenta	Stop e rientro del traffico di test.	BoNet™ + IT	Analisi della causa; ripresa con nuovo ok.
Danno a un cavo o a un passaggio REI120	Fermo lavori nell'area.	Cablature + facility	Ripristino e collaudo documentati, compresa la tenuta al fuoco, prima di riaprire l'area.
Si scopre un incidente di sicurezza già in corso	Stop; informazione immediata a sponsor e DPO; le prove non si toccano.	Sponsor + DPO + BoNet™	Il titolare gestisce le notifiche di legge; BoNet™ supporta con le evidenze raccolte.
Smarrimento o furto dell'unità di test	Si informa subito il cliente; il disco è cifrato e protetto dal TPM.	BoNet™	Revoca di credenziali e accessi usati nei test; relazione scritta entro 24 ore.

RECOVERY · PRESENZA IN LOCO

Il responsabile di progetto BoNet™ è **in loco** durante tutte le attività a rischio e per ogni emergenza o recovery. L'elettricista e il cablatore sono in loco nei giorni G1 e G12 e raggiungibili entro 2 ore negli altri giorni. Il cliente garantisce l'accesso al CED per tutta la durata dell'incarico.

4.5 CHE COSA PRODUCE IL KICK-OFF

Il **verbale firmato**, che conferma o aggiorna lo studio di fattibilità, con perimetro, calendario, limiti e scelta del cablaggio · il **piano di test e di recovery**, con la rubrica di emergenza · l'**elenco delle licenze** degli strumenti (appendice A) · le **autorizzazioni di terzi** (fornitori di connettività, proprietario dell'edificio, manutentori) · il **rilievo iniziale** del CED: temperatura, assorbimento e stato dei backup.

Hardware e software di test

CAPITOLO 5 · CHE COSA INSTALLA BONET™ E CON QUALI STRUMENTI LAVORA

Per questo incarico BoNet™ installa nel CED di Voltaria un'unità di test dedicata, con collegamenti in fibra verso sei switch di piano scelti dal cliente. Il pool descritto qui è quello scelto per questa **prova simulata**: in un incarico reale viene progettato di volta in volta, in base a che cosa si fa e a per quale infrastruttura, e può essere di maggiore o di minore impegno.

STRUMENTI E ATTIVITÀ BONET™ · IL POOL È PROPORZIONATO ALL'INCARICO

Una rete di casa, uno studio professionale o un'azienda su sei piani richiedono dotazioni diverse. Per questo, prima di ogni incarico reale, BoNet™ definisce il pool, compra o noleggia gli strumenti necessari, intesta le licenze a BoNet™ e le elenca al kick-off e nella relazione finale. Gli strumenti di questo capitolo sono quelli che useremmo qui.

5.1 Hardware

Sigla	Componente	Modello	Funzione e caratteristiche principali
H1	Unità di test principale, nel CED	Protectli Vault Pro VP6670 ✓ dati dalla scheda tecnica del produttore (15/12/2025)	Esegue scansioni e raccolta delle prove. Intel Core i7-1255U (10 core, 12 thread); 2 porte SFP+ 10G (Intel X710-BM2) e 4 porte 2,5G (Intel i226-V); memoria DDR5 fino a 64 GB (configurati 64 GB); disco NVMe M.2 2280 (configurato 2 TB, cifrato); modulo TPM 2.0 opzionale (installato); slot M.2 per modulo LTE con SIM (installato: accesso di emergenza). Consumo 12 W a riposo e 100 W al massimo; temperatura di funzionamento da -10 a +50 °C; 191 × 178 × 76 mm. Ha due ventole interne: non è un apparato senza ventole.
H2	Aggregatore ottico, nel CED	MikroTik CRS309-1G-8S+IN ✓ dati dalle schede dei rivenditori; consumo da confermare	8 porte SFP+ 10G e una porta 1G di gestione, raffreddamento passivo. 2 porte verso H1 (20 Gbit/s aggregati) e 6 porte verso i punti sotto test T1-T6: sono le sei fibre dell'incarico. Consumo massimo 23-33 W (le fonti discordano: vale la scheda del produttore).
H3	Unità di riserva	Seconda VP6670, configurata come H1	Sostituisce H1 in caso di guasto, senza perdere giornate di test.
H4	Punto di osservazione esterno	Server in un data center in Italia, con indirizzo fisso (da scegliere al kick-off)	Per le prove «da Internet»: si osserva il perimetro di Voltaria da fuori, non dalla sua rete.
H5	Moduli ottici SFP+	10G SR (multimodale OM4) e 10G LR (monomodale OS2) (da definire)	Otto moduli più scorta, scelti dopo il rilievo della fibra e degli switch del cliente.
H6	Cavi e prova	Patch in fibra OM4 e OS2, bobine Cat6, strumenti per certificare rame e fibra	Per i tiri dedicati (capitolo 7) e per i controlli di continuità: a cura del cablatore.
H7	TAP di rete passivi	Rame e fibra (da definire)	Permettono di osservare il traffico senza interromperlo.
H8	UPS dedicato e misura dei consumi	UPS compatto con PDU misurata (da definire)	Spegnimento ordinato e misura dell'assorbimento durante tutto l'incarico.
H9	Unità mobile	Portatile con adattatori SFP+ ed Ethernet (da definire)	Per l'opzione C del cablaggio: si collega direttamente allo switch del piano, senza tiri di cavo.
H10	Adattatore Wi-Fi	USB, con modalità di monitoraggio (da definire)	Per le verifiche sul Wi-Fi ospiti (giornata G9).

NOTA · BASTA UN'UNITÀ?

Per i test dal CED, una sola unità basta: 10 core, 64 GB di memoria e 20 Gbit/s verso l'aggregatore reggono con ampio margine i carichi di questo incarico, che sono limitati per scelta. Ma un incarico invasivo non si affida a un solo apparato: per questo il pool comprende l'unità di riserva (H3), il punto di osservazione esterno (H4), l'accesso di emergenza (LTE) e l'adattatore per il Wi-Fi (H10).

5.2 Software

Funzione	Strumento	Licenza	Note
Sistema di base	Kali Linux (versione rolling, immagine ufficiale)	Software libero (licenze varie, in prevalenza GPL)	Disco cifrato; immagine verificata con la firma del produttore prima dell'uso.
Inventario e scansione	Nmap	Nmap Public Source License	Rilevamento di dispositivi, porte e servizi, con velocità limitata concordata.
Ricerca di vulnerabilità	Greenbone Community Edition (OpenVAS) · Tenable Nessus Professional	GPL · commerciale , abbonamento annuale per scanner	Due motori diversi, per confrontare i risultati ed eliminare i falsi allarmi.
Analisi del traffico	Wireshark · Zeek · Suricata	GPLv2 · BSD · GPLv2	Anche per capire se i sistemi del cliente si accorgono dei test.
Applicazioni web e cifrature	Burp Suite Professional (PortSwigger) · testssl.sh	Commerciale , abbonamento annuale per utente · GPLv2	Verifica di sito, posta e portali; solidità delle cifrature.
Directory e identità	PingCastle (Netwrix) · BloodHound Community Edition (SpecterOps)	Commerciale per i consulenti · Apache 2.0	Stato di salute della directory aziendale e percorsi di privilegio.
Wi-Fi	Kismet	GPLv2	Rilevamento e verifica della rete ospiti.
Prestazioni	iperf3	BSD	Misure di velocità tra i piani e il CED, in finestre concordate.
Registro delle prove	Orologio sincronizzato (NTP), registrazione delle sessioni, impronta SHA-256 dei file, archivio cifrato	Procedure interne BoNet™	Ogni prova ha data, ora, operatore e impronta: si può ripetere e verificare.

Gli strumenti per lo sfruttamento controllato (giornata G11) non sono elencati qui: si scelgono caso per caso e si concordano al kick-off, una prova alla volta, con il consenso del referente tecnico.

LICENZE · COME LE GESTIAMO

Ogni licenza commerciale è **acquistata a fronte dell'incarico** e intestata a BoNet™ (non al cliente). Tipo di licenza, numero e scadenza sono presentati **al kick-off** e riportati nella **relazione finale** (appendice A). Le versioni degli strumenti sono quelle in vigore all'inizio dell'incarico e sono congelate fino alla chiusura, così che i risultati siano ripetibili.

Le giornate di test

CAPITOLO 6 · DODICI GIORNATE PIENE, UNA DOPO L’ALTRA

Il test è distribuito su **dodici giornate piene**, dall’11 al 26 maggio 2026, precedute dal kick-off (28 aprile) e seguite dalla relazione (8 giugno), dall’handover (10 giugno) e da una verifica dopo trenta giorni (8 luglio). Le giornate più delicate si svolgono con il responsabile di progetto BoNet™ in loco e, dove serve, con l’elettricista e il cablatore. Ogni giornata inizia con la rilettura del piano di recovery e finisce con la verifica che tutto sia tornato come prima.

Giorno	Attività	Dove	Rischio operativo	Presenze oltre a BoNet™
G1	Installazione nel CED. Posa di H1 e H2, verifiche elettriche e termiche, collegamento delle fibre, prove di continuità. Nessun test.	CED	MEDIO	Elettricista, cablatore, facility, IT
G2	Inventario e topologia (livelli 1 e 2): rilevamento passivo, verifica dello schema, misure di base delle prestazioni.	CED	BASSO	IT
G3	Perimetro esterno, parte 1. Osservazione dall’esterno (H4): servizi pubblicati, DMZ, posta e sito.	Esterno	BASSO	IT
G4	Perimetro esterno, parte 2. Router di bordo e sessioni BGP (solo controlli di configurazione in lettura), firewall, VPN delle agenzie.	Esterno + CED	MEDIO	IT; fornitori reperibili
G5	Rete interna dal CED. Separazione tra dati, voce, stampanti, telecamere e gestione; regole dei firewall.	CED	MEDIO	IT
G6	Piani 1 e 2 (punti T1 e T2): prove dalle porte di accesso, isolamento delle reti, stampanti. Fuori orario.	Piani 1–2	MEDIO	IT, cablatore reperibile
G7	Piani 3 e 4 (punti T3 e T4): prove dalle porte di accesso, telefoni IP, postazioni. Fuori orario.	Piani 3–4	MEDIO	IT, cablatore reperibile
G8	Piano 5 (punti T5 e T6, i due switch): prove dalle porte di accesso e prova di failover tra gli switch A e B, solo in finestra protetta e concordata.	Piano 5	ALTO	IT, elettricista e cablatore reperibili
G9	Wi-Fi ospiti, telecamere e stampanti. Isolamento della rete ospiti, reti dedicate, interfacce di gestione.	Piano terra + CED	BASSO	IT
G10	Servizi e backup. Posta, file, directory, gestionali; accessi al sistema di backup e stato delle copie.	CED	MEDIO	IT
G11	Sfruttamento controllato e verifica dell’impatto. Una prova alla volta, solo per i punti già emersi, con il consenso del referente tecnico.	Secondo il punto	ALTO	IT, DPO, elettricista reperibile
G12	Pulizia e ripristino. Rimozione di ogni file, utenza o configurazione creati dai test; verifica del ritorno allo stato iniziale; disinstallazione dell’hardware; riunione di chiusura.	CED + piani	MEDIO	Elettricista, cablatore, facility, IT, sponsor

NOTA · IL RISCHIO OPERATIVO

La colonna «Rischio operativo» usa gli stessi colori della gravità dei rilievi, ma indica un’altra cosa: **quanto una giornata può incidere sul servizio se qualcosa va storto**. Le giornate a rischio più alto (G8 e G11) si svolgono in finestre protette, con il piano di recovery già aperto sul tavolo.

