SYNSPHERE

WHITE PAPER · GIUGNO 2026

NIS2 per le PMI italiane: guida operativa alla conformità con lo stack Microsoft

Perimetro, obblighi dell'art. 21, misure tecniche con Microsoft 365 e Azure, roadmap di adeguamento in 90 giorni.

In sintesi

La NIS2 estende gli obblighi di cybersicurezza a un numero molto più ampio di imprese italiane e, con l'effetto filiera, raggiunge anche le PMI formalmente fuori perimetro. Questo white paper spiega chi rientra fra soggetti essenziali e importanti secondo il D.Lgs. 138/2024, quali responsabilità ricadono sugli organi di gestione e come funzionano le notifiche degli incidenti al CSIRT Italia. Le dieci misure dell'articolo 21 vengono tradotte in azioni concrete e mappate sugli strumenti Microsoft 365, Defender, Entra, Intune e Purview che molte PMI hanno già in licenza. Chiudono il documento una roadmap di adeguamento in 90 giorni e una checklist operativa pronta all'uso.

NIS2 per le PMI italiane: guida operativa alla conformità con lo stack Microsoft — Prima edizione: giugno 2026.

Indice

1. NIS2 in breve: perché riguarda anche le PMI italiane

La NIS2 (direttiva UE 2022/2555) è la normativa europea sulla cybersicurezza che sostituisce la prima direttiva NIS del 2016. In Italia è stata recepita con il **decreto legislativo 138/2024**, in vigore da ottobre 2024, che designa l'Agenzia per la Cybersicurezza Nazionale (ACN) come autorità competente. Rispetto alla prima NIS il salto è netto: i settori coperti aumentano in modo considerevole, le soglie dimensionali si abbassano fino a includere le medie imprese e gli obblighi diventano concreti e verificabili, con misure minime di sicurezza, scadenze precise per la notifica degli incidenti e sanzioni che possono incidere sul fatturato.

La norma distingue due categorie di organizzazioni: i **soggetti essenziali** e i **soggetti importanti**. La differenza non sta tanto negli obblighi di sicurezza, in larga parte identici, quanto nell'intensità della vigilanza e nel tetto delle sanzioni. Rientrano nel perimetro le organizzazioni che operano nei settori elencati negli allegati al decreto — tra gli altri energia, trasporti, sanità, acqua, infrastrutture digitali e gestione di servizi ICT, spazio, servizi postali, gestione dei rifiuti, chimica, agroalimentare, fabbricazione di prodotti critici come dispositivi medici, elettronica, macchinari e autoveicoli, fornitori di servizi digitali e ricerca — e che superano determinate soglie dimensionali. In linea generale il perimetro parte dalle **medie imprese** (almeno 50 dipendenti oppure più di 10 milioni di euro di fatturato o bilancio annuo), ma alcune categorie rientrano a prescindere dalla dimensione, come certi fornitori di infrastrutture digitali e i soggetti identificati come critici dalle autorità.

Categoria	Chi rientra in sintesi	Vigilanza e sanzioni
Soggetti essenziali	Grandi imprese dei settori ad alta criticità; alcune categorie a prescindere	Vigilanza anche preventiva; sanzioni fino a 10 milioni di euro o 2% del fatturato, se superiore
Soggetti importanti	Medie imprese dei settori ad alta criticità e imprese degli altri settori critici	Vigilanza successiva; sanzioni fino a 7 milioni di euro o 1,4% del fatturato

Chi rientra nel perimetro deve **registrarsi sulla piattaforma digitale dell'ACN** nelle finestre temporali previste ogni anno e mantenere aggiornate le informazioni comunicate. Gli obblighi seguono poi il calendario fissato dalle determinazioni dell'Agenzia, che concentrano nel 2026 le scadenze principali: gli obblighi di notifica degli incidenti sono già operativi, mentre le misure di sicurezza di base devono essere implementate entro i termini indicati dall'ACN. Chi non è certo di rientrare dovrebbe comunque documentare la propria valutazione: in caso di controlli, dimostrare di essersi posti la domanda con metodo è molto diverso dall'averla ignorata.

