MESH PC

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

REPORT DI AUDIT IT

Studio Legale Esempio (report dimostrativo)

Data dell'audit: 25 novembre 2026 · kancelaria-demo.example · Auditor: Sebastiano Blanco, MeshPC · 3 computer

VALUTAZIONE COMPLESSIVA

Richiede interventi urgenti

Ci sono minacce che possono fermare l'azienda o causare una fuga di dati.

Risultati per area

Dominio ed email	Microsoft 365	Account, password e MFA	Computer
Da migliorare verificati 10 su 10	Non verificato	Da migliorare verificati 1 su 1	Urgente verificati 12 su 12

Backup	Rete e Wi-Fi	Preparazione NIS2
Non verificato	Urgente verificati 6 su 6	Non verificato

Bene · Da migliorare · Urgente · Non verificato

Le aree indicate come “Non verificato” non sono state incluse in questo report. L'audit completo copre tutte le 8 aree e dura 60–90 minuti.

Priorità principali

1. **Sistema operativo ancora supportato**
   Un sistema non supportato non riceve correzioni di sicurezza: le falle note restano aperte per sempre.
   Cosa abbiamo trovato: 3 su 3: RECEPCJA-PC – Windows 10 Pro 22H2 – supporto terminato il 14/10/2025; LAPTOP-SZEF – …
   Raccomandazione: Aggiornare a una versione supportata (Windows 11 25H2; macOS 15, 26 o 27); l'hardware non compatibile va sostituito o, temporaneamente, coperto da Windows 10 ESU.

2. **Aggiornamenti installati**
   Gli aggiornamenti mancanti sono la via più comune del ransomware nelle piccole aziende.
   Cosa abbiamo trovato: 2 su 3: RECEPCJA-PC – ultimo aggiornamento 2026-08-02 (115 giorni fa); MacBook-Kasia – ultimo …
   Raccomandazione: Installazione automatica degli aggiornamenti di sistema e applicazioni con riavvio imposto entro pochi giorni (es. Windows Update for Business / Intune) e verifica periodica della conformità.

3. **Antivirus / EDR attivo e aggiornato**
   Senza protezione attiva il malware agisce inosservato.
   Cosa abbiamo trovato: 3 su 3: RECEPCJA-PC – più antivirus attivi contemporaneamente: Windows Defender, Avast Free …
   Raccomandazione: Un solo prodotto di protezione attivo per computer; una soluzione di classe EDR (es. Microsoft Defender for Business) con protezione antimanomissione e visibilità centralizzata degli avvisi.

ESEMPIO

MESH PC

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

Piano d'azione

La priorità riflette la gravità della minaccia: i punti che possono fermare l'azienda o causare una fuga di dati sono indicati come urgenti.

URGENTE – ENTRO 7 GIORNI

D1 **Sistema operativo ancora supportato** — Urgente

Cosa abbiamo trovato: 3 su 3: RECEPCJA-PC – Windows 10 Pro 22H2 – supporto terminato il 14/10/2025; LAPTOP-SZEF – Windows 11 Pro 24H2 – supporto terminato il 2026-10-13; MacBook-Kasia – macOS 14.7 – senza più correzioni di sicurezza

Raccomandazione: Aggiornare a una versione supportata (Windows 11 25H2; macOS 15, 26 o 27); l'hardware non compatibile va sostituito o, temporaneamente, coperto da Windows 10 ESU.

D2 **Aggiornamenti installati** — Urgente

Cosa abbiamo trovato: 2 su 3: RECEPCJA-PC – ultimo aggiornamento 2026-08-02 (115 giorni fa); MacBook-Kasia – ultimo aggiornamento 2026-10-20 (36 giorni fa)

Raccomandazione: Installazione automatica degli aggiornamenti di sistema e applicazioni con riavvio imposto entro pochi giorni (es. Windows Update for Business / Intune) e verifica periodica della conformità.

D3 **Antivirus / EDR attivo e aggiornato** — Urgente

Cosa abbiamo trovato: 3 su 3: RECEPCJA-PC – più antivirus attivi contemporaneamente: Windows Defender, Avast Free Antivirus; LAPTOP-SZEF – Windows Defender (senza EDR); MacBook-Kasia – solo XProtect integrato

Raccomandazione: Un solo prodotto di protezione attivo per computer; una soluzione di classe EDR (es. Microsoft Defender for Business) con protezione antimanomissione e visibilità centralizzata degli avvisi.