Dopo i test

Quando	Che cosa
Entro 8 giugno 2026	Relazione con rilievi per gravità, prove, impatto e correzioni consigliate; presentazione allo sponsor e al referente tecnico.
10 giugno 2026	Handover: consegna e passaggio al team IT di Voltaria, con la matrice di tracciabilità delle richieste dello studio di fattibilità (capitolo 23).
8 luglio 2026	Verifica successiva (livello Avanzato): si ripetono le prove sui punti corretti, con un breve aggiornamento della relazione. Una nuova installazione dell’hardware si concorda caso per caso.

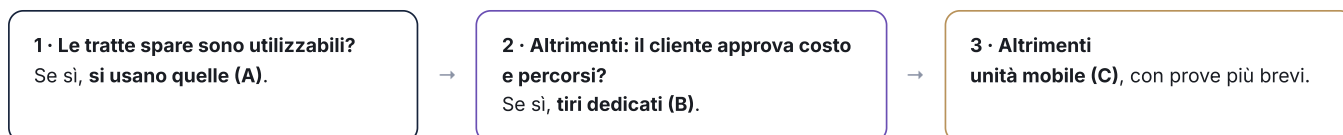
Cablaggio ai piani: tre opzioni

CAPITOLO 7 · COME SI RAGGIUNGONO I SEI SWITCH SOTTO TEST

L'unità di test nel CED deve poter raggiungere i sei switch scelti dal cliente (T1-T6, ai piani 1-5): servono quindi sei tratte dal CED ai piani. Esistono tre modi per averle. **L'impostazione principale usa le tratte di scorta (spare) che il cliente ha già predisposto in caso di guasto**; se non sono utilizzabili si passa ai tiri dedicati, e in ultimo all'unità mobile. La scelta si fa al kick-off, dopo un rilievo del cablaggio esistente.

A · Tratte spare esistenti impostazione principale	B · Tiri dedicati	C · Unità mobile
Che cosa. Coppie di fibra o cavi che Voltaria ha già posato come scorta per i guasti, nei due cavedi REI120 o nel cablaggio verticale. Quando. Se al kick-off risultano libere, etichettate, certificate e utilizzabili senza ridurre la scorta oltre il limite concordato. Chi. Il cablatore del cliente verifica e certifica le tratte; BoNet™ le collega alle sei porte dell'aggregatore. Vantaggi. Costo minore, nessun nuovo cavo, nessuna nuova opera nei cavedi, tempi brevi. Attenzione. La scorta è il paracadute del cliente: finché è in uso, la riserva si riduce. Si concorda una restituzione entro 4 ore su richiesta e si controlla la continuità prima e dopo. COSTO MINORE	Che cosa. Nuove tratte posate solo per l'incarico, dal CED ai sei switch, usando i passaggi esistenti. Quando. Se le tratte spare non esistono, non sono libere o il cliente preferisce non impegnarle. Chi. Cablatore certificato, con elettricista e facility dove serve. Il ripristino della tenuta al fuoco dei varchi è a cura del cablatore, documentato. Vantaggi. Indipendenza dalla scorta; percorsi e lunghezze scelti per il test. Attenzione. Costo maggiore (materiali, manodopera, collaudo); tempi più lunghi; serve l'autorizzazione a usare i passaggi REI120; rimozione o mantenimento delle tratte da concordare a fine incarico. COSTO MAGGIORE	Che cosa. Un portatile con adattatori (SFP+ ed Ethernet) che si collega direttamente alla porta dello switch di piano, senza tiri di cavo. Quando. Se A e B non sono praticabili, oppure per verifiche puntuali in più punti oltre ai sei. Chi. BoNet™, con il referente IT; il cablatore resta reperibile. Vantaggi. Nessuna opera; flessibile; installazione in pochi minuti. Attenzione. L'unità mobile non è collegata al CED: le prove sono più brevi e meno complete (nessuna cattura continua, nessuna correlazione immediata con l'unità principale) e richiedono presenza fisica a ogni piano, fuori orario. COSTO MINORE PIÙ PRESENZA BONET™

Come si sceglie



DA DECIDERE AL KICK-OFF · CHE COSA SI VERIFICA PRIMA DI SCEGLIERE

- Quante coppie spare esistono in ciascun cavedio, dove terminano e se sono etichettate.
- Tipo di fibra (multimodale OM4 o monomodale OS2) e connettori; perdita ottica e lunghezza di ogni tratta.
- Se gli switch dei sei punti hanno **porte SFP+ libere**; in caso contrario si usa una porta di accesso con un adattatore, a velocità minore.
- Chi del cliente può autorizzare l'uso della scorta e per quanto tempo; entro quanto la si restituisce se serve.
- Chi esegue e documenta il ripristino dei varchi REI120 se si apre un passaggio.

STOP · CAVEDI REI120

I compartimenti resistenti al fuoco non si aprono e non si forano per fare spazio ai nostri cavi: si usano solo i passaggi già esistenti, e solo il cablatore tocca i varchi, documentandone il ripristino.

Livello I · Rilevamento e inventario

CAPITOLO 8 · PARTE B — LE SETTE ANALISI DI RETE

Il primo livello risponde a una domanda semplice: **che cosa c'è davvero sulla rete?** Prima di giudicare qualsiasi cosa, si confronta l'inventario che Voltaria aveva con ciò che gli apparati dichiarano di avere collegato. Le differenze non sono errori da attribuire a qualcuno: sono il punto di partenza per avere, per la prima volta, un elenco di cui ci si può fidare (richiesta R4). L'attività si è svolta nella giornata G2, in orario di lavoro, in modo passivo, senza inviare traffico fuori dal normale.



8.1 Che cosa si è confrontato

Da una parte l'elenco di Voltaria (foglio di calcolo aggiornato l'ultima volta nel gennaio 2025, più lo schema della rete). Dall'altra ciò che risulta dalle tabelle degli apparati (indirizzi MAC e ARP degli switch e dei core, concessioni DHCP, elenco delle macchine virtuali dell'ipervisore) e da una scansione passiva di una settimana. Ogni dispositivo è stato associato a una categoria, a un piano e a una rete.

Categoria	Nell'elenco	Rilevati	Differenza
Postazioni di lavoro (computer)	433	441	+8
Telefoni IP	433	433	0
Stampanti e multifunzione	60	62	+2
Telecamere e registratore video	57	57	0
Switch di piano e core	14	14	0
Firewall e router di bordo	4	4	0
Server fisici e macchine virtuali	17	19	+2
Punti di accesso Wi-Fi (ospiti)	2	2	0
Sistema di backup e UPS gestiti	4	4	0
Altri dispositivi (display, lettori badge, orologi)	21	29	+8
Totale	1.045	1.065	+20

✓ PUNTO DI FORZA

Tutti gli apparati che reggono la rete (switch, core, firewall, router di bordo, server fisici) sono presenti nell'elenco, con nome, ruolo e piano. L'inventario è affidabile dove conta di più.

8.2 Rilievi

ID	Gravità	Titolo	Che cosa abbiamo osservato	Che cosa consigliamo
R1-01	ALTO	Macchina virtuale con sistema operativo non più supportato	Tra le due macchine virtuali non in elenco, una usa un sistema operativo che il produttore non aggiorna più. Appartiene a un vecchio progetto e risulta raggiungibile dalla rete dei server.	Individuare il responsabile; se non serve, spegnerla e archivarla; se serve, aggiornarla o isolarla in una rete a parte con regole minime.
R1-02	MEDIO	Venti dispositivi non in inventario	Otto computer, due stampanti, due macchine virtuali e otto dispositivi vari (display, lettori badge) sono collegati ma non sono nell'elenco. Per alcuni non si conosce il responsabile.	Associare ogni dispositivo a una persona; inserire nell'inventario; per quelli senza responsabile, scollegarli dopo un preavviso.
R1-03	BASSO	Cartellini dei punti presa non allineati	In tre armadi di piano, circa un punto presa su dieci ha un cartellino diverso dal nome nella tabella dello switch.	Rietichettare in una mezza giornata di lavoro, con il cablatore; mantenere la tabella come unica fonte.

Gli otto computer in più comprendono portatili degli ospiti e di tecnici esterni collegati ai piani. Gli identificatori dei dispositivi (indirizzi MAC) restano nel registro delle prove, non in questo documento.

NOTA · COME SI LEGGE IL NUMERO «+20»

Venti dispositivi su 1.045 sono meno del 2 %: per una sede di quattrocento persone è un risultato nella media. Il punto non è il numero, ma sapere **chi è responsabile** di ciascuno e perché è collegato.

Livello 2 · Topologia e instradamento

CAPITOLO 9 · PARTE B — LE SETTE ANALISI DI RETE

Il secondo livello verifica **come il traffico trova la strada**: collegamenti fisici e logici, instradamento verso Internet, comportamento delle coppie di apparati. Si confronta lo schema ufficiale con quello ricostruito dagli apparati. Sul bordo, verso i fornitori, si sono eseguiti solo controlli **in sola lettura**: nessuna rotta è stata annunciata, modificata o ritirata. Attività della giornata G2, con il referente tecnico presente e il fornitore reperibile.

0
CRITICI

0
ALTI

1
MEDIO

2
BASSI

2
INFORMATIVI E PUNTI
DI FORZA

9.1 La rete come la vediamo

Tratto	Che cosa abbiamo verificato	Esito
Linee e fornitori	Quattro sessioni BGP stabili, due per fornitore. Il blocco di indirizzi pubblici di Voltaria (203.0.113.0/24) e il numero di sistema autonomo (AS 64500) risultano annunciati da entrambi i fornitori.	✓ COME PROGETTATO
Filtri sul bordo	I router accettano dai fornitori solo i prefissi attesi e hanno un limite al numero di rotte ricevute per sessione.	✓ FORZA
Coppia di firewall	La commutazione tra attivo e passivo è documentata; lo stato delle sessioni VPN viene sincronizzato tra i due.	✓ COME PROGETTATO
Core e piani	Ogni piano ha due switch su core diversi, collegati fra loro. Il percorso di ogni piano verso il centro dati è doppio.	✓ COME PROGETTATO
Schema ufficiale	Quattro differenze rispetto allo schema di Voltaria (un collegamento tra switch non riportato, due etichette di porta, una rete non più in uso), corrette nello schema consegnato.	INFORMATIVO

✓ PUNTO DI FORZA

Filtri sui prefissi e limiti di rotte sul bordo (BGP): un errore di un fornitore, o un tentativo di annuncio indesiderato, non entra nella rete di Voltaria.

9.2 Rilievi

ID	Gravità	Titolo	Che cosa abbiamo osservato	Che cosa consigliamo
R2-01	MEDIO	Radice dello spanning tree non fissata	Lo switch che coordina la rete di ogni piano (la «radice») è scelto dagli apparati stessi e non da una regola del cliente: un apparato nuovo o ripristinato con impostazioni di fabbrica potrebbe diventare radice e deviare il traffico.	Fissare la radice con una priorità esplicita sui core, e la radice di riserva sul secondo core; attivare le protezioni delle porte di accesso.
R2-02	BASSO	Uscita su Internet sbilanciata	Le preferenze di uscita mandano quasi tutto il traffico sulle linee di un fornitore (Fibra Marmolada); l'altro fornitore (Rete Lavaredo) è usato soprattutto in caso di guasto.	Valutare un riparto del traffico per servizio (per esempio, VPN e posta su un fornitore, il resto sull'altro) dopo aver misurato il carico (capitolo 10).
R2-03	BASSO	Tre rotte statiche verso reti dismesse	Sul firewall restano tre rotte verso reti che non esistono più: non fanno danni oggi, ma confondono chi legge la configurazione.	Rimuoverle al prossimo intervento programmato, dopo averne verificato l'inutilità.

I controlli sulle sessioni BGP sono stati eseguiti con il consenso scritto di entrambi i fornitori e sono rimasti in sola lettura. Il consenso è parte della documentazione del kick-off.