C'è poi un secondo perimetro, informale ma molto concreto: l'**effetto filiera**. La NIS2 impone ai soggetti obbligati di presidiare la sicurezza della propria catena di approvvigionamento. Il risultato è che sempre più spesso le PMI italiane che non rientrano direttamente nel perimetro si vedono recapitare questionari di sicurezza e clausole contrattuali da parte dei clienti soggetti NIS2. In pratica la conformità diventa un requisito commerciale prima ancora che un obbligo normativo: chi non sa rispondere rischia di perdere commesse, chi risponde bene si differenzia. È il motivo per cui questa guida riguarda anche, e forse soprattutto, le PMI formalmente fuori perimetro.

Per una prima autovalutazione del livello di preparazione rispetto alle misure richieste, SynSphere mette a disposizione gratuitamente lo strumento NIS2 Self-Assessment (synsphere.it/strumenti/nis2-self-assessment): dodici domande sulle quattro aree chiave

dell'articolo 21, con un report immediato delle priorità su cui intervenire.

> **Nota importante**
> Questo documento ha finalità informative e **non costituisce consulenza legale**. La determinazione esatta del perimetro di applicazione, della categoria di appartenenza e degli obblighi specifici richiede una valutazione puntuale della singola organizzazione, da svolgere con il supporto di un legale specializzato in diritto delle nuove tecnologie.

2. Sanzioni e responsabilità degli organi di gestione

Il regime sanzionatorio è uno dei motivi per cui la NIS2 è arrivata sui tavoli dei consigli di amministrazione. Per i **soggetti essenziali** le sanzioni amministrative pecuniarie arrivano fino a **10 milioni di euro o al 2% del fatturato mondiale annuo**, se superiore; per i **soggetti importanti** fino a **7 milioni di euro o all'1,4% del fatturato mondiale annuo**. A queste si aggiungono i poteri dell'ACN: ispezioni, richieste di informazioni ed evidenze, diffide con termini perentori, ordini vincolanti di adeguamento e sanzioni ulteriori in caso di mancata collaborazione.

Per i soggetti essenziali, nei casi più gravi di inosservanza reiterata, l'autorità può arrivare a misure che colpiscono direttamente le persone: la sospensione temporanea di certificazioni o autorizzazioni relative ai servizi erogati e l'**incapacità temporanea a ricoprire funzioni dirigenziali** per le persone fisiche che esercitano responsabilità di vertice. Non è un dettaglio teorico: significa che un amministratore delegato può essere temporaneamente interdetto dal proprio ruolo per inadempienze di cybersicurezza dell'azienda che guida.

Il punto più innovativo riguarda però la **responsabilità degli organi di gestione**. La norma stabilisce che gli organi di amministrazione e direttivi:

- **approvano** le modalità di implementazione delle misure di gestione dei rischi informatici;
- **sovrintendono** all'attuazione degli obblighi e rispondono delle violazioni;
- **seguono una formazione specifica** in materia di sicurezza informatica e promuovono una formazione analoga, su base periodica, per i dipendenti.

In pratica la cybersicurezza esce dal perimetro dell'ufficio IT ed entra formalmente nell'agenda del consiglio. Per una PMI questo si traduce in alcune abitudini nuove ma sostenibili: inserire la sicurezza informatica come punto ricorrente nelle riunioni di direzione, approvare e **verbalizzare** il piano di adeguamento e la politica di sicurezza, assegnare un budget dedicato, nominare un referente interno con un mandato chiaro e tracciare la formazione svolta dagli amministratori. Il verbale che documenta una decisione consapevole, con le sue motivazioni, è la prima evidenza che un organo di gestione può esibire in caso di verifica.

Va detto che la sanzione massima non è il punto di partenza: il percorso tipico passa da richieste di informazioni, diffide e termini per l'adeguamento. È però un percorso in cui la differenza la fa la documentazione: chi può esibire un piano approvato, evidenze di attuazione e una collaborazione tempestiva con l'autorità si trova in una posizione molto diversa da chi deve ricostruire tutto a posteriori. Anche le polizze cyber, sempre più diffuse fra le PMI, spingono nella stessa direzione: i questionari assuntivi chiedono in larga parte le stesse misure richieste dalla NIS2 — MFA, backup, piano di risposta agli incidenti — e premiano chi le ha già implementate con condizioni migliori.