D4 **Cifratura del disco (BitLocker / FileVault)** — Urgente

Cosa abbiamo trovato: 3 su 3: RECEPCJA-PC – disco non cifrato; LAPTOP-SZEF – BitLocker attivo, backup della chiave non confermato; MacBook-Kasia – FileVault disattivato (portatile)

Raccomandazione: BitLocker con TPM (Windows) o FileVault (macOS) su tutti i computer, prima sui portatili; chiavi di ripristino archiviate in Entra ID o nell'MDM.

G1 **Servizi dell'ufficio esposti su internet** — Urgente

Cosa abbiamo trovato: indirizzo ufficio 203.0.113.25: porte aperte 443, 3389

Raccomandazione: Rimuovere sul router i port forwarding dei servizi amministrativi (RDP, SMB, pannello NAS, SSH); accesso remoto solo tramite VPN con MFA.

ALTA – ENTRO 30 GIORNI

A9 **Domini simili al vostro** — Urgente

Cosa abbiamo trovato: Domini simili con posta attiva: kancelaria-dem0.example; registrati: kancelaria-demo.example.com, kancelariademo.example

Raccomandazione: Verificare i proprietari dei domini (WHOIS/RDAP), segnalare gli abusi al registrar, valutare la registrazione delle varianti principali e avvisare personale e contabilità.

ESEMPIO

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

D7 **Strumenti di accesso remoto** — Urgente

Cosa abbiamo trovato: 2 su 3: RECEPCJA-PC – AnyDesk, TeamViewer; MacBook-Kasia – AnyDesk (non gestito)

Raccomandazione: Un solo strumento di assistenza remota con account aziendale, MFA e registro delle sessioni; disinstallare gli altri e bloccarne l'installazione.

D8 **Software obsoleto o vulnerabile** — Urgente

Cosa abbiamo trovato: 2 su 3: RECEPCJA-PC – WinRAR 6.11.0 (CVE-2025-8088), Microsoft Office Professional Plus 2016 – non supportato, Java 8 Update 251; LAPTOP-SZEF – 7-Zip 23.01

Raccomandazione: Disinstallare il software non più supportato, aggiornare il resto alle versioni correnti e includerlo negli aggiornamenti automatici.

F5 **Servizi rischiosi in rete (SMBv1, Telnet, RDP)** — Urgente

Cosa abbiamo trovato: 192.168.1.1 Telnet; 192.168.1.10 nas.local SMBv1

Raccomandazione: Disattivare SMBv1 e Telnet su tutti i dispositivi (aggiornando il firmware di NAS e stampanti se necessario) e limitare RDP a indirizzi specifici o alle connessioni VPN.

F6 **Filtro DNS (blocco dei siti malevoli)** — Urgente

Cosa abbiamo trovato: 3 su 3 senza filtro (DNS: 192.168.1.1)

Raccomandazione: Filtro DNS che blocca i domini malevoli e di phishing (es. Quad9, Cloudflare Gateway, DNSFilter), impostato sul router e sui portatili usati fuori ufficio.

A7 **Software del sito aggiornato** — Urgente

Cosa abbiamo trovato: Il sito usa PHP 8.1, senza più aggiornamenti di sicurezza.

Raccomandazione: Aggiornare CMS, plugin e PHP a versioni ancora coperte da correzioni di sicurezza; nascondere gli header Server/X-Powered-By e il tag generator.

D6 **Blocco automatico dello schermo** — Urgente

Cosa abbiamo trovato: 3 su 3: RECEPCJA-PC – nessun blocco automatico; LAPTOP-SZEF – blocco dopo 15 min; MacBook-Kasia – blocco dopo 15 min

Raccomandazione: Blocco dello schermo dopo massimo 10 minuti di inattività, imposto da policy (GPO, Intune o profilo MDM) e con richiesta di password o PIN.

D10 **Età dell'hardware** — Urgente

Cosa abbiamo trovato: 2 su 3: RECEPCJA-PC – OptiPlex 3050, BIOS del 2017; MacBook-Kasia – MacBook Air M1 (~2020)

Raccomandazione: Un piano di sostituzione dei computer con più di 6 anni, a partire da quelli che non soddisfano i requisiti di Windows 11.