Livello 3 · Prestazioni e capacità

CAPITOLO 10 · PARTE B — LE SETTE ANALISI DI RETE

Il terzo livello misura **quanto sono carichi i collegamenti e gli apparati** e quanto margine resta, in vista di nuovi servizi come il portale ordini che Voltaria aprirà a luglio. I dati vengono da due fonti: i contatori degli apparati su due settimane, e misure attive di velocità e ritardo in finestre concordate, a intensità limitata. Nessuna prova ha saturato una linea o un apparato in orario di lavoro.



10.1 Carico e margine

Collegamento o apparato	Capacità	Carico medio · picco	Commento
Linee Internet (4 × 1 Gbit/s)	4 Gbit/s	14 % · 61 % (in uscita)	Il picco è su una sola linea, nelle prime ore del pomeriggio, quando partono ordini e copie.
Dorsali core–piani (10 Gbit/s)	12 × 10	3 % · 11 %	Margine molto ampio.
Collegamento tra i due core	2 × 10	2 % · 7 %	Margine molto ampio.
Firewall (processore)	—	24 % · 71 %	Con il controllo delle intrusioni attivo e 40 VPN, il picco sale vicino alla soglia consigliata (70–75 %).
Ritardo piano–CED	—	< 1 ms	Nessuna differenza tra i piani.
Wi-Fi ospiti (2 punti)	—	fino a 14 dispositivi	Capacità adeguata alla sala d'attesa.

✓ PUNTO DI FORZA

Le dorsali tra core e piani e il collegamento tra i core lavorano a una piccola frazione della capacità: la rete interna può crescere molto senza intervenire.

10.2 Rilievi

ID	Gravità	Titolo	Che cosa abbiamo osservato	Che cosa consigliamo
R3-01	MEDIO	Margine ridotto sul firewall	Il processore del firewall arriva al 71 % nei picchi. Il portale ordini di luglio e le nuove VPN aumenteranno il carico.	Prima di luglio: misurare il carico con il portale in prova; valutare la sostituzione con un modello più potente o lo spostamento del controllo delle intrusioni; calcolare il margine con almeno il 30 % di crescita.
R3-02	BASSO	Qualità del servizio per le telefonate non uniforme	Sui piani 2 e 5 le telefonate non hanno la priorità sul traffico dati: ora non si nota, ma si noterebbe in un picco.	Applicare la stessa regola di priorità su tutti gli switch di piano.

Livello 4 · Sicurezza e segmentazione

CAPITOLO 11 · PARTE B — LE SETTE ANALISI DI RETE

Il quarto livello guarda **come la rete è divisa in zone e chi può parlare con chi**. Una buona segmentazione limita i danni: se un dispositivo viene compromesso, non arriva dappertutto. Qui si esaminano le regole dei firewall, le reti virtuali (VLAN) e le interfacce di gestione, **leggendo le configurazioni**, senza provare nulla. Le prove vere, dall'interno, si fanno nella parte C del documento. Attività delle giornate G2 e G5.

O
CRITICI

I
ALTO

2
MEDI

I
BASSO

2
PUNTI DI FORZA

11.1 Le zone e chi può parlare con chi

La tabella mostra i flussi consentiti tra le zone, come risultano dalle regole in vigore. **Si**: consentito per scelta. **No**: bloccato.

Eccezione: consentito oltre l'intenzione di progetto (vedi i rilievi).

Da → verso	UTENTI	VOCE	STAMPANTI	TELECAMERE	OSPITI	SERVER	GESTIONE	DMZ	INTERNET
UTENTI	—	No	Sì	No	No	Sì	Eccezione	Sì	Sì
VOCE	No	—	No	No	No	Sì (telefonia)	No	No	Sì (linee)
STAMPANTI	Sì (risposte)	No	—	No	No	Sì (code)	No	No	No
TELECAMERE	No	No	No	—	No	Sì (registratore)	Eccezione	No	No
OSPITI	No	No	No	No	—	No	No	No	Sì
SERVER	Sì (risposte)	Sì	No	Sì (registratore)	No	—	Sì	Sì	Sì
DMZ	No	No	No	No	No	Sì (solo servizi)	No	—	Sì

✓ PUNTI DI FORZA

- **Zone ben pensate.** Voce, stampanti, telecamere e ospiti sono su reti separate, con regole di partenza «nega tutto» e aperture esplicite.
- **DMZ isolata.** La zona dei servizi pubblici può raggiungere i server solo sui servizi necessari e non raggiunge le reti degli utenti.

11.2 Rilievi

ID	Gravità	Titolo	Che cosa abbiamo osservato	Che cosa consigliamo
R4-01	ALTO	Rete di gestione raggiungibile dagli utenti	Una regola consente alla rete utenti di raggiungere le interfacce di amministrazione di server e apparati (sistema di backup compreso). Era un'apertura temporanea, rimasta in vigore. È la causa di fondo del rilievo PT-01.	Subito: restringere l'accesso a due postazioni di amministrazione. Poi: rete di gestione separata, raggiungibile solo da lì.
R4-02	MEDIO	Porta di gestione del registratore video verso la rete dati	Il registratore video ha due porte: una sulla rete telecamere, una sulla rete dati per la gestione. Così la rete telecamere ha un percorso verso la rete dati. Verificato in pratica con il rilievo PT-07.	Spostare la gestione del registratore sulla rete di gestione; regola esplicita tra le due reti; non lasciare altre porte.
R4-03	MEDIO	Nessuna autenticazione dei dispositivi sulle porte di accesso	Chi collega un dispositivo a una presa ottiene una rete in base alla porta, senza che il dispositivo si identifichi. Se un dispositivo è sostituito o un apparato rimane indietro, nessun controllo lo segnala.	Introdurre l'autenticazione dei dispositivi sulle porte (802.1X) a fasi: prima i piani con più ospiti, poi gli altri.
R4-04	BASSO	Regole inutilizzate sui firewall	Ventitré regole su 187 non hanno traffico da oltre sei mesi, e molte non hanno una descrizione.	Pulizia: disattivare, osservare un mese, rimuovere; descrizione obbligatoria per ogni regola.

Livello 5 · Configurazioni e aggiornamenti

CAPITOLO 12 · PARTE B — LE SETTE ANALISI DI RETE

Il quinto livello controlla **come sono impostati gli apparati e quanto sono aggiornati**. Una configurazione corretta oggi può diventare un problema domani, se un aggiornamento di sicurezza non arriva su un apparato: per questo si guardano insieme le impostazioni, le versioni del software e il modo in cui gli aggiornamenti vengono distribuiti. Attività delle giornate G2 e G5, sulle configurazioni salvate e sulle versioni dichiarate dagli apparati, senza modificarle.



12.1 Versioni del software degli apparati

Le versioni sono state lette dagli apparati e confrontate con la versione di riferimento che Voltaria si è data (l'ultima con le correzioni di sicurezza note). I numeri sono in forma generica; il dettaglio è nel registro delle prove.

Famiglia	Apparati	Allineati	Note
Core	2	2 di 2	Aggiornati in finestra di manutenzione a gennaio.
Switch di piano	12	11 di 12	Lo switch del piano 4 è indietro di una versione di sicurezza (rilievo R5-01).
Firewall e router di bordo	4	4 di 4	—
Server di posta in DMZ	1	0 di 1	Aggiornamenti arretrati di quattro mesi (rilievo R5-02).
Altri server e ipervisor	3 + 19 VM	20 su 22	Due macchine virtuali non aggiornate; una è quella del rilievo R1-01.
Stampanti	62	41 di 62	Firmware vecchio: tema trattato anche nel penetration test (PT-02).

12.2 Rilievi

ID	Gravità	Titolo	Che cosa abbiamo osservato	Che cosa consigliamo
R5-01	ALTO	Aggiornamento degli switch senza controllo di completezza	Gli switch di piano si aggiornano con una procedura programmata. Lo switch del piano 4 era spento per manutenzione al momento dell'ultimo aggiornamento e non lo ha ricevuto; la procedura non ha segnalato l'apparato non raggiunto né ha ritentato. Il rilievo è provato in pratica dal PT-03 (capitolo 16).	La procedura deve riportare gli apparati non raggiunti, ritentare, e produrre un rapporto per l'IT; confronto automatico con la versione di riferimento; controllo mensile con verbale.
R5-02	MEDIO	Aggiornamenti arretrati sul server di posta	Il server di posta in DMZ ha quattro mesi di aggiornamenti di sicurezza non applicati; non ha una finestra di manutenzione programmata.	Finestra mensile concordata con l'azienda; applicare subito quelli critici; prova su una copia prima di produzione.
R5-03	MEDIO	Account di amministrazione condiviso	Sugli apparati di rete si usa un account di amministrazione unico, conosciuto da cinque persone: non si capisce chi ha fatto che cosa.	Account personali, con autenticazione centralizzata; account di emergenza custodito e usato solo in caso di bisogno.
R5-04	BASSO	Gestione SNMP con parametri predefiniti su alcuni apparati	Sei apparati (stampanti e un gruppo di continuità) rispondono con la parola di accesso di fabbrica al protocollo di monitoraggio.	Passare alla versione con autenticazione e cifratura; disattivare dove non serve.
R5-05	BASSO	Registri degli apparati non centralizzati	I registri sono conservati su ogni apparato per circa 30 giorni, e non in un archivio comune.	Archivio centralizzato con conservazione di almeno 12 mesi e avvisi sugli eventi importanti.

✓ PUNTO DI FORZA

Le configurazioni di tutti gli apparati di rete vengono salvate ogni notte con cronologia delle modifiche: in caso di guasto o di errore si torna indietro in pochi minuti. Questa buona pratica ha permesso il ripristino rapido previsto dal piano di recovery (capitolo 4).

Livello 6 · Affidabilità e continuità

CAPITOLO 13 · PARTE B — LE SETTE ANALISI DI RETE

Il sesto livello misura quanto la rete continua a funzionare quando qualcosa si rompe, e in quanto tempo torna normale. Si guardano la ridondanza degli apparati, delle linee, dell'alimentazione, dei percorsi fisici e dei dati. Per Voltaria il quadro è buono: i guasti singoli sono quasi tutti coperti. I margini di miglioramento riguardano soprattutto gli eventi che colpiscono **tutto il centro dati insieme**.



✓ PUNTI DI FORZA

- **Accesso a Internet.** Quattro linee su due fornitori e due anelli ciascuno, con BGP: la perdita di una linea, di un anello o di un intero fornitore non cambia gli indirizzi pubblici di Voltaria.
- **Apparati.** Router di bordo, firewall e core in coppia; doppio alimentatore ovunque.
- **Piani.** Due switch per piano, su core diversi e collegati fra loro: la caduta di un core non isola il piano.
- **Percorsi fisici.** Due cavedi REI120 distinti per la fibra: un guasto fisico in uno non interrompe l'altro.

13.1 Rilievi

ID	Gravità	Titolo	Che cosa abbiamo osservato	Che cosa consigliamo
R6-01	ALTO	Centro dati in un solo locale	Core, firewall, server e backup stanno nella stessa sala: un evento locale (incendio, allagamento, guasto del condizionamento o dell'impianto elettrico) fermerebbe tutto, nonostante i doppi apparati.	Piano di continuità; una sala secondaria per i servizi essenziali e per le copie; nel breve, rilevazione fumo e allagamento e una copia dei dati fuori sede.
R6-02	ALTO	Backup nella stessa sala dei server	Le copie sono solo nel CED, senza copia fuori sede né copia non modificabile. L'ultima prova di ripristino completo risale a 14 mesi fa.	Regola 3-2-1 (tre copie, due supporti, una fuori sede); copia cifrata fuori sede; copia non modificabile; prova di ripristino ogni trimestre.
R6-03	MEDIO	Doppia alimentazione sulla stessa linea	I due alimentatori dei core sono collegati a PDU alimentate dallo stesso UPS: proteggono dal guasto dell'alimentatore, non da quello dell'UPS o della linea elettrica.	Due linee elettriche indipendenti (A e B) con UPS distinti; prova periodica di stacco di una linea.
R6-04	MEDIO	Dispositivi con un solo collegamento	Telefoni IP, stampanti e computer hanno un solo cavo: se uno switch di piano si guasta, perdono la rete i dispositivi collegati a quello. Lo switch gemello protegge dal guasto del core, non dallo switch del singolo dispositivo.	Ripartire i punti critici (reception, sale riunioni, stampanti, telefoni della direzione) tra lo switch A e lo switch B; tenere uno switch di scorta già configurato.
R6-05	BASSO	Prove di failover non ripetute	L'ultima prova documentata di commutazione tra core, firewall e router di bordo risale a più di 12 mesi fa.	Calendario di prove almeno annuale, in finestra protetta, con verbale.
R6-06	INFORMATIVO	Tratte spare etichettate	Le tratte di scorta nei cavedi esistono e sono etichettate: utile per i guasti e per il cablaggio dei test.	Mantenere la documentazione aggiornata.