Un ultimo chiarimento, importante per chi lavora abitualmente con partner esterni: la responsabilità non si trasferisce delegando. Affidare la gestione dell'IT a un fornitore, anche qualificato, non sposta gli obblighi: il soggetto resta responsabile delle misure, della loro verifica periodica e delle notifiche alle autorità. Il fornitore giusto aiuta a progettare le misure e a costruire le evidenze, ma non sostituisce la governance interna. Diffidate di chi promette la conformità chiavi in mano senza coinvolgere la direzione.

3. Le misure dell'articolo 21 spiegate in pratica

L'articolo 21 della direttiva, recepito dal decreto italiano con un elenco corrispondente, definisce le **misure minime di gestione dei rischi** che tutti i soggetti, essenziali e importanti, devono adottare. L'impostazione è **multirischio**: non solo attacchi informatici, ma anche guasti, errori umani ed eventi fisici o naturali che possono compromettere reti e sistemi informativi. Vale inoltre il principio di **proporzionalità**: le misure vanno commisurate alla dimensione dell'organizzazione, alla sua esposizione ai rischi, alla probabilità che gli incidenti si verifichino e alla loro potenziale gravità. Ecco le dieci famiglie di misure, tradotte in linguaggio operativo:

1. **Politiche di analisi dei rischi e di sicurezza dei sistemi informativi** — un documento approvato dalla direzione che definisce come l'azienda identifica, valuta e tratta i rischi cyber, con riesame periodico.
2. **Gestione degli incidenti** — procedure scritte per rilevare, classificare, contenere e notificare gli incidenti, con ruoli, contatti e tempi definiti prima che l'incidente accada.
3. **Continuità operativa e gestione delle crisi** — backup testati, disaster recovery e un piano per continuare a operare anche durante un attacco o un guasto grave.
4. **Sicurezza della catena di approvvigionamento** — valutazione dei fornitori diretti e dei prestatori di servizi, con requisiti di sicurezza portati dentro i contratti.
5. **Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi** — gestione delle vulnerabilità, aggiornamenti regolari e canali per la divulgazione coordinata delle falle.
6. **Politiche e procedure per valutare l'efficacia delle misure** — audit interni, test e indicatori: non basta adottare le misure, bisogna poter dimostrare che funzionano.
7. **Igiene informatica di base e formazione** — password robuste, aggiornamenti, consapevolezza del phishing: pratiche di base estese a tutto il personale, nessuno escluso.
8. **Crittografia e cifratura** — politiche e procedure sull'uso della crittografia per proteggere i dati, sia archiviati sia in transito.
9. **Sicurezza delle risorse umane, controllo degli accessi e gestione degli attivi** — chi accede a cosa e perché, inventario di dispositivi e dati, revoca degli accessi quando una persona esce.
10. **Autenticazione a più fattori e comunicazioni protette** — soluzioni di MFA o autenticazione continua, comunicazioni vocali, video e testuali protette e sistemi di comunicazione di emergenza interni.

Una chiave di lettura utile per pianificare il lavoro: le misure 1, 2 e 6 sono prevalentemente **organizzative** (documenti, procedure, verifiche), le misure 3, 5, 8, 9 e 10 sono prevalentemente **tecniche**, le misure 4 e 7 sono **trasversali**, perché coinvolgono fornitori e persone. Nei progetti di adeguamento seguiti da SynSphere sulle PMI italiane il divario maggiore non è quasi mai tecnologico: chi usa Microsoft 365 con un piano adeguato ha già in licenza gran parte degli strumenti richiesti dalle misure tecniche. Quello che manca, di solito, è la parte documentale e organizzativa: politiche scritte e approvate, registri aggiornati, procedure provate almeno una

volta, evidenze raccolte in modo sistematico.

Un'ultima avvertenza sulle specifiche tecniche: l'ACN ha pubblicato determinazioni che dettagliano le misure di sicurezza di base, articolate in controlli puntuali, e i relativi termini di adeguamento. Il testo della direttiva è la cornice; il lavoro vero si gioca sui controlli specifici, sulla loro attuazione e sulla capacità di dimostrarla con evidenze datate e firmate.

4. Mappatura: dalle misure dell'articolo 21 allo stack Microsoft

Per una PMI che lavora già su Microsoft 365 la domanda corretta non è quali prodotti comprare, ma **quali funzionalità attivare** fra quelle in gran parte già incluse nelle licenze o attivabili come servizi aggiuntivi. La tabella che segue mappa le dieci misure dell'articolo 21 sui componenti dello stack Microsoft più rilevanti per una PMI: è il punto di partenza della gap analysis tecnica.

