SERVIZIO SU PREVENTIVO · D.LGS. 138/2024

Assessment NIS2 guidato

Cosa succede nei dieci giorni lavorativi, cosa ti chiediamo e cosa ti consegniamo alla fine. La prova gratuita ti fa vedere la piattaforma; l'assessment ti dice dove sei rispetto agli obblighi ACN, e lo fanno i nostri specialisti sul tuo ambiente.

DURATA
10 giorni lavorativi

RIFERIMENTO
Misure di base ACN, Det. 379907/2025

COSA RICEVI
Gap analysis, registro fornitori, piano delle priorità, dossier di accountability

PREZZO
Su preventivo, in base a dispositivi e sedi. Scalato dal canone se attivi Sherlock Guard con l'annuale

1 **Il percorso**
Le sei fasi, giorno per giorno, e l'impegno richiesto al tuo team

2 **Perché farlo su Sherlock Guard**
Cosa cambia rispetto a un assessment su foglio di calcolo

3 **Esempio di risultato**
Il dossier finale di un'azienda fittizia, con dati dimostrativi

ESEMPIO Questo è un documento dimostrativo. I dati del capitolo 3 riguardano un'azienda inventata: servono a mostrare forma e contenuto del risultato, non descrivono alcun cliente reale.

Capitolo 1

Il percorso in dieci giorni lavorativi

Per i soggetti in elenco dal 2025 il termine per le misure di base è scaduto il 31 ottobre 2026 e l'ACN può avviare le verifiche. Chi è entrato nel 2026 ha tempo fino al 31 luglio 2027. In entrambi i casi il primo passo è lo stesso: misurare la distanza tra dove sei e dove devi arrivare.

Fase 0

Prima dell'avvio

Riunione di avvio

Un'ora con il responsabile IT per fissare il perimetro (sedi, dispositivi, servizi erogati), i referenti e il calendario delle interviste. Firmiamo l'accordo di riservatezza e l'accordo sul trattamento dei dati.

Esce: perimetro concordato e calendario dei dieci giorni.

Fase 1

Giorni 1–2

Sherlock Guard sul tuo ambiente

Creiamo la tua organizzazione e installiamo l'agent sui server e sulle postazioni concordate. L'agent è difensivo: legge la macchina su cui gira, non scansiona altri dispositivi. Se usi Microsoft 365 o un cloud pubblico li colleghiamo; switch, firewall e NAS si leggono, se vuoi, con il sensore di rete in sola lettura.

Esce: inventario di hardware e software e prima lista delle vulnerabilità, ordinate per sfruttamento reale (KEV, EPSS).

Fase 2

Giorno 3

Perimetro e qualificazione

Verifichiamo settore e soglia dimensionale, la qualifica di soggetto essenziale o importante e quindi l'allegato che ti riguarda. Controlliamo la registrazione sulla Piattaforma NIS, il punto di contatto e le scadenze dell'anno.

Esce: scheda di qualificazione con allegato applicabile e calendario degli adempimenti.

Fase 3

Giorni 3–6

Gap analysis requisito per requisito

Confrontiamo la situazione con l'allegato: 87 requisiti per i soggetti importanti (Allegato 1, 37 misure), 116 per gli essenziali (Allegato 2, 43 misure). Ogni requisito riceve un esito motivato: conforme, parziale, non conforme o non applicabile. Le parti tecniche le misura la piattaforma; quelle organizzative le raccogliamo con brevi interviste ai responsabili di area.

Esce: gap analysis completa, con l'evidenza collegata a ogni requisito.

Fase 4

Giorni 5–7

Fornitori critici

Impostiamo il registro fornitori con quelli che toccano i tuoi sistemi o i tuoi dati: classe di rischio, contratti e DPA, clausole di sicurezza. Ai fornitori in fascia alta inviamo il questionario di sicurezza dal portale dedicato.

Esce: registro fornitori pronto anche per la comunicazione annuale all'ACN.

Fase 5

Giorni 7–9

Piano delle priorità e dossier

Trasformiamo i gap in azioni ordinate per rischio: prima ciò che riduce di più l'esposizione con poco sforzo. Ogni azione ha un responsabile, una data e l'evidenza attesa. Raccogliamo tutto nella prima versione del dossier di accountability.