13.2 Un rilievo in dettaglio

R6-01 ALTO Centro dati in un solo locale	
CHE COSA	Tutti gli apparati che reggono la rete e i dati (core, firewall, server, backup, accesso di test) sono nello stesso locale, al piano interrato.
PERCHÉ CONTA	La ridondanza degli apparati protegge dal guasto di un componente. Non protegge da un evento che colpisce il locale intero : in quel caso i due core, i due firewall e le copie di backup sono fuori uso insieme.
COME L'ABBIAMO VERIFICATO	Sopralluogo al CED (G1), esame dello schema elettrico, della documentazione dell'impianto antincendio e della posizione dei sistemi di backup.
IMPATTO	Fermo totale della sede e delle agenzie per un tempo legato al ripristino dei locali e dei dati: giorni, non ore.
CHE COSA CONSIGLIAMO	Subito : rilevazione fumo e allagamento con allarme; copia dei dati fuori sede. Entro 6 mesi : sala secondaria, anche piccola, nell'edificio o altrove, con i servizi essenziali e una copia aggiornata. Piano di continuità con obiettivi di ripristino dichiarati.
SFORZO E PRIORITÀ	Intervento breve: basso. Sala secondaria: medio-alto. Priorità alta (correzione entro 30 giorni per gli interventi brevi).

Livello 7 · Piano di intervento

CAPITOLO 14 · PARTE B — LE SETTE ANALISI DI RETE

L'ultimo livello mette in ordine ciò che i sei precedenti hanno trovato: **che cosa fare per primo, che cosa dopo, chi lo fa e quanto costa in impegno**. È un piano di miglioramento della rete, in prospettiva più ampia di quello dei soli rilievi di sicurezza (capitolo 22, dopo il penetration test). I due piani sono coordinati: alcune azioni compaiono in entrambi e si fanno una volta sola.

14.1 I numeri delle sette analisi e del test

Parte	CRITICI	ALTI	MEDI	BASSI	INFO · FORZA	Totale
Livello 1 · Rilevamento e inventario	0	1	1	1	1	4
Livello 2 · Topologia e instradamento	0	0	1	2	2	5
Livello 3 · Prestazioni e capacità	0	0	1	1	1	3
Livello 4 · Sicurezza e segmentazione	0	1	2	1	2	6
Livello 5 · Configurazioni e aggiornamenti	0	1	2	2	1	6
Livello 6 · Affidabilità e continuità	0	2	2	1	1	6
Sette analisi	0	5	9	8	8	30
Penetration test (capitolo 20)	1	3	4	3	5	16
Totale	1	8	13	11	13	46

Il livello 7 è questo piano: non produce rilievi propri. Le sigle R1-... R6-... indicano i rilievi dei livelli; PT-... quelli del penetration test.

14.2 Che cosa fare, e quando

Quando	Rilievi	Azione	Chi	Impegno
SUBITO · 72 ORE	PT-01 · R4-01	Cambiare le credenziali della console del backup; limitare la gestione a due postazioni di amministrazione.	Referente tecnico	Basso
SUBITO · 72 ORE	PT-03 · R5-01	Aggiornare lo switch del piano 4; verificare le versioni di tutti gli apparati di piano; controllare i registri.	Team IT	Basso
SUBITO · 72 ORE	R1-01	Isolare la macchina virtuale con sistema non più supportato, in attesa di decidere se tenerla.	Team IT	Basso
ENTRO 30 GIORNI	PT-02 · PT-04 · R5-02	Credenziali delle stampanti; aggiornamenti del server di posta con finestra mensile.	Team IT	Basso
ENTRO 30 GIORNI	R5-01	Procedura di aggiornamento che segnala gli apparati non raggiunti; rapporto per l'IT.	Team IT	Medio
ENTRO 30 GIORNI	R6-02	Copia dei backup fuori sede, cifrata; copia non modificabile.	Referente tecnico	Medio
ENTRO 30 GIORNI	R1-01 · R1-02	Dismettere o aggiornare la macchina virtuale; associare un responsabile a ciascun dispositivo non in elenco.	Team IT	Basso
ENTRO 90 GIORNI	PT-05 · PT-06 · PT-07 · PT-08	Algoritmi delle VPN; isolamento del Wi-Fi ospiti; gestione del registratore video; account di servizio con scadenza.	Team IT	Medio
ENTRO 90 GIORNI	R2-01 · R3-01 · R5-03	Radice dello spanning tree fissata; prova di carico del firewall prima di luglio; account personali sugli apparati.	Team IT	Medio
ENTRO 90 GIORNI	R4-02 · R4-03	Rete di gestione separata; avvio dell'autenticazione dei dispositivi sulle porte (primo piano pilota).	Team IT + consulente	Alto
ENTRO 6 MESI	R6-01 · R6-03	Rilevazione fumo e allagamento; sala secondaria per i servizi essenziali; seconda linea elettrica con UPS distinto.	Sponsor + impianti	Alto
ENTRO 6 MESI	R5-04 · R5-05 · R3-02	Gestione SNMP sicura; archivio centrale dei registri; stessa priorità voce su tutti i piani.	Team IT	Medio
ENTRO 12 MESI	R2-02 · R6-04 · R6-05	Riparto del traffico tra i fornitori; punti critici ripartiti tra switch A e B; prove di failover annuali e di ripristino ogni trimestre.	Team IT	Medio

DA DECIDERE · CHE COSA PORTA PIÙ VALORE PER PRIMO

Le azioni «Subito» e «Entro 30 giorni» costano poche ore e riducono in modo evidente il rischio: proteggono i backup, il centro dei piani e i servizi pubblici. Gli interventi di architettura (sala secondaria, rete di gestione, autenticazione dei dispositivi) hanno un impegno maggiore e conviene programmarli con un budget dedicato, dopo la verifica del 8 luglio.

Perimetro esterno

CAPITOLO 15 · PARTE C — IL PENETRATION TEST (EFESTO, LIVELLO AVANZATO)

Il penetration test comincia da fuori: **che cosa vede e che cosa può provare chiunque da Internet**. L'obiettivo è sapere se gli indirizzi pubblici di Voltaria, i servizi in DMZ e le VPN delle agenzie reggono a un tentativo realistico, senza mai superare i limiti del kick-off. Attività delle giornate G3 (solo osservazione dall'esterno) e G4 (bordo, firewall e VPN, con controlli di configurazione in sola lettura).

STRUMENTI E ATTIVITÀ BONET™ · COME SI LAVORA DALL'ESTERNO

Le prove partono dal punto di osservazione esterno (H4, un server in un data center in Italia con indirizzo fisso, concordato al kick-off): Voltaria sa da dove arrivano e può riconoscerle. Intensità limitata, una prova alla volta, nessun tentativo di saturazione. Ogni sessione inizia e finisce con una comunicazione al referente tecnico.

15.1 Che cosa si è provato

Area	Perimetro e consenso	Che cosa si è fatto
Indirizzi pubblici	Blocco 203.0.113.0/24; consenso dei due fornitori (lettere del 21 aprile).	Rilevamento di indirizzi, porte e servizi raggiungibili; confronto con l'elenco dei servizi pubblicati.
Posta e sito	Server di posta e web in DMZ.	Controllo di versioni, certificati, impostazioni di sicurezza e aggiornamenti dichiarati.
VPN delle agenzie	Concentratore in DMZ; solo il lato sede (le reti delle 40 agenzie sono fuori perimetro).	Verifica di algoritmi, parametri di cifratura e criteri di accesso.
Bordo (BGP)	Router di bordo; solo lettura.	Controllo dei filtri e dei limiti di rotte; nessun annuncio né ritiro di rotte.
Firewall	Coppia di firewall in alta affidabilità.	Confronto delle regole in vigore con la documentazione; verifica delle zone.
DMZ	Zona intermedia verso la rete interna.	Verifica che i servizi pubblici non raggiungano le reti interne oltre il necessario.

15.2 Che cosa è emerso

ID	Gravità	Titolo	Che cosa significa
PT-04	ALTO	Server di posta in DMZ con aggiornamenti di sicurezza arretrati	Quattro mesi di correzioni non applicate su un servizio raggiungibile da Internet: chi conosce le correzioni mancanti ha un punto di partenza. Nessuno sfruttamento è stato tentato su questo servizio: il rilievo si basa sulla versione e sulle correzioni mancanti.
PT-05	MEDIO	VPN delle agenzie con algoritmi di cifratura datati	Il concentratore accetta ancora impostazioni oggi sconsigliate, per compatibilità con apparati vecchi di alcune agenzie.
PT-09	BASSO	Servizi web che rivelano nome e versione del software	L'informazione aiuta chi cerca punti deboli noti. Facile da nascondere.
PT-12	✓ FORZA	Filtri sui prefissi BGP corretti	Il bordo accetta solo ciò che deve.
PT-13	✓ FORZA	Firewall: regole documentate e coerenti con le zone	Il comportamento osservato coincide con la documentazione.
PT-15	✓ FORZA	DMZ separata correttamente dalla rete interna	Dai servizi pubblici non si raggiungono le reti degli utenti.

NOTA · SERVIZI PUBBLICATI

Undici servizi sono raggiungibili da Internet: tutti presenti nell'elenco e tutti attesi. Nessun servizio inatteso, nessuna interfaccia di amministrazione esposta. Questo dato è un punto di forza del perimetro e giustifica il giudizio complessivo positivo del capitolo 20.

CHE COSA NON SI È FATTO

Nessuna prova di negazione del servizio o di saturazione; nessun tentativo di indovinare password sui servizi pubblicati; nessuna modifica di rotte BGP; nessuna prova sulle reti delle agenzie; nessuna ingegneria sociale.

Rete interna e piani

CAPITOLO 16 · PARTE C — IL PENETRATION TEST (EFESTO, LIVELLO AVANZATO)

La seconda domanda è: **che cosa può fare un dispositivo già dentro la rete**, per esempio il computer di un dipendente, di un ospite o di un tecnico esterno collegato a una presa. Per rispondere, l'unità di test nel CED raggiunge sei switch di piano scelti dal cliente (T1–T6) con collegamenti dedicati, e da lì si prova, in modo controllato, ciò che un dispositivo collegato a quel punto vedrebbe. Attività delle giornate G5 (dal CED), G6, G7 e G8 (piani, fuori orario).

16.1 I sei punti sotto test

Punto	Piano	Giornata	Finestra	Esito
T1	Piano 1	G6	20:30–2:00	Nessuna anomalia oltre i rilievi PT-10, PT-11
T2	Piano 2	G6	20:30–2:00	Nessuna anomalia oltre i rilievi PT-10, PT-11
T3	Piano 3	G7	20:30–2:00	PT-01 (accesso alla rete del backup, capitolo 18)
T4	Piano 4	G7	20:30–2:00	ALTO PT-03 (switch indietro di versione)
T5	Piano 5 · switch A	G8	22:00–4:00	Failover verificato (PT-14)
T6	Piano 5 · switch B	G8	22:00–4:00	Failover verificato (PT-14)

Per lo switch del piano 3, privo di porta in fibra libera, si usa un adattatore su una porta di accesso (studio di fattibilità, capitolo 6). Le finestre sono quelle approvate al kick-off; in ognuna sono presenti il responsabile di progetto BoNet™ e un referente IT di Voltaria.