Misura art. 21	Strumenti Microsoft	In pratica
Analisi dei rischi	Secure Score, Defender Vulnerability Management	Baseline misurabile della postura di sicurezza e delle vulnerabilità
Gestione incidenti	Defender XDR, Microsoft Sentinel	Incidenti correlati su email, endpoint e identità; SIEM cloud per indagini
Continuità operativa	Azure Backup, Azure Site Recovery	Backup protetti dalla cancellazione e ripristino di sistemi e VM
Supply chain	Entra ID (guest, access review)	Governance degli accessi di fornitori, consulenti ed esterni
Vulnerabilità e patching	Intune, Windows Autopatch	Aggiornamenti gestiti di sistemi e applicazioni su tutto il parco
Verifica efficacia	Secure Score, report Defender e Purview	Indicatori e report periodici per audit e riesami di direzione
Igiene e formazione	Attack Simulation Training	Campagne di phishing simulato con formazione mirata a chi clicca
Crittografia	BitLocker, Microsoft Purview	Cifratura dei dispositivi e protezione dei documenti sensibili
Accessi e asset	Entra ID, Conditional Access, Intune	Controllo degli accessi, inventario dei dispositivi, offboarding
MFA e comunicazioni	Entra MFA, Microsoft Teams	Autenticazione forte e comunicazioni cifrate in transito

Sul piano delle licenze, **Microsoft 365 Business Premium** è il punto di equilibrio per la maggior parte delle PMI in perimetro o in filiera: include Entra ID P1 con Conditional Access, Microsoft Intune per la gestione di dispositivi e aggiornamenti, Defender for Business per la protezione degli endpoint, Defender for Office 365 per email e collaborazione e le funzionalità di base di Microsoft Purview per l'etichettatura e la protezione delle informazioni. Le esigenze più avanzate — un SIEM come Microsoft Sentinel, le versioni superiori dei piani Defender (Attack Simulation Training, ad esempio, richiede Defender per Office 365 Piano 2), le funzioni avanzate di Purview

per audit e conservazione estesa dei log — richiedono piani enterprise o componenti aggiuntivi, da valutare in base al profilo di rischio. Una panoramica dei piani è disponibile nella pagina dedicata a Microsoft 365 Business Premium (synsphere.it/licenze-microsoft-365/business-premium).

Per chi ha anche server e workload in cloud, il versante Azure completa il quadro: **Microsoft Defender for Cloud** valuta e migliora la postura di sicurezza delle risorse, **Azure Backup** fornisce copie di sicurezza con protezione dalla cancellazione accidentale o malevola, **Azure Site Recovery** replica i sistemi critici per il disaster recovery. Sono gli strumenti naturali per dare sostanza alla misura sulla continuità operativa quando l'infrastruttura non si esaurisce in Microsoft 365.

Il consiglio SynSphere

Prima di acquistare nuovi prodotti di sicurezza, fate l'inventario di ciò che le licenze Microsoft già includono. Nei progetti di ottimizzazione SynSphere ha ottenuto in media un **-30% sui costi di licensing** proprio razionalizzando piani e componenti aggiuntivi: molto spesso la misura NIS2 che manca non richiede un nuovo acquisto, ma l'attivazione e la configurazione di una funzionalità già pagata e mai usata.

5. Analisi e gestione del rischio: da dove partire

L'analisi dei rischi è la prima misura dell'elenco e il fondamento di tutte le altre: senza sapere quali asset esistono, quali dati contano davvero e quali scenari possono fermare l'operatività, ogni investimento in sicurezza è una scommessa. Per una PMI non serve una metodologia accademica: serve un percorso ripetibile in quattro passi, documentato a ogni passaggio.

Passo 1: inventario di asset, identità e dati

Non si protegge ciò che non si conosce. Lo stack Microsoft offre già le fonti per il censimento: **Entra ID** per utenti, amministratori e applicazioni collegate al tenant; **Intune** per l'inventario dei dispositivi e del loro stato di conformità; SharePoint e **Microsoft Purview** per capire dove risiedono i dati e quali sono sensibili. A questo va affiancata una mappa dei processi critici di business: quali attività non possono fermarsi, da quali sistemi, persone e fornitori dipendono.