Esce: piano di adeguamento e dossier esportabile in PDF con impronta di controllo.

Fase 6

Giorno 10

Incontro di restituzione

Presentiamo esito e piano al responsabile IT e, se lo desideri, alla direzione. Il D.Lgs. 138/2024 (art. 23) chiede agli organi di amministrazione di approvare le misure e di sovrintenderne l'attuazione: il dossier è pensato per quella discussione.

Esce: decisioni sulle priorità e date dei primi interventi.

Cosa ti chiediamo

- Un referente IT con accesso amministrativo, per installare l'agent
- Interviste di circa un'ora con i responsabili di IT, direzione, personale e acquisti
- I documenti che hai già: policy, contratti dei fornitori, procedure di backup e di gestione incidenti
- Due ore per l'incontro di restituzione

Tempi indicativi: li adattiamo al perimetro nella riunione di avvio.

Cosa non è

- Non è un'attestazione di conformità: il dossier documenta lo stato delle misure e le priorità
- Non è consulenza legale: per gli obblighi fanno fede i testi ACN e la tua comunicazione individuale
- Non è un penetration test: nessuno strumento attacca i tuoi sistemi
- Non sostituisce il tuo consulente, se ne hai uno: lavorerà su dati aggiornati

Capitolo 2

Perché farlo già su Sherlock Guard

Un assessment tradizionale produce una fotografia: un foglio di calcolo che invecchia il giorno dopo la consegna. Fatto sulla piattaforma, lo stesso lavoro diventa la base su cui gestisci la NIS2 nei mesi successivi.

Evidenze misurate, non dichiarate

Inventario, versioni del software, patch mancanti e stato dell'MFA arrivano dai sistemi. La risposta a «avete l'inventario aggiornato?» è l'inventario stesso, con la data di oggi.

Il lavoro non si butta

Gap analysis, registro fornitori e piano restano nella tua console. Quando chiudi una vulnerabilità il finding si risolve da solo alla scansione successiva, e l'avanzamento si vede senza rifare il documento.

Pronto quando arriva una verifica

Il dossier si esporta in PDF, JSON o ZIP con impronta sha256. Un auditor esterno può consultarlo da un portale in sola lettura, a tempo e revocabile.

Incidenti nei termini di legge

Il flusso di notifica è già impostato: pre-notifica entro 24 ore, notifica entro 72, relazione finale entro un mese. L'invio alle autorità passa dalla tua casella PEC, con le ricevute conservate.

Un lavoro, più framework

Le evidenze raccolte per l'ACN si riusano per ISO 27001, NIST CSF 2.0 e gli altri framework guidati, grazie alla mappatura tra i controlli.

Il costo non si paga due volte

Se dopo l'assessment attivi Sherlock Guard con un contratto annuale, il prezzo dell'assessment viene scalato dal canone.

	ASSESSMENT SU FOGLIO DI CALCOLO	ASSESSMENT GUIDATO SU SHERLOCK GUARD
Fonte dei dati	Interviste e autodichiarazioni	Dati letti dai sistemi, interviste per la parte organizzativa
Dopo la consegna	Il documento resta fermo alla data dell'analisi	Lo stato si aggiorna a ogni scansione dell'agent
Fornitori	Elenco statico	Registro con classi di rischio, questionari e scadenze dei contratti
Verifica ACN	Si ricostruiscono le evidenze a mano	Dossier esportabile con impronta e portale per l'auditor
Incidente	Si cerca la procedura nel momento peggiore	Flusso 24h / 72h / 30 giorni pronto, con invio PEC
Anno successivo	Si riparte da zero	Si riparte dal piano e dalle evidenze già raccolte

Capitolo 3

Esempio di risultato

Estratto del dossier consegnato a fine assessment. Le pagine seguenti mostrano la sintesi per la direzione, il piano delle priorità, un estratto della gap analysis e del registro fornitori, e l'indice del dossier.

DATI DEMO Alfa Componenti S.p.A. è un'azienda inventata. Nomi, numeri e date sono dimostrativi.