D12 **Controllo delle memorie USB** — Urgente

Cosa abbiamo trovato: 3 su 3: RECEPCJA-PC – memorie USB senza limiti; LAPTOP-SZEF – memorie USB senza limiti; MacBook-Kasia – memorie USB senza limiti

Raccomandazione: Una policy che blocca o registra l'uso delle memorie USB (GPO o Intune Device Control), con eccezioni per dispositivi cifrati approvati.

ESEMPIO

MESH PC

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

PIANIFICATA – ENTRO 90 GIORNI

A6 **Certificato SSL e HTTPS del sito** — Da migliorare

Cosa abbiamo trovato: kancelaria-demo.example: nessun header HSTS; www.kancelaria-demo.example: nessun header HSTS

Raccomandazione: Certificato a rinnovo automatico, redirect 301 da http a https per dominio e www, header Strict-Transport-Security con max-age di almeno 6 mesi (RFC 6797).

A10 **Indirizzi email aziendali in violazioni note** — Da migliorare

Cosa abbiamo trovato: Indirizzi aziendali solo in violazioni più vecchie.

Raccomandazione: Cambiare le password degli account presenti nelle violazioni, imporre l'MFA e verificare che le stesse password non siano usate in altri servizi.

C6 **Diritti di amministratore sui computer** — Da migliorare

Cosa abbiamo trovato: 2 su 3: RECEPCJA-PC – l'utente anna è amministratore; MacBook-Kasia – l'utente kasia è amministratore

Raccomandazione: Lavoro quotidiano con un account standard; installazioni tramite un account amministrativo separato gestito ad es. con Windows LAPS o Intune Endpoint Privilege Management.

D5 **Firewall del computer** — Da migliorare

Cosa abbiamo trovato: 2 su 3: RECEPCJA-PC – firewall disattivato: Private; MacBook-Kasia – firewall di macOS disattivato

Raccomandazione: Firewall attivo per i profili dominio, privato e pubblico, gestito centralmente; regole in ingresso solo per i servizi necessari.

D9 **Stato e spazio libero del disco** — Da migliorare

Cosa abbiamo trovato: 2 su 3: RECEPCJA-PC – libero 9% (21 GB); MacBook-Kasia – libero 12% (30 GB)

Raccomandazione: Eseguire un backup e sostituire i dischi con avvisi SMART; liberare spazio fino ad almeno il 20% sul disco di sistema.

D11 **Gestione centralizzata dei dispositivi (Intune / RMM)** — Da migliorare

Cosa abbiamo trovato: 2 su 3: RECEPCJA-PC – non gestito; MacBook-Kasia – non gestito

Raccomandazione: Registrare i computer in Microsoft Intune (o altro MDM/RMM) per applicare policy di sicurezza, aggiornamenti e inventario.

G2 **Vulnerabilità note sull'IP pubblico** — Da migliorare

Cosa abbiamo trovato: 203.0.113.25: potenziali vulnerabilità da verificare (2): CVE-2023-44487, CVE-2024-3400

Raccomandazione: Verificare le CVE indicate sul dispositivo perimetrale (router, firewall, NAS) e installare gli aggiornamenti firmware o disattivare il servizio esposto.

A4 **Provider di posta (record MX)** — Da migliorare

Cosa abbiamo trovato: Posta su un server di hosting: mx.hosting-provider.example

Raccomandazione: Valutare una posta di livello aziendale con protezione antispam e antiphishing (es. Exchange Online con Defender for Office 365); nel frattempo attivare i filtri disponibili presso il provider attuale.

ESEMPIO

MESH PC

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

A5 **Cifratura della posta tra server (TLS, MTA-STS)** — Da migliorare

Cosa abbiamo trovato: Impossibile verificare STARTTLS (porta 25 bloccata); nessun MTA-STS.

Raccomandazione: Richiedere TLS per le connessioni SMTP, pubblicare una policy MTA-STS in modalità enforce (RFC 8461) e i report TLS-RPT (RFC 8460).