Passo 2: valutazione e registro dei rischi

Per ogni scenario rilevante — ransomware, compromissione di una casella email aziendale, perdita o esfiltrazione di dati, indisponibilità prolungata di un fornitore, errore umano su un sistema critico — si stimano probabilità e impatto su una scala semplice e si decide il trattamento: **mitigare** con misure tecniche o organizzative, **trasferire** il rischio, per esempio con una polizza cyber, **accettarlo** formalmente quando è dentro la soglia di tolleranza o **evitarlo** cambiando processo. Il risultato è il registro dei rischi: un documento vivo, con un responsabile per ogni rischio e una data di riesame.

Passo 3: una baseline misurabile con Secure Score

Microsoft Secure Score fotografa la postura di sicurezza del tenant e propone azioni di miglioramento ordinate per impatto; **Microsoft Defender Vulnerability Management** fa lo stesso sulle vulnerabilità dei dispositivi. Nessuno dei due equivale alla conformità NIS2, ma insieme offrono esattamente ciò che un audit chiede: un punteggio iniziale, obiettivi trimestrali e la prova oggettiva di un miglioramento continuo. Fissare un target e rivederlo ogni trimestre in un riesame di direzione è una delle pratiche più semplici ed efficaci che una PMI possa adottare.

Passo 4: la politica di sicurezza scritta e approvata

Il percorso si chiude con la **politica di sicurezza delle informazioni**: il documento, approvato dalla direzione, che fissa principi, responsabilità e regole operative — uso dei dispositivi, gestione di password e MFA, classificazione dei dati, comportamento in caso di incidente. Per non partire dal foglio bianco è disponibile un template di policy di sicurezza informatica (synsphere.it/download/template-word-policy-sicurezza-informatica) in formato Word, da adattare alla propria realtà. La politica va riesaminata almeno una volta all'anno e dopo ogni incidente significativo: una policy ferma da tre anni, in un controllo, è quasi peggio di una policy assente.

6. Gestione e notifica degli incidenti: 24 ore, 72 ore, un mese

Gli obblighi di notifica sono la parte della NIS2 con le scadenze più stringenti, pensate per dare alle autorità visibilità tempestiva sugli incidenti in corso. L'obbligo scatta per gli **incidenti significativi**: quelli che causano o possono causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto, oppure ripercussioni considerevoli su altre persone fisiche o giuridiche, con danni materiali o immateriali. Le tappe verso il **CSIRT Italia**, la squadra nazionale di risposta agli incidenti che opera presso l'ACN, sono queste:

Scadenza	Adempimento	Contenuto in sintesi
Entro 24 ore	Pre-allarme al CSIRT Italia	Prima segnalazione; indicare il sospetto di atti illeciti o impatti transfrontalieri
Entro 72 ore	Notifica dell'incidente	Aggiornamento con valutazione iniziale di gravità, impatto e indicatori disponibili
Su richiesta	Relazione intermedia	Aggiornamenti di stato richiesti dal CSIRT durante la gestione dell'incidente
Entro 1 mese dalla notifica	Relazione finale	Descrizione dettagliata, causa probabile, misure adottate, eventuale impatto estero

Le notifiche viaggiano attraverso i canali e la piattaforma indicati dall'ACN. In parallelo possono scattare obblighi di **comunicazione ai destinatari dei servizi**: se l'incidente può incidere sui clienti, questi vanno informati senza ingiustificato ritardo, e in presenza di una minaccia significativa vanno indicate anche le misure che i destinatari stessi possono adottare per proteggersi. Se l'incidente coinvolge dati personali si aggiunge il binario GDPR verso il Garante privacy, con la sua scadenza di 72 ore: due notifiche distinte, con contenuti diversi, da gestire in

modo coordinato.

Ventiquattro ore sono poche, e gli incidenti hanno la sgradevole tendenza a manifestarsi il venerdì sera o sotto le feste. L'unico modo per rispettare i tempi è avere **prima** un piano di risposta agli incidenti scritto: chi decide, chi comunica, chi chiama il legale e l'assicurazione, quali runbook seguire per gli scenari più probabili, dove si trovano i recapiti del CSIRT e le credenziali per la piattaforma di notifica. Per non partire da zero, SynSphere ha pubblicato un template di Incident Response Plan in Word (synsphere.it/download/template-word-incident-response-plan-pmi) pensato per le PMI: si compila, si adatta e si fa approvare alla direzione.