16.2 Che cosa è emerso

ID	Gravità	Titolo	Che cosa significa
PT-03	ALTO	Switch di piano rimasto senza aggiornamento dopo una manutenzione: una postazione ottiene un accesso non previsto	Il punto debole non è un apparato guasto ma un passaggio del processo: l'aggiornamento periodico non ha raggiunto uno switch spento per manutenzione e nessun controllo lo ha segnalato. Scheda completa al capitolo 20.
PT-10	BASSO	Protocolli di risoluzione dei nomi locali attivi senza necessità	Servizi di ricerca dei nomi che i computer usano quando non trovano un nome nei sistemi principali: oggi utili a pochi, possono essere sfruttati per intercettare richieste.
PT-11	BASSO	Interfaccia web dei telefoni IP raggiungibile dalla rete dati	La pagina di gestione di ogni telefono si apre dai computer; senza password robusta potrebbe essere usata impropriamente.
PT-14	✓ FORZA	Failover tra gli switch A e B funzionante come progettato	Vedi sotto.

16.3 La prova di failover al piano 5 (G8)

È la prova a rischio più alto della parte interna, per questo si svolge in finestra protetta (22:00–4:00), con il piano di recovery già aperto, il responsabile di progetto BoNet™ in loco, il referente IT e l'elettricista reperibile. Si è **spento in modo ordinato** uno dei due switch del piano (A), con il consenso del referente tecnico, e si è osservato che cosa succedeva ai dispositivi collegati, poi si è fatto lo stesso con l'altro (B).

Che cosa si è osservato	Risultato
I dispositivi collegati a entrambi gli switch tramite doppio collegamento rimangono raggiungibili	✓ COME PROGETTATO

Che cosa si è osservato	Risultato
Tempo di commutazione dei collegamenti tra i core	circa 3 secondi
I telefoni IP e i computer con un solo collegamento sullo switch spento perdono la rete fino al ripristino	ATTESO (R6-04)
Ritorno allo stato iniziale, con verifica delle sessioni, dei telefoni e delle stampanti	✓ RIUSCITO

RECOVERY · NESSUNO STOP

La giornata G8 si è conclusa senza che si attivasse alcuna condizione di stop. L'ultimo passo è stato il controllo, con il referente IT, dei dispositivi del piano 5 alla riapertura degli uffici.

CHE COSA NON SI È FATTO

Nessuna modifica alle configurazioni degli switch o dei core; nessuna prova che saturi collegamenti; nessuna lettura di contenuti di computer, telefoni o stampanti; nessuna prova fuori dalle finestre.

Wi-Fi ospiti, telecamere, stampanti

CAPITOLO 17 · PARTE C — IL PENETRATION TEST (EFESTO, LIVELLO AVANZATO)

Wi-Fi per gli ospiti, telecamere e stampanti hanno una cosa in comune: sono dispositivi **che si dimenticano facilmente**, spesso con impostazioni di fabbrica. Per questo si provano insieme, nella giornata G9, in orario ridotto (Wi-Fi e stampanti di giorno, telecamere in finestra concordata con il responsabile della sicurezza fisica). Non si è toccata alcuna ripresa video né alcun documento in coda di stampa.

17.1 Che cosa si è provato

Area	Che cosa si è verificato	Esito
WI-FI OSPITI	Separazione della rete ospiti dalla rete interna; visibilità tra dispositivi ospiti; pagina di accettazione e durata dell'accesso.	Separazione ok; PT-06
STAMPANTI	Interfacce di amministrazione su un campione di 60 stampanti dei piani 1-5: credenziali, servizi attivi, firmware.	PT-02
TELECAMERE	Isolamento della rete telecamere; interfacce di gestione del registratore e delle telecamere; percorsi verso la rete dati.	PT-07

17.2 Che cosa è emerso

ID	Gravità	Titolo	Che cosa significa
PT-02	ALTO	Stampanti con credenziali di amministrazione predefinite	Su 14 stampanti su 60 le credenziali del costruttore sono ancora valide. Le stampanti conservano rubriche e, a volte, documenti: sono un punto di appoggio per chi si muove nella rete. Scheda completa al capitolo 20.
PT-06	MEDIO	Wi-Fi ospiti senza isolamento tra i dispositivi collegati	La rete interna di Voltaria non è raggiungibile dagli ospiti, ma gli ospiti si vedono tra loro. Scheda al capitolo 20.
PT-07	MEDIO	La rete telecamere raggiunge la rete dati attraverso una porta di gestione	Il registratore video ha una seconda porta sulla rete dati. Non è stato aperto alcun flusso video: si è verificato solo il percorso. Conferma il rilievo R4-02.

✓ PUNTI DI FORZA

La rete ospiti è separata dalla rete interna come progettato. Le telecamere non sono raggiungibili da Internet e non comunicano tra loro in modo non previsto. Le stampanti stanno su una rete dedicata e rispondono solo ai server di stampa e agli utenti.

CHE COSA NON SI È FATTO

Nessuna visione di riprese o di documenti stampati; nessuna modifica delle impostazioni di stampanti e telecamere (le credenziali predefinite sono state verificate solo con un accesso breve e subito chiuso, su due stampanti scelte dall'IT); nessuna prova di intercettazione di altri ospiti sul Wi-Fi.

Servizi e backup

CAPITOLO 18 · PARTE C — IL PENETRATION TEST (EFESTO, LIVELLO AVANZATO)

Questa è la parte che interessa di più al titolare: **i servizi da cui dipende il lavoro di tutti** (posta, file, directory degli utenti, gestionali) e **le copie di sicurezza** da cui si ripartirebbe dopo un guasto o un attacco. Attività della giornata G10, in orario di lavoro, senza modificare nulla, con il referente tecnico presente. Il capitolo 13 aveva già mostrato i limiti della continuità; qui si vede se, da dentro la rete, le copie sono davvero al sicuro.

18.1 Che cosa si è verificato

Area	Che cosa si è verificato	Esito
Directory degli utenti	Stato di salute dell'elenco degli utenti e dei gruppi; account di servizio; criteri delle password; percorsi di privilegio.	PT-08
Posta e file	Controlli di accesso ai servizi interni e alle condivisioni; esposizione dall'interno.	Nessun rilievo aggiuntivo
Gestionali	Accesso ai portali e ai servizi di database, solo nella parte di autenticazione; nessuna lettura di dati.	Nessun rilievo aggiuntivo
Sistema di backup	Raggiungibilità della console di amministrazione dalla rete utenti; credenziali; stato delle copie; isolamento dalla rete di produzione.	PT-01

18.2 Che cosa è emerso

ID	Gravità	Titolo	Che cosa significa
PT-01	CRITICO	Console del sistema di backup raggiungibile dalla rete utenti con credenziali deboli	Chi arrivasse a quella console potrebbe cancellare o alterare le copie di sicurezza. È l'unico rilievo critico, ed è tale perché mette a rischio la possibilità di ripartire dopo un incidente. Scheda completa al capitolo 20; prova controllata al capitolo 19.
PT-08	MEDIO	Account di servizio della directory con password che non scade	Account usati da programmi e non da persone, con password mai cambiate da anni: se la password venisse scoperta, l'accesso resterebbe valido a lungo.

18.3 Lo stato delle copie

La **prova di ripristino del 20-21 aprile**, eseguita da Voltaria come condizione preliminare dell'incarico, è riuscita: i dati dell'ultima copia si sono ripristinati in ambiente separato. La prova precedente risaliva a quattordici mesi prima (rilievo R6-02). Le copie sono tutte nel centro dati e nessuna è non modificabile: perciò la console di backup raggiungibile dagli utenti (PT-01) è critica.

RECOVERY · IL BACKUP PRIMA DI TUTTO

La giornata G10 era subordinata alla prova di ripristino riuscita (condizione 1 dello studio). Se la prova fosse fallita, il test non sarebbe partito: nessun incarico invasivo comincia senza sapere di poter ripristinare.

CHE COSA NON SI È FATTO

Nessuna lettura di caselle di posta, documenti o dati dei gestionali; nessuna modifica o cancellazione di copie di backup; nessun tentativo di indovinare password sugli account della directory; nessun ripristino dai dati di produzione durante il test.

Sfruttamento controllato e verifica dell'impatto

CAPITOLO 19 · PARTE C — IL PENETRATION TEST (EFESTO, LIVELLO AVANZATO)

Alcuni rilievi si possono dimostrare solo provando fino a un certo punto che cosa accadrebbe davvero. È la parte più delicata dell'incarico: per questo avviene nella giornata G11, **una prova alla volta**, soltanto per punti già emersi nelle giornate precedenti, con il consenso scritto del referente tecnico per ciascuna e con il responsabile di progetto BoNet™ in loco. Lo scopo non è «entrare»: è **misurare l'impatto con la minima prova possibile**, poi fermarsi.

STRUMENTI E ATTIVITÀ BONET™ · GLI STRUMENTI DI QUESTA GIORNATA

Gli strumenti per queste prove non sono elencati nel capitolo 5: si scelgono caso per caso e si concordano al kick-off, una prova alla volta. Nessuno di essi è usato fuori dalla finestra e dal perimetro approvati.

19.1 Le tre prove della giornata

Prova	Rilievo	Che cosa si è dimostrato	Che cosa non si è toccato
1	PT-01 Console del backup	Accesso alla console con una credenziale deducibile da elenchi di password diffuse, dalla porta di accesso del piano 3. Accesso chiuso subito.	Nessuna copia letta, modificata o cancellata; nessuna impostazione cambiata.
2	PT-03 Switch del piano 4	Dal punto T4, una postazione collegata ha raggiunto una rete diversa da quella assegnata, verso un sistema di prova indicato dal referente tecnico.	Nessun altro sistema; nessun dato letto; nessuna configurazione modificata.
3	PT-02 Stampanti	Accesso all'interfaccia di amministrazione di due stampanti scelte dall'IT, con la credenziale predefinita del costruttore. Accesso chiuso subito.	Nessun documento, nessuna rubrica letti; nessuna impostazione cambiata.

19.2 Come si svolge ogni prova

1. **Consenso.** Il referente tecnico firma, su un modulo dedicato, la prova che sta per iniziare: punto, rilievo, finestra, che cosa si toccherà e che cosa no.
2. **Piano di recovery aperto.** Si rilegge lo scenario della prova e chi interviene.
3. **Prova minima.** Si dimostra il rilievo con il minimo indispensabile; nessun dato viene letto o copiato, nessuna modifica resta.
4. **Evidenza.** Data, ora, operatore e impronta (SHA-256) nel registro delle prove; nessun contenuto personale.
5. **Stop e verifica.** Si chiude l'accesso, si verifica che tutto sia come prima e si firma la chiusura della prova.

✓ ESITO DELLA GIORNATA

Nessuna condizione di stop attivata; nessun servizio ha mostrato anomalie; nessun allarme da parte del sistema di monitoraggio di Voltaria. L'IT interno **non ha rilevato** le prove 1 e 3: è un'informazione utile, perché indica che il monitoraggio degli accessi alle console e alle stampanti può migliorare (raccomandazione nel piano di rimedio).