A8 **Protezione del dominio (DNSSEC, blocco trasferimento)** — Da migliorare

Cosa abbiamo trovato: DNSSEC: no, blocco trasferimento: sì; dominio pagato fino al 2027-10-01

Raccomandazione: Attivare DNSSEC presso l'operatore DNS e pubblicare il record DS presso il registrar (RFC 4033); mantenere il blocco trasferimento e il rinnovo automatico.

F4 **Dispositivi nella rete dell'ufficio** — Da migliorare

Cosa abbiamo trovato: dispositivi nella rete 192.168.1.25/24: 3 – elenco in allegato da confermare con il cliente; senza nome, con porte amministrative aperte: 192.168.1.1 (80,443,23)

Raccomandazione: Inventario dei dispositivi di rete con un responsabile assegnato, password predefinite cambiate e dispositivi sconosciuti scollegati.

Prossimo passo
Saremo lieti di discutere i risultati, rispondere alle domande sui singoli punti e aiutare a definire l'ordine degli interventi. Contatti: +48 789 599 983, info@meshpc.pl.

ESEMPIO

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

Allegato: tutti i punti verificati

N.	CONTROLLO	STATO	COSA ABBIAMO TROVATO
A. Dominio ed email			
A1	Record SPF (chi può inviare email per il dominio)	Bene	`v=spf1 a mx include:_spf.hosting-provider.example ~all (query DNS: 4)`
A2	Firma DKIM sulle email in uscita	Bene	`DKIM: x (2048-bit+)`
A3	Policy DMARC (protezione contro i falsi mittenti)	Bene	`v=DMARC1; p=quarantine; sp=quarantine; adkim=r; aspf=r; fo=1; rua=mailto:dmarc@kancelaria-demo.example`
A4	Provider di posta (record MX)	Da migliorare	`Posta su un server di hosting: mx.hosting-provider.example`
A5	Cifratura della posta tra server (TLS, MTA-STS)	Da migliorare	`Impossibile verificare STARTTLS (porta 25 bloccata); nessun MTA-STS.`
A6	Certificato SSL e HTTPS del sito	Da migliorare	`kancelaria-demo.example: nessun header HSTS; www.kancelaria-demo.example: nessun header HSTS`
A7	Software del sito aggiornato	Urgente	`Il sito usa PHP 8.1, senza più aggiornamenti di sicurezza.`
A8	Protezione del dominio (DNSSEC, blocco trasferimento)	Da migliorare	`DNSSEC: no, blocco trasferimento: sì; dominio pagato fino al 2027-10-01`
A9	Domini simili al vostro	Urgente	`Domini simili con posta attiva: kancelaria-dem0.example; registrati: kancelaria-demo.example.com, kancelariademo.example`
A10	Indirizzi email aziendali in violazioni note	Da migliorare	`Indirizzi aziendali solo in violazioni più vecchie.`
C. Account, password e MFA			
C6	Diritti di amministratore sui computer	Da migliorare	`2 su 3: RECEPCJA-PC – l'utente anna è amministratore; MacBook-Kasia – l'utente kasia è amministratore`
D. Computer			
D1	Sistema operativo ancora supportato	Urgente	`3 su 3: RECEPCJA-PC – Windows 10 Pro 22H2 – supporto terminato il 14/10/2025; LAPTOP-SZEF – Windows 11 Pro 24H2 – supporto terminato il 2026-10-13; MacBook-Kasia – macOS 14.7 – senza più correzioni di sicurezza`