Gli strumenti Microsoft aiutano soprattutto nella ricostruzione dei fatti, che è ciò che le notifiche richiedono: **Defender XDR** correla automaticamente i segnali provenienti da email, endpoint e identità in incidenti unici, con una timeline leggibile anche da chi non è un analista; l'**audit log di Microsoft Purview** traccia le attività di utenti e amministratori; **Microsoft Sentinel**, dove presente, conserva i log con la retention necessaria e permette ricerche mirate. La condizione è una sola: log e audit devono essere abilitati e conservati prima dell'incidente, perché attivarli dopo non restituisce il passato.

> **Il consiglio SynSphere**
> Fate almeno una **simulazione tabletop** all'anno: un incidente finto — un ransomware su un file server, una casella di posta compromessa — gestito sul serio attorno a un tavolo, cronometrando le scadenze di notifica. È l'unico modo per scoprire prima, e non durante, che il referente non sa chi chiamare alle 22 di venerdì o che nessuno ricorda dove sono le credenziali della piattaforma di notifica.

7. Supply chain: l'effetto filiera e le clausole verso i fornitori

La sicurezza della catena di approvvigionamento è la misura che più distingue la NIS2 dalle normative precedenti, perché scavalca i confini dell'azienda. Va letta in due direzioni: come soggetti obbligati che devono governare i propri fornitori, e come fornitori che devono saper rispondere ai clienti obbligati. Per molte PMI italiane la seconda direzione arriva prima della prima.

Se siete in perimetro: governare i fornitori

L'obbligo è valutare e presidiare la sicurezza dei fornitori diretti e dei prestatori di servizi, tenendo conto delle loro vulnerabilità e della qualità complessiva delle loro pratiche di cybersicurezza. In concreto significa:

- censire i **fornitori critici**: chi accede a sistemi o dati aziendali e chi eroga servizi da cui dipendono i processi essenziali — gestionale, cloud, manutenzione IT, logistica;
- valutarli con un **questionario proporzionato** al rischio: misure adottate, MFA, backup, gestione degli incidenti, eventuali certificazioni di sicurezza;
- inserire nei contratti **clausole di sicurezza**: obbligo di notifica tempestiva al cliente degli incidenti che lo riguardano, misure minime richieste, diritto di verifica, regole sui subfornitori e condizioni di uscita ordinata con restituzione dei dati;

- riesaminare periodicamente le valutazioni, non solo al momento della firma: il profilo di rischio di un fornitore cambia nel tempo.

Se siete fornitori di soggetti NIS2: l'effetto filiera

Se i vostri clienti rientrano nel perimetro, i loro obblighi diventano le vostre richieste: questionari di sicurezza da compilare, clausole contrattuali da accettare, evidenze da produrre. Conviene prepararsi in anticipo con un **dossier di sicurezza** sintetico e onesto: quali misure avete adottato, come gestite MFA e backup, se avete un piano di risposta agli incidenti, come formate il personale. Chi risponde in modo rapido e credibile trasforma un adempimento in un vantaggio commerciale; chi improvvisa la risposta a ogni questionario perde tempo e credibilità. Il tema è approfondito nella guida dedicata NIS2 e fornitori di filiera: gli obblighi per le PMI non soggette (synsphere.it/notizie/nis2-fornitori-filiera-pmi-non-soggette-obblighi).

Sul piano tecnico, il punto di contatto fra supply chain e operatività quotidiana è la gestione degli **accessi di terze parti**: account guest in Entra ID al posto di credenziali condivise, **access review** periodiche (richiedono Entra ID P2 o Entra ID Governance) per verificare che gli accessi esterni siano ancora necessari, Conditional Access con MFA anche per consulenti e fornitori, e dismissione delle VPN permanenti non monitorate dove esistono alternative più controllabili. Ogni accesso esterno dimenticato è una porta lasciata aperta nella vostra filiera — e, in caso di incidente, una domanda scomoda a cui rispondere.

Un'attenzione particolare merita infine la **concentrazione del rischio ICT**: se gestionale, posta, backup e assistenza dipendono tutti dallo stesso fornitore, la sua indisponibilità diventa automaticamente il vostro incidente. Non sempre diversificare è possibile o conveniente, ma la dipendenza va almeno resa esplicita nel registro dei rischi, con una **exit strategy** scritta: dove sono i dati, in quale formato si possono riottenere, in quanto tempo e a quali condizioni economiche. Sono domande da fare al fornitore quando il rapporto è sereno, non nel mezzo di una crisi o di una disdetta.