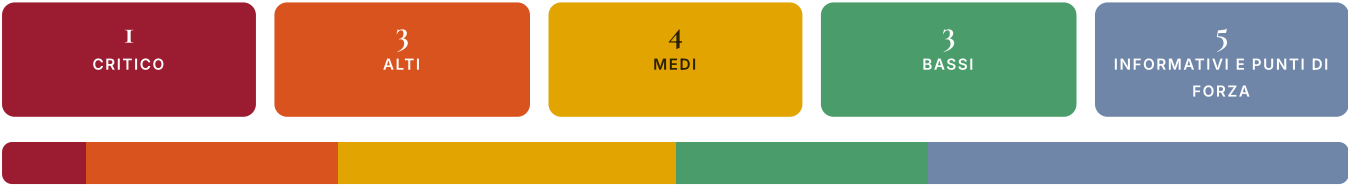
CHE COSA NON SI È FATTO, MAI

Nessuna prova di negazione del servizio; nessun accesso persistente lasciato sui sistemi; nessuna modifica o cancellazione di dati del cliente; nessuna esfiltrazione di contenuti; nessuna prova fuori dal perimetro approvato; nessun tentativo di eludere il monitoraggio di Voltaria.

Rilievi del penetration test

CAPITOLO 20 · PARTE C — EFESTO, LIVELLO AVANZATO

Il penetration test ha provato, in modo controllato e autorizzato, se i punti deboli individuati potessero essere sfruttati davvero, e che cosa ne sarebbe seguito. Il risultato è positivo sul perimetro (firewall, BGP, DMZ e separazione delle reti sono ben impostati) e mostra pochi punti su cui intervenire con priorità, quasi tutti all'**interno** della rete; uno riguarda una **procedura** (l'aggiornamento degli switch di piano) più che un singolo apparato. Tutti i rilievi sono stati provati senza leggere né modificare i dati del cliente.



20.1 Quadro riassuntivo

ID	Gravità	Titolo	Dove	Scheda
PT-01	CRITICO	Console del sistema di backup raggiungibile dalla rete utenti con credenziali deboli	CED · rete utenti	§ 20.2
PT-02	ALTO	Stampanti con credenziali di amministrazione predefinite	Piani 1-5	§ 20.2
PT-03	ALTO	Switch di piano rimasto senza aggiornamento dopo una manutenzione: una postazione ottiene un accesso non previsto	Piano 4 · T4	§ 20.2
PT-04	ALTO	Server di posta in DMZ con aggiornamenti di sicurezza arretrati	DMZ	Doc. completo
PT-05	MEDIO	VPN delle agenzie con algoritmi di cifratura datati	Firewall	Doc. completo
PT-06	MEDIO	Rete Wi-Fi ospiti senza isolamento tra i dispositivi collegati	Piano terra	§ 20.2
PT-07	MEDIO	La rete telecamere raggiunge la rete dati attraverso una porta di gestione	CED	Doc. completo
PT-08	MEDIO	Account di servizio della directory con password che non scade	CED · directory	Doc. completo
PT-09	BASSO	I servizi web in DMZ rivelano nome e versione del software	DMZ	Doc. completo
PT-10	BASSO	Protocolli di risoluzione dei nomi locali attivi senza necessità	Rete utenti	Doc. completo
PT-11	BASSO	Interfaccia web dei telefoni IP raggiungibile dalla rete dati	Piani 1-5	Doc. completo
PT-12	✓ FORZA	Router di bordo: filtri sui prefissi BGP corretti	Bordo	Doc. completo
PT-13	✓ FORZA	Firewall: regole documentate e coerenti con le zone	Firewall	Doc. completo
PT-14	✓ FORZA	Failover tra gli switch A e B funzionante come progettato (G8)	Piano 5	Doc. completo
PT-15	✓ FORZA	DMZ separata correttamente dalla rete interna	DMZ	Doc. completo
PT-16	INFORMATIVO	Cavedi REI120 e passaggi: nessuna anomalia riscontrata	Cavedi	Doc. completo

20.2 Quattro schede come esempio

PT-01	CRITICO	Console del backup raggiungibile dalla rete utenti con credenziali deboli
DOVE	Sistema di backup nel CED; prova eseguita dalla porta di accesso del piano 3 (punto T3), giornata G7/G10.	
CHE COSA ABBIAMO OSSERVATO	L'interfaccia di amministrazione del sistema di backup è raggiungibile da qualunque computer della rete utenti. Le credenziali di amministrazione sono risultate tra quelle più comuni.	
PROVA	Accesso eseguito alla console con una credenziale deducibile da elenchi di password diffuse. Non è stato letto né modificato alcun dato ; l'accesso è stato chiuso subito. Evidenza EV-031, con data, ora e impronta nel registro delle prove.	
IMPATTO	Chi ottenesse questo accesso potrebbe cancellare o alterare le copie di sicurezza. Unito al rilievo R6-02, il ripristino dopo un attacco o un guasto sarebbe a rischio.	
CHE COSA CONSIGLIAMO	Subito (entro 72 ore) : cambiare le credenziali; limitare l'accesso alla console a due postazioni di amministrazione. Entro 30 giorni : autenticazione a più fattori; rete di gestione separata; copia non modificabile.	
VERIFICA SUCCESSIVA	Ripetizione della prova a 30 giorni (8 luglio 2026).	

PT-02	ALTO	Stampanti con credenziali di amministrazione predefinite
DOVE	Rete stampanti, piani 1-5; prova dai punti T1-T6.	
CHE COSA ABBIAMO OSSERVATO	Su 14 delle 60 stampanti l'interfaccia di amministrazione accetta le credenziali fornite dal costruttore.	
IMPATTO	Le stampanti conservano documenti e rubriche, e sono spesso un punto di appoggio per chi cerca di muoversi nella rete.	
CHE COSA CONSIGLIAMO	Cambiare le credenziali su tutte le stampanti; disattivare i servizi non usati; aggiornare il firmware; limitare l'accesso di amministrazione a una postazione.	
SFORZO	Basso (alcune ore). Priorità alta: correzione entro 30 giorni.	

PT-03	ALTO	Switch di piano rimasto senza aggiornamento dopo una manutenzione: una postazione ottiene un accesso non previsto
DOVE	Switch del piano 4 (punto T4); giornata G7. Emerso dal confronto tra le versioni del software degli switch (inventario del livello 5) e confermato con una prova dal punto T4.	
CHE COSA ABBIAMO OSSERVATO	Gli switch di piano vengono aggiornati periodicamente dall'IT interno con una procedura programmata. Lo switch del piano 4 risultava una versione di sicurezza indietro rispetto agli altri undici: era spento per manutenzione nella finestra dell'ultimo aggiornamento e la procedura non ha segnalato che quell'apparato non era stato raggiunto, né lo ha ripreso quando è tornato in servizio. Su quell'apparato una postazione di lavoro collegata a una porta di accesso ha potuto raggiungere reti diverse da quella assegnata, per un problema di controllo degli accessi di cui non abbiamo individuato la causa precisa (l'ipotesi più probabile è la mancata correzione contenuta nella versione successiva: da confermare con il costruttore).	
PROVA	Dal punto T4, nella finestra concordata, si è verificato che la separazione prevista tra la rete utenti e le altre reti non era rispettata, raggiungendo soltanto un sistema di prova indicato dal referente tecnico. Non è stato letto né modificato alcun dato . Evidenza EV-044, con data, ora e impronta nel registro delle prove.	
IMPATTO	Una postazione compromessa, o semplicemente collegata a quello switch, potrebbe arrivare a reti e sistemi che non le competono. Il punto debole non è un guasto isolato ma un passaggio del processo : nessun controllo segnala gli apparati rimasti indietro, e lo stesso potrebbe accadere con qualunque switch spento o irraggiungibile durante un aggiornamento.	
CHE COSA CONSIGLIAMO	Subito (entro 72 ore) : aggiornare lo switch del piano 4; verificare la versione di tutti gli apparati di piano; controllare i registri per accessi insoliti dalle postazioni di quel piano. Entro 30 giorni : far segnalare alla procedura gli apparati non raggiunti, con nuovi tentativi automatici e un rapporto per l'IT; confronto automatico delle versioni con quella di riferimento; autenticazione dei dispositivi sulle porte di accesso. Entro 90 giorni : verifica trimestrale delle versioni, registrata.	
SFORZO	Basso per l'aggiornamento (alcune ore); medio per la correzione della procedura. Priorità alta.	
VERIFICA SUCCESSIVA	Ripetizione della prova a 30 giorni (8 luglio 2026).	

PT-06	MEDIO	Rete Wi-Fi ospiti senza isolamento tra i dispositivi collegati
DOVE	Sala d'attesa al piano terra, giornata G9.	
CHE COSA ABBIAMO OSSERVATO	La rete ospiti è separata dalla rete interna, come previsto. I dispositivi collegati alla stessa rete ospiti, però, possono vedersi tra loro.	
IMPATTO	Un visitatore potrebbe osservare o disturbare i dispositivi di un altro visitatore. La rete interna di Voltaria non è raggiungibile.	
CHE COSA CONSIGLIAMO	Attivare l'isolamento dei client sul punto di accesso; pagina di accettazione con scadenza dell'accesso; limite di banda per ospite.	
SFORZO	Basso (impostazione). Priorità media: correzione entro 90 giorni.	

Pulizia e ripristino

CAPITOLO 21 · PARTE C — IL PENETRATION TEST (EFESTO, LIVELLO AVANZATO)

L'ultima giornata di test (G12) non produce rilievi: **riporta tutto com'era**. Si rimuove ogni cosa creata dai test, si restituiscono le tratte e gli spazi, si verifica che la rete sia identica a come era prima e si chiude l'incarico sul campo con una riunione e un verbale firmato. Presenti: responsabile di progetto BoNet™, tecnico di supporto, referente tecnico e responsabile impianti di Voltaria, elettricista, cablatore, sponsor per la riunione di chiusura.

21.1 Che cosa si è fatto

Area	Azione	Verifica
Hardware di test	Spegnimento ordinato e rimozione dell'unità di test (H1), dell'aggregatore ottico (H2), dell'UPS dedicato, dei moduli ottici e dei cavi dal rack del CED.	Foto del rack prima e dopo; verbale firmato
Alimentazione e raffreddamento	Scollegamento dalla linea dedicata; letture finali di assorbimento e temperatura.	Valori confrontati con il rilievo iniziale
Tratte verso i piani	Restituzione delle tratte spare con prova di continuità (cablatore); nessuna fibra lasciata collegata.	Certificati delle tratte; verbale
Accessi e utenze	Revoca di ogni utenza, chiave e credenziale creata per i test; chiusura dell'accesso di emergenza (LTE) e della SIM.	Elenco firmato dal referente tecnico
Configurazioni di Voltaria	Confronto con le copie di configurazione prese al kick-off: nessuna modifica nei core, negli switch, nei firewall e nei router.	Impronte confrontate; esito: nessuna differenza
Evidenze	Chiusura del registro delle prove con impronta finale; copia cifrata verso l'archivio BoNet™; cancellazione sicura dei dispositivi di test entro 30 giorni.	Registro (appendice B); certificato di cancellazione
Passaggi nei cavedi	Nessun varco aperto: si sono usati solo passaggi esistenti. Controllo del cablatore e del facility manager.	Anomalie: nessuna (rilievo PT-16 informativo)

21.2 Prima e dopo

Misura nel CED	Rilievo iniziale (G1)	Dopo la rimozione (G12)
Temperatura dell'aria in ingresso al rack	22,1 °C	22,2 °C
Assorbimento della linea dedicata	0 W	0 W (scollegata)
Assorbimento di punta durante i test (unità + aggregatore + UPS)	—	187 W (picco), 64 W medi
Differenze nelle configurazioni di Voltaria	—	Nessuna
Utenze e credenziali dei test	—	Tutte revocate

RECOVERY · VERIFICA DEL RITORNO ALLO STATO INIZIALE

Prima di lasciare il centro dati, il referente tecnico controlla insieme a BoNet™ lo stato dei servizi critici (posta, gestionali, VPN delle agenzie, backup) e l'assenza di allarmi. Solo dopo si firma il **verbale di ripristino**, che entra nell'handover (capitolo 23).