ESEMPIO

MESH PC

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

N.	CONTROLLO	STATO	COSA ABBIAMO TROVATO
D2	Aggiornamenti installati	Urgente	2 su 3: RECEPCJA-PC – ultimo aggiornamento 2026-08-02 (115 giorni fa); MacBook-Kasia – ultimo aggiornamento 2026-10-20 (36 giorni fa)
D3	Antivirus / EDR attivo e aggiornato	Urgente	3 su 3: RECEPCJA-PC – più antivirus attivi contemporaneamente: Windows Defender, Avast Free Antivirus; LAPTOP-SZEF – Windows Defender (senza EDR); MacBook-Kasia – solo XProtect integrato
D4	Cifratura del disco (BitLocker / FileVault)	Urgente	3 su 3: RECEPCJA-PC – disco non cifrato; LAPTOP-SZEF – BitLocker attivo, backup della chiave non confermato; MacBook-Kasia – FileVault disattivato (portatile)
D5	Firewall del computer	Da migliorare	2 su 3: RECEPCJA-PC – firewall disattivato: Private; MacBook-Kasia – firewall di macOS disattivato
D6	Blocco automatico dello schermo	Urgente	3 su 3: RECEPCJA-PC – nessun blocco automatico; LAPTOP-SZEF – blocco dopo 15 min; MacBook-Kasia – blocco dopo 15 min
D7	Strumenti di accesso remoto	Urgente	2 su 3: RECEPCJA-PC – AnyDesk, TeamViewer; MacBook-Kasia – AnyDesk (non gestito)
D8	Software obsoleto o vulnerabile	Urgente	2 su 3: RECEPCJA-PC – WinRAR 6.11.0 (CVE-2025-8088), Microsoft Office Professional Plus 2016 – non supportato, Java 8 Update 251; LAPTOP-SZEF – 7-Zip 23.01
D9	Stato e spazio libero del disco	Da migliorare	2 su 3: RECEPCJA-PC – libero 9% (21 GB); MacBook-Kasia – libero 12% (30 GB)
D10	Età dell'hardware	Urgente	2 su 3: RECEPCJA-PC – OptiPlex 3050, BIOS del 2017; MacBook-Kasia – MacBook Air M1 (~2020)
D11	Gestione centralizzata dei dispositivi (Intune / RMM)	Da migliorare	2 su 3: RECEPCJA-PC – non gestito; MacBook-Kasia – non gestito
D12	Controllo delle memorie USB	Urgente	3 su 3: RECEPCJA-PC – memorie USB senza limiti; LAPTOP-SZEF – memorie USB senza limiti; MacBook-Kasia – memorie USB senza limiti
F. Rete e Wi-Fi			
F2	Sicurezza della rete Wi-Fi	Bene	Firma: WPA2-Personal CCMP (robustezza della chiave verificata con il cliente)
F4	Dispositivi nella rete dell'ufficio	Da migliorare	dispositivi nella rete 192.168.1.25/24: 3 – elenco in allegato da confermare con il cliente; senza nome, con porte amministrative aperte: 192.168.1.1 (80,443,23)
F5	Servizi rischiosi in rete (SMBv1, Telnet, RDP)	Urgente	192.168.1.1 Telnet; 192.168.1.10 nas.local SMBv1

ESEMPIO

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

N.	CONTROLLO	STATO	COSA ABBIAMO TROVATO
F6	Filtro DNS (blocco dei siti malevoli)	Urgente	`3 su 3 senza filtro (DNS: 192.168.1.1)`
G. Server ed esposizione su internet			
G1	Servizi dell'ufficio esposti su internet	Urgente	`indirizzo ufficio 203.0.113.25: porte aperte 443, 3389`
G2	Vulnerabilità note sull'IP pubblico	Da migliorare	`203.0.113.25: potenziali vulnerabilità da verificare (2): CVE-2023-44487, CVE-2024-3400`

Computer inclusi nell'audit

COMPUTER	SISTEMA	MODELLO	UTENTE	ULTIMO AGGIORNAMENTO
RECEPCJA-PC	Windows 10 Pro 22H2	Dell Inc. OptiPlex 3050	anna	2026-08-02
LAPTOP-SZEF	Windows 11 Pro 24H2	Lenovo ThinkPad T14 Gen 4 (portatile)	jan	2026-11-12
MacBook-Kasia	macOS 14.7	Apple MacBook Air (portatile)	kasia	2026-10-20

Dispositivi trovati nella rete dell'ufficio

INDIRIZZO IP	NOME	MAC	PORTE APERTE
192.168.1.1	– (router)	`AA-BB`	`80, 443, 23`
192.168.1.10	nas.local	`CC`	`445, 5000 SMBv1`
192.168.1.25	RECEPCJA-PC (RECEPCJA-PC)		`445`
192.168.1.40	–		`9100, 80`

L'audit è stato in sola lettura – non abbiamo modificato nulla nei vostri sistemi. I dati dell'audit sono conservati secondo l'accordo di riservatezza e cancellati dopo 90 giorni.

ESEMPIO