ORGANIZZAZIONE	Alfa Componenti S.p.A. — fabbricazione di macchinari per l'industria
DIMENSIONE	210 addetti · fatturato 38 M€ · 2 sedi (stabilimento e uffici)
QUALIFICA	Soggetto **importante**, in elenco dal 2026 · Allegato 1: 37 misure, 87 requisiti
SCADENZA	Misure di base entro il **31 luglio 2027**
ASSESSMENT	19 – 30 ottobre 2026 · restituzione il 30 ottobre con direzione e responsabile IT

In breve

Le basi tecniche ci sono: inventario completo, backup giornalieri, firewall gestito. Mancano soprattutto le parti formali e di presidio: nessuna delibera della direzione sulle misure, log non centralizzati, nessun test di ripristino documentato, procedura incidenti senza i termini di notifica. Con le dieci azioni del piano la copertura stimata sale oltre il 90% entro giugno 2027, un mese prima della scadenza.

Sintesi per la direzione

58%
copertura dei requisiti applicabili

21
requisiti non conformi su 87

9
vulnerabilità sfruttate attivamente (CISA KEV)

23
account Microsoft 365 senza MFA, su 187



34 conformi · 27 parziali · 21 non conformi · 5 non applicabili

Copertura = (conformi + metà dei parziali) / requisiti applicabili = (34 + 13,5) / 82.

Copertura per funzione



In giallo le funzioni sotto il 50%.

Piano delle priorità

Ordinato per rischio ridotto e sforzo richiesto: le prime due azioni chiudono le esposizioni più gravi in poche settimane. Le sigle indicano la funzione e la categoria del Framework Nazionale.

#	AZIONE	MISURA	GRAVITÀ	SFORZO	RESPONSABILE	ENTRO
1	MFA su tutti gli account Microsoft 365 e sulla VPN (23 account scoperti)	PR.AA	Critica	Basso	Resp. IT	30/11/2026
2	Aggiornare firewall e 3 server esposti alle 9 vulnerabilità in KEV	ID.RA · PR.PS	Critica	Basso	Resp. IT	15/12/2026
3	Delibera del CdA su misure, ruoli e punto di contatto	GV.RR	Alta	Basso	Direzione	31/01/2027
4	Analisi del rischio documentata e approvata	GV.RM	Alta	Medio	Resp. IT + Direzione	28/02/2027
5	Procedura incidenti con notifica 24h / 72h e reperibilità	RS.MA · RS.CO	Alta	Medio	Resp. IT	28/02/2027
6	Test di ripristino dei backup, ripetuto ogni sei mesi e verbalizzato	PR.DS · RC.RP	Alta	Medio	Fornitore sistemistico	31/03/2027
7	Valutazione di sicurezza dei 4 fornitori in fascia alta e clausole nei contratti	GV.SC	Media	Medio	Acquisti	31/03/2027
8	Formazione su rischi cyber per vertici e personale	PR.AT	Media	Basso	Personale	30/04/2027
9	Raccolta centralizzata dei log e soglie di allarme	DE.CM	Media	Medio	Resp. IT	31/05/2027
10	Dismettere o isolare i 4 server con sistema operativo fuori supporto	PR.PS	Media	Alto	Resp. IT	30/06/2027

Calendario fino alla scadenza

nov – dic 2026

Esposizioni gravi

Azioni 1–2: MFA e vulnerabilità sfruttate

gen – mar 2027

Governo e procedure

Azioni 3–7: delibera, rischio, incidenti, backup, fornitori

apr – giu 2027

Presidio

Azioni 8–10: formazione, log, server obsoleti

lug 2027

Verifica

Nuova gap analysis e aggiornamento del dossier prima del 31 luglio

Scadenze annuali sulla Piattaforma NIS già a calendario: dichiarazione dal 1° gennaio al 28 febbraio, dati e fornitori dal 15 aprile al 31 maggio, categorizzazione di attività e servizi dal 1° maggio al 30 giugno.

Gap analysis e fornitori

Estratto di 8 requisiti su 87. Nel dossier completo ogni riga porta l'evidenza allegata e la data in cui è stata raccolta.