DA DECIDERE · DOPO LA CHIUSURA

La verifica a trenta giorni (capitolo 24) non richiede di reinstallare l'hardware nel CED: si usa l'unità mobile, salvo diverso accordo. Una nuova installazione si concorda caso per caso.

Piano di rimedio

CAPITOLO 22 · PARTE C — IL PENETRATION TEST (EFESTO, LIVELLO AVANZATO)

Un rilievo non corretto è un problema rimandato. Il piano di rimedio trasforma i rilievi del penetration test in **azioni con un responsabile, una scadenza e una prova di verifica** (richiesta R9). Le correzioni sono un'attività del cliente: BoNet™ propone e verifica, non modifica i sistemi. Il piano è coordinato con quello del capitolo 14: le azioni che compaiono in entrambi si fanno una volta sola.

22.1 Le azioni, rilievo per rilievo

ID	Gravità	Azione	Quando	Chi	Prova di verifica
PT-01	CRITICO	Cambiare le credenziali; limitare la console a due postazioni di amministrazione; autenticazione a più fattori; rete di gestione separata; copia non modificabile.	72 ore (misure); 30 giorni	Referente tecnico	Ripetizione della prova dal punto T3: l'accesso non deve riuscire
PT-02	ALTO	Cambiare le credenziali su tutte le stampanti; disattivare i servizi non usati; aggiornare il firmware.	30 giorni	Team IT	Verifica su tutte e 62 le stampanti
PT-03	ALTO	Aggiornare lo switch del piano 4; rapporto automatico degli apparati non raggiunti; autenticazione dei dispositivi sulle porte (pilota).	72 ore; 30 giorni; 90 giorni	Team IT	Versioni di tutti gli switch; prova di separazione dal punto T4
PT-04	ALTO	Applicare gli aggiornamenti arretrati; finestra mensile.	30 giorni	Team IT	Versione e correzioni verificate dall'esterno
PT-05	MEDIO	Disattivare gli algoritmi datati; aggiornare le agenzie con apparati vecchi.	90 giorni	Team IT + agenzie	Verifica del concentratore; elenco delle agenzie migrate
PT-06	MEDIO	Isolamento dei client sul Wi-Fi ospiti; scadenza dell'accesso; limite di banda.	90 giorni	Team IT	Prova dalla sala d'attesa
PT-07	MEDIO	Spostare la gestione del registratore sulla rete di gestione; regola esplicita tra le reti.	90 giorni	Team IT + sicurezza fisica	Prova di percorso tra le due reti
PT-08	MEDIO	Account di servizio con password lunga e scadenza; inventario degli account di servizio.	90 giorni	Team IT	Controllo della directory
PT-09	BASSO	Nascondere nome e versione del software nei servizi web.	Intervento programmato	Team IT	Controllo dall'esterno
PT-10	BASSO	Disattivare i protocolli di ricerca dei nomi locali non necessari.	Intervento programmato	Team IT	Controllo dai punti T1-T6
PT-11	BASSO	Limitare l'accesso alla pagina web dei telefoni alla rete di gestione; password robusta.	Intervento programmato	Team IT	Controllo dai punti T1-T6

I rilievi PT-12-PT-16 sono punti di forza o informativi: nessuna azione, ma vanno mantenuti nel tempo. Le azioni sui rilievi dei livelli (R1-... R6-...) sono nel capitolo 14.

22.2 Un suggerimento per il monitoraggio

DA DECIDERE · VEDERE CIÒ CHE ACCADE

Nella giornata G11 il sistema di monitoraggio di Voltaria non ha segnalato l'accesso alla console di backup né alle stampanti. Si consiglia di attivare gli avvisi su accessi amministrativi alle console, nuovi dispositivi sulle porte di accesso e variazioni di versione degli apparati: non evitano un incidente, ma permettono di accorgersene in minuti e non in settimane.

22.3 L'ordine consigliato

1. **Proteggere i backup** (PT-01): è ciò da cui si riparte dopo un incidente.
2. **Chiudere il punto debole dei piani** (PT-03): aggiornamento e controllo delle versioni.
3. **Chiudere le porte aperte dall'esterno** (PT-04, PT-05).
4. **Sistemare i dispositivi dimenticati** (PT-02, PT-06, PT-07).
5. **Programmare le correzioni di fondo** (rete di gestione, autenticazione dei dispositivi, archivio dei registri).

Handover: consegna e passaggio

CAPITOLO 23 · PARTE C — LA CHIUSURA DELL'INCARICO

L'handover è il momento in cui BoNet™ **restituisce tutto a Voltaria** e passa le conoscenze al team interno: documenti, prove, hardware, accessi e responsabilità. Non è una formalità. Qui si verifica che ciò che lo studio di fattibilità SF-2026-014 aveva promesso, e che il kick-off del 28 aprile aveva firmato, sia stato davvero consegnato. L'handover si svolge il **10 giugno 2026**, due giorni dopo la consegna della relazione.

23.1 Che cosa si consegna

Documento o bene	Contenuto	A chi
Relazione completa	Le sette analisi, il penetration test, i rilievi per gravità, il piano di rimedio; in italiano e in inglese, firmata.	Sponsor, referente tecnico
Attestazione sintetica	Due pagine, senza dettagli sensibili, da mostrare a clienti e assicuratore (richiesta R7).	Sponsor
Registro delle prove	Ogni prova con data, ora, operatore e impronta SHA-256, su supporto cifrato.	Referente tecnico, referente privacy
Inventario e schema aggiornati	La rete com'è, con le differenze rispetto ai documenti di Voltaria elencate e corrette (richiesta R4).	Referente tecnico
Piano di rimedio	Interventi in ordine di priorità, con tempi, responsabili proposti e prova di verifica (richiesta R9).	Sponsor, referente tecnico
Dossier del cablaggio	Tratte usate, certificazioni, ripristino dei passaggi nei cavedi REI120, firmati dal cablatore.	Responsabile impianti
Verbale di ripristino (G12)	Ritorno allo stato iniziale, con letture di temperatura e assorbimento, foto e firme.	Responsabile impianti
Elenco di strumenti e licenze	Versioni e tipi di licenza impiegati (appendice A).	Sponsor
Studio e verbale di kick-off	Lo studio SF-2026-014 e il verbale del 28 aprile, aggiornati con ciò che è cambiato durante l'incarico.	Sponsor

23.2 Il passaggio al team IT

Il workshop è di mezza giornata, il 10 giugno 2026, con i due tecnici interni, lo sponsor e il referente privacy. Serve a far sì che i risultati restino nelle mani di Voltaria (richiesta R10).

Orario	Argomento	Partecipanti
9:00–10:00	Sintesi per la direzione: che cosa è emerso, che cosa conta di più.	Sponsor, referente tecnico, referente privacy
10:00–11:30	I rilievi uno per uno, con le prove: dal critico al basso.	Team IT, referente tecnico
11:30–12:30	Il piano di rimedio: si assegnano responsabili e scadenze.	Sponsor, referente tecnico, team IT
12:30–13:00	Come ripetere le prove di failover e i controlli periodici; calendario annuale proposto.	Team IT

23.3 Chiusura e restituzione

Si restituisce o si ripristina

- L'hardware di test è **rimosso dal CED (G12)** e le configurazioni tornano com'erano.
- Le **tratte spare** sono restituite con verbale e prova di continuità.
- Le credenziali e gli accessi creati per i test sono **revocati**.
- Gli apparati del cliente non hanno subito modifiche.

Si conserva o si distrugge

- I dati dei dispositivi di test sono **cancellati in modo sicuro** entro 30 giorni dalla chiusura.
- Una copia cifrata delle prove è **conservata 12 mesi**, per la verifica e per eventuali contestazioni, poi distrutta con certificato.
- L'accesso all'archivio avviene solo su richiesta scritta del referente tecnico.
- Le licenze restano di BoNet™.

23.4 Matrice di tracciabilità

Ogni richiesta dello studio di fattibilità ha il suo **esito**, con il capitolo della relazione che la tratta. L'esito dice se la richiesta ha ricevuto risposta; la correzione dei punti deboli trovati è un'attività distinta, nel piano di rimedio.

ID	Richiesta (studio SF-2026-014)	Dove si tratta	Esito
R1	Tenuta ai guasti senza fermare gli ordini	Cap. 13 · G8 · PT-14	✓ SODDISFATTA
R2	Esposizione da Internet	Cap. 15 · PT-04, PT-05, PT-09	✓ SODDISFATTA
R3	Dispositivo compromesso nei piani o dal Wi-Fi ospiti	Cap. 16-17 · T1-T6 · PT-03, PT-06	✓ SODDISFATTA
R4	Inventario aggiornato e verificato	Cap. 8-9 · allegato	✓ SODDISFATTA
R5	VPN delle agenzie sicure	Cap. 15 · PT-05	🚫 CON RISERVA dal lato della sede
R6	Stato dei backup e ripristino	Cap. 13 · cap. 18 · PT-01	? DA VERIFICARE dopo la correzione
R7	Relazione e attestazione per clienti e assicuratore	Cap. 23.1	✓ SODDISFATTA
R8	Nessun fermo degli ordini	Cap. 4 · cap. 6	✓ SODDISFATTA
R9	Piano di rimedio e verifica	Cap. 22 · cap. 24	? DA VERIFICARE l'8 luglio
R10	Passaggio delle conoscenze	Cap. 23.2	✓ SODDISFATTA
R11	Riservatezza e dati personali	Cap. 4 · cap. 23.3	✓ SODDISFATTA

In sintesi: 8 richieste soddisfatte, 1 con riserva (le reti delle agenzie erano fuori perimetro), 2 da verificare dopo la correzione. La verifica del 8 luglio (capitolo 24) le chiude.

STRUMENTI E ATTIVITÀ BONET™ · DOPO LA CONSEGNA

Per trenta giorni dalla consegna i chiarimenti sulla relazione sono compresi nell'incarico. Il mandato VD-2026-031 si chiude con il **verbale di consegna**, firmato dallo sponsor di Voltaria e dal responsabile di progetto BoNet™; la verifica a trenta giorni è un'attività distinta, già prevista dallo studio di fattibilità.

Per Voltaria Distribuzione S.p.A. — Direttore generale
Data e firma

Per BoNet™ — Responsabile di progetto
Data e firma

Verifica successiva a 30 giorni

CAPITOLO 24 · PARTE C — LA CHIUSURA DELL'INCARICO

Il livello Avanzato prevede una **verifica dopo trenta giorni**: si ripetono le prove sui punti che Voltaria ha dichiarato di aver corretto, per controllare che la correzione funzioni davvero. L'8 luglio 2026 la verifica si è svolta in una mezza giornata, con l'unità mobile e il referente tecnico presente, senza reinstallare l'hardware nel CED. Questo capitolo è un aggiornamento della relazione, nello stesso formato.

24.1 Esito per rilievo

ID	Gravità iniziale	Che cosa ha fatto Voltaria	Esito della verifica
PT-01	CRITICO	Credenziali cambiate; console limitata a due postazioni; autenticazione a più fattori attivata; copia non modificabile in corso.	✓ CHIUSO (restano le copie fuori sede)
PT-02	ALTO	Credenziali cambiate su 60 stampanti su 62; due modelli vecchi in sostituzione.	🔒 PARZIALE (2 aperte)
PT-03	ALTO	Switch del piano 4 aggiornato; la procedura ora produce un rapporto degli apparati non raggiunti e ritenta; controllo mensile delle versioni.	✓ CHIUSO
PT-04	ALTO	Aggiornamenti applicati; finestra mensile concordata.	✓ CHIUSO
PT-05	MEDIO	Algoritmi datati disattivati su 31 agenzie su 40; le altre in aggiornamento.	🔒 PARZIALE (9 agenzie)
PT-06	MEDIO	Isolamento dei client attivato.	✓ CHIUSO
PT-07 ... PT-11	MEDIO · BASSO	Nei programmi di intervento a 90 giorni o al prossimo intervento programmato.	? IN CORSO

24.2 Le richieste che erano «da verificare»

ID	Richiesta	Esito aggiornato
R6	Stato dei backup e ripristino	✓ SODDISFATTA prova di ripristino ripetuta il 7 luglio; copia non modificabile attiva
R9	Piano di rimedio e verifica	✓ SODDISFATTA con quattro rilievi chiusi e due parziali
R5	VPN delle agenzie sicure	🔒 CON RISERVA lato sede migliorato; il lato agenzie resta fuori perimetro

✓ ESITO COMPLESSIVO

Sei rilievi su undici sono chiusi o in chiusura con una prova ripetuta. I due punti più importanti (backup e switch dei piani) sono chiusi. Per gli interventi di architettura (rete di gestione, sala secondaria, autenticazione dei dispositivi) si propone una revisione tra sei mesi.

NOTA · COME SI LEGGONO LE DATE

Il documento descrive un incarico di fantasia, con date inventate: la verifica «dell'8 luglio» è il modo di mostrare come si chiude il cerchio.

Appendice A · Licenze degli strumenti

APPENDICI · ELENCO PRESENTATO AL KICK-OFF DEL 28 APRILE 2026

Ogni strumento usato nell'incarico è elencato con il tipo di licenza e con la versione, **congelata al kick-off**: i risultati restano ripetibili fino alla chiusura. Le licenze commerciali sono acquistate a fronte dell'incarico e **intestate a BoNet™**, **non al cliente**. In un incarico reale la tabella riporta numeri e scadenze veri: qui compaiono valori di esempio.

A.1 Software libero

Strumento	Funzione	Licenza	Versione
Kali Linux	Sistema di base	Software libero (licenze varie, in prevalenza GPL)	Edizione rolling dell'aprile 2026; immagine verificata con la firma del produttore
Nmap	Inventario e scansione	Nmap Public Source License	Registrata al kick-off
Greenbone Community Edition	Ricerca di vulnerabilità	GPL	Registrata al kick-off; dati delle vulnerabilità aggiornati alla stessa data
Wireshark · Zeek · Suricata	Analisi del traffico	GPLv2 · BSD · GPLv2	Registrate al kick-off
testssl.sh	Solidità delle cifrature	GPLv2	Registrata al kick-off
Kismet	Wi-Fi	GPLv2	Registrata al kick-off
iperf3	Prestazioni	BSD	Registrata al kick-off
BloodHound Community Edition	Percorsi di privilegio nella directory	Apache 2.0	Registrata al kick-off

A.2 Licenze commerciali

Strumento	Tipo di licenza	Numero (esempio)	Scadenza (esempio)	Intestata a
Tenable Nessus Professional	Abbonamento annuale per scanner	ESEMPIO-0001	31 dicembre 2026	BoNet™
Burp Suite Professional (PortSwigger)	Abbonamento annuale per utente	ESEMPIO-0002	31 dicembre 2026	BoNet™
PingCastle (Netwrix), per consulenti	Commerciale per prestatori di servizi	ESEMPIO-0003	31 dicembre 2026	BoNet™

DA CONTROLLARE IN UN INCARICO REALE

I termini d'uso di ogni strumento (in particolare dei commerciali) vanno riletti prima dell'incarico: possono limitare l'uso su sistemi di terzi, il numero di indirizzi o la consegna dei risultati al cliente.

A.3 Hardware di test

I modelli sono nel capitolo 5. Al termine, i dischi di tutte le unità sono stati cancellati in modo sicuro (certificato nel registro delle prove) e le unità riconsegnate alla scorta di BoNet™.

Appendice B · Registro delle prove

APPENDICI · UN ESTRATTO DEL REGISTRO, IN FORMA D'ESEMPIO

Ogni prova ha un numero (EV-xxx), una data e un'ora, un operatore e un'impronta (**SHA-256**) del file di evidenza: se il file viene modificato, l'impronta cambia. Il registro è tenuto su supporto cifrato e consegnato a Voltaria all'handover; nelle schede dei rilievi compare solo il numero. Le impronte qui sono accorciate e inventate. I nomi delle persone non compaiono: solo il ruolo.

EV	Data · ora	Giornata	Operatore	Che cosa documenta	Impronta
EV-004	12 mag · 09:40	G2	Tecnico di supporto	Elenco di dispositivi rilevati (inventario passivo, 7 giorni)	a3f9...c07e
EV-012	13 mag · 11:15	G3	Responsabile di progetto	Servizi raggiungibili da Internet (11), dal punto esterno H4	71be...09d2
EV-019	14 mag · 15:02	G4	Responsabile di progetto	Filtri e limiti BGP sui router di bordo (sola lettura)	e45c...2a19
EV-027	18 mag · 22:30	G6	Responsabile di progetto	Visibilità tra reti dai punti T1 e T2	0d88...f3a4
EV-031	19 mag · 21:12	G7	Responsabile di progetto	Accesso alla console del backup dal punto T3 (chiuso subito)	c2b0...58ee
EV-044	19 mag · 23:48	G7	Responsabile di progetto	Separazione tra reti dal punto T4: versione del software dello switch del piano 4	94ac...d1b7
EV-053	20 mag · 00:25	G8	Tecnico di supporto	Prova di failover del piano 5: tempi di commutazione e ritorno	6f10...ab33
EV-061	21 mag · 10:50	G9	Tecnico di supporto	Stampanti: 14 interfacce con credenziali predefinite	38d5...7e90
EV-072	22 mag · 14:05	G10	Responsabile di progetto	Stato della directory: account di servizio senza scadenza	b71e...0c25
EV-086	25 mag · 23:10	G11	Responsabile di progetto	Prova controllata n. 2 (switch del piano 4): consenso firmato e chiusura	1ee9...44f8
EV-098	26 mag · 16:30	G12	Responsabile di progetto	Verbale di ripristino: letture finali, confronto delle configurazioni	cd04...a6b2

NOTA · COME SI USA IL REGISTRO

Se un rilievo viene messo in discussione, o se un anno dopo si vuole ripetere una prova, il registro permette di sapere esattamente che cosa è stato fatto, quando e da chi, e di controllare che le evidenze non siano state alterate. Le evidenze sono conservate cifrate per dodici mesi e poi distrutte, con certificato (capitolo 23.3).

Appendice C · Glossario

APPENDICI · LE PAROLE USATE, IN PAROLE SEMPLICI

Termine	Che cosa significa
802.1X	Regola per cui un dispositivo deve identificarsi prima di ottenere una rete da una presa o dal Wi-Fi.
Alta affidabilità	Due apparati uguali, di cui uno subentra se l'altro si ferma.
BGP	Il sistema con cui un'azienda con più fornitori di Internet annuncia i propri indirizzi: se una linea cade, il traffico passa dalle altre.
CED	Centro elaborazione dati: la sala dei server e degli apparati principali.
Core	L'apparato centrale della rete interna, a cui si collegano gli switch dei piani.
DMZ	Zona separata della rete in cui stanno i servizi raggiungibili da Internet (posta, sito, VPN), distinta dalla rete interna.
Evidenza	La prova di ciò che si è fatto: un file con data, ora e impronta.
Failover	Il passaggio automatico dall'apparato principale a quello di riserva.
Firewall	Apparato che decide quali comunicazioni sono ammesse tra le zone della rete.
Firmware	Il software incorporato in un apparato (switch, stampante, telefono).
Grey box · black box · white box	Con quante informazioni parte il test: con un'utenza ordinaria, con nessuna informazione, con documentazione e accessi dedicati.
Handover	La consegna finale, con il passaggio delle conoscenze al team del cliente.
Impronta (SHA-256)	Un codice calcolato dal contenuto di un file: se il file cambia, il codice cambia.
Kick-off	La riunione iniziale in cui si fissano ruoli, limiti, condizioni di stop e recovery.
Penetration test	Prova autorizzata e controllata, che verifica se i punti deboli possono essere sfruttati davvero.
Perimetro	L'insieme di indirizzi, apparati e giornate autorizzati: ciò che non è scritto resta fuori.
Recovery	Che cosa si fa per tornare alla normalità dopo un'interruzione.
REI120	Classe di resistenza al fuoco: il compartimento regge 120 minuti.
Rilievo	Un punto debole o una buona pratica emersi dall'analisi, con gravità, prova e correzione consigliata.
SNMP	Protocollo con cui gli apparati forniscono dati di monitoraggio.
Spanning tree	Meccanismo che evita i «giri» nella rete tra switch collegati in più modi.
Spare (tratte)	Collegamenti di scorta già posati, usati solo in caso di guasto.
Switch	Apparato che collega fra loro computer, telefoni e stampanti di un piano.
TAP	Dispositivo passivo che permette di osservare il traffico senza interromperlo.
VLAN	Divisione logica di una rete fisica in reti separate (utenti, voce, stampanti...).
VPN	Tunnel cifrato per collegare una sede lontana alla rete aziendale.

Appendice D · Aspetti legali

APPENDICI · CHE COSA DEVE ESSERE CHIARO PER ISCRITTO PRIMA DI INIZIARE

Un test invasivo ha senso solo se tutte le parti sanno che cosa accade, su che cosa e con quali responsabilità. Questa appendice riassume in forma semplice i punti che l’incarico firmato definisce. **Non è consulenza legale**: fa fede il testo del mandato VD-2026-031 e della sua appendice tecnica.

Tema	Che cosa prevede l’incarico
Autorizzazione scritta	Accedere a un sistema informatico senza autorizzazione è reato (art. 615-ter del Codice penale). Per questo nessuna attività è partita prima del mandato firmato dal titolare e della sua appendice tecnica; l'autorizzazione dell'analisi di rete non si estende ai test invasivi.
Perimetro, tempi, durata	L'autorizzazione vale solo per indirizzi, sedi, apparati, tipi di test, approcci, finestre orarie e durata indicati. Ciò che non è scritto è escluso; ogni estensione richiede un nuovo accordo scritto.
Terze parti	Per le linee dei due fornitori è stato necessario il consenso scritto di ciascuno (lettere del 21 aprile 2026). Senza consenso, quei sistemi restano fuori.
Rischi e responsabilità	Voltaria è stata informata per iscritto che i test possono causare rallentamenti, malfunzionamenti o interruzioni, e ha confermato di avere un backup verificato (prova di ripristino del 20–21 aprile). La ripartizione delle responsabilità e i limiti sono nel mandato.
Assicurazione	L'assicurazione è a carico di Voltaria, come da mandato. Voltaria ha informato per iscritto il proprio assicuratore dell'attività di test e ha conservato la risposta.
Dati personali	Il test non cerca né conserva contenuti. Dove emergano dati personali, BoNet™ opera come responsabile del trattamento con apposita nomina (art. 28 del GDPR), si limita alla prova minima e distrugge le evidenze entro i termini dell’incarico, con attestazione su richiesta.
Compromissioni già in corso	Se emerge un incidente già in atto, le attività si sospendono e il referente è informato subito; le notifiche di legge, per esempio al Garante per la protezione dei dati personali, spettano al titolare.
Riservatezza	Le informazioni su configurazioni, vulnerabilità e credenziali restano riservate. La relazione è consegnata solo al titolare; le credenziali non compaiono nei documenti.
Chi può fermare tutto	Un referente indicato da Voltaria può chiedere in ogni momento la sospensione immediata. Ogni sessione inizia e finisce con una comunicazione al referente.
Conservazione delle evidenze	Copia cifrata conservata dodici mesi, poi distrutta con certificato; dispositivi di test cancellati in modo sicuro entro trenta giorni dalla chiusura (capitolo 23.3).

NOTA
Qualsiasi dubbio su questi punti va chiarito prima della firma, non dopo. Il presente documento è dimostrativo: nomi, date e riferimenti sono di fantasia, e il testo di un mandato reale va redatto e rivisto con un professionista del diritto.