MISURA	REQUISITO	ESITO	EVIDENZA
ID.AM	Inventario aggiornato di hardware e dispositivi	Conforme	Inventario dall'agent: 196 dispositivi, aggiornato ogni giorno
ID.AM	Inventario del software in uso	Conforme	Inventario dall'agent: 3.912 pacchetti e applicazioni con versione
PR.AA	Autenticazione a più fattori per gli accessi critici	Parziale	Microsoft 365: 164 account su 187 con MFA; VPN senza secondo fattore
PR.PS	Software mantenuto e aggiornato	Non conforme	4 server fuori supporto; 9 vulnerabilità in KEV non corrette
PR.DS	Backup protetti e verificati	Parziale	Backup giornaliero su NAS; nessun test di ripristino registrato
DE.CM	Monitoraggio di reti e sistemi	Non conforme	Log solo sulle singole macchine, nessuna soglia di allarme
GV.SC	Gestione del rischio dei fornitori	Parziale	12 fornitori censiti, 4 in fascia alta, 2 contratti senza clausole di sicurezza
PR.AA	Controllo degli accessi fisici alla sala server	Non applicabile	Nessuna sala server propria: i server sono in colocation presso il fornitore sistemistico, verificato sul contratto

Registro fornitori · estratto

FORNITORE	SERVIZIO	FASCIA	QUESTIONARIO	CONTRATTO E DPA
Fornitore ERP	Gestionale in cloud, dati di clienti e ordini	Alta	Inviato il 27/10	DPA firmato, clausole di sicurezza da integrare
Assistenza sistemistica	Gestione server e backup, accesso amministrativo	Alta	Completato, 74/100	DPA firmato
Manutentore macchine CNC	Teleassistenza sulle linee di produzione	Alta	Inviato il 27/10	Nessuna clausola di sicurezza
Posta e collaborazione	Microsoft 365	Alta	Certificazioni acquisite	Condizioni standard del fornitore
Consulente paghe	Elaborazione cedolini, dati del personale	Media	Da inviare	DPA firmato

Capitolo 3 · segue

Il dossier di accountability

È il documento che il responsabile IT porta in direzione e che si mostra in caso di verifica. Resta collegato alla piattaforma: ogni nuova esportazione riporta lo stato del giorno.

Indice del dossier

1. Perimetro, qualifica e allegato applicabile
2. Governo: ruoli, punto di contatto, delibere
3. Inventario di dispositivi, software e servizi
4. Gap analysis requisito per requisito, con le evidenze
5. Vulnerabilità prioritizzate (KEV, EPSS)
6. Registro dei fornitori e questionari
7. Piano di adeguamento con responsabili e date
8. Bozza della procedura di gestione e notifica degli incidenti
9. Calendario degli adempimenti sulla Piattaforma NIS

Esportazione

Formati: PDF per la lettura, JSON per i sistemi, ZIP con PDF, indice e file allegati.

Impronta sha256 dell'esportazione d'esempio:

`9c41e7d0b2a85f36e1c4d97a0f2b68e35d7a1c90b4e2f8a63d05c7b19e4a2f71`

L'impronta permette di dimostrare che il documento consegnato non è stato modificato.

Prossimi passi

1

Incontro conoscitivo

Gratuito: capiamo il tuo perimetro e se l'assessment è il passo giusto.

2

Preventivo

Su misura per numero di dispositivi e sedi, con le date di avvio disponibili. Ne avviamo un numero limitato ogni mese.

3

Avvio

Riunione di avvio e, dieci giorni lavorativi dopo, la restituzione con il dossier.

Richiedi l'assessment dal modulo contatti: `reterea.com/contatti?richiesta=assessment`

Il dossier documenta lo stato delle misure di sicurezza e le priorità di intervento: non è un'attestazione di conformità né una consulenza legale. Per gli obblighi fanno fede i testi ufficiali pubblicati su acn.gov.it e la comunicazione individuale dell'ACN, che stabilisce le scadenze effettive. Riferimenti: D.Lgs. 4 settembre 2024, n. 138; Determinazione ACN 379907/2025 (misure di base). Sherlock Guard è un prodotto Reterea s.r.l.