8. Formazione del personale e governance: il fattore umano

Le pratiche di igiene informatica di base e la formazione sono una misura esplicita dell'articolo 21, e per gli organi di gestione la formazione è un obbligo diretto. Il punto debole, nella maggior parte delle organizzazioni, non è la mancanza di un corso: è l'assenza di un **programma**. La formazione una tantum si dimentica in poche settimane; quella periodica, misurata e collegata a esempi reali cambia i comportamenti. Un programma sostenibile per una PMI prevede:

- **organi di gestione**: una sessione dedicata a responsabilità, scenari di rischio e decisioni da prendere, da ripetere quando cambiano la norma o l'azienda;
- **tutto il personale**: formazione annuale su phishing, gestione di password e MFA, trattamento dei dati e modalità di segnalazione degli incidenti;
- **micro-formazione continua**: pillole brevi e simulazioni distribuite nell'anno, al posto della maratona annuale;
- **ruoli tecnici**: approfondimenti specifici per chi amministra sistemi, identità e backup;
- **ingressi e uscite**: un modulo di sicurezza nell'onboarding dei nuovi assunti e una procedura di offboarding che revoca accessi e dispositivi lo stesso giorno.

Per la parte pratica, **Attack Simulation Training** in Microsoft Defender for Office 365 — che richiede il Piano 2, incluso nei piani enterprise come E5 o disponibile come componente aggiuntivo — permette di lanciare campagne di phishing simulato e di assegnare automaticamente moduli formativi a chi cade nella trappola. Le metriche da seguire sono due: il tasso di clic, che deve scendere nel tempo, e il tasso di segnalazione da parte degli utenti, che deve salire. La seconda è la più importante: una segnalazione tempestiva accorcia i tempi di rilevamento e, di conseguenza, rende più realistico rispettare le scadenze di notifica.

Alla formazione va affiancato un canale di segnalazione semplice: il pulsante per segnalare i messaggi sospetti integrato in Outlook, una casella dedicata o un contatto diretto con il referente per la sicurezza. Le persone segnalano se segnalare è facile e se non vengono colpevolizzate quando sbagliano: una cultura punitiva produce solo silenzio, e il silenzio allunga i tempi di rilevamento degli incidenti veri.

La governance tiene insieme tutto il resto: un referente per la sicurezza con un mandato formale, un momento periodico di riesame — rischi, Secure Score, incidenti e quasi-incidenti, fornitori — e un **registro della formazione** con date, partecipanti e contenuti. In un controllo dell'ACN, un registro firmato e aggiornato vale più di qualunque dichiarazione di intenti.

La formazione è uno dei pilastri storici di SynSphere: oltre **5.000 ore erogate** e più di **800 professionisti formati**, con il **95% di soddisfazione** nei corsi. Per strutturare un percorso interno sui temi della sicurezza è disponibile gratuitamente il percorso formativo Security (synsphere.it/formazione/percorsi/security), mentre per il finanziamento conviene valutare i fondi interprofessionali: molte PMI li versano già in busta paga senza mai utilizzarli.

9. Roadmap di adeguamento in 90 giorni

Novanta giorni sono un orizzonte realistico per portare una PMI che usa già Microsoft 365 da una situazione non presidiata a una posizione difendibile. Non significa completare tutto: significa mettere in fila le misure a maggiore riduzione del rischio, con responsabilità chiare e date certe. Le tre fasi che seguono presuppongono un tenant Microsoft 365 esistente; chi parte da infrastrutture miste dovrà aggiungere il versante server e rete, ma la logica non cambia: prima la visibilità, poi i controlli tecnici, poi le procedure e le persone.

Giorni 1-30: capire e decidere

- eseguire l'autovalutazione del perimetro (settore, dimensioni, posizione in filiera) e documentarla, anche con il supporto del legale;
- nominare il referente per la sicurezza e ottenere lo sponsor formale della direzione, con delibera verbalizzata;
- costruire l'inventario di identità, dispositivi e dati a partire da Entra ID, Intune e Purview;
- rilevare la baseline di Microsoft Secure Score e le vulnerabilità principali del parco macchine;
- redigere il primo registro dei rischi e la gap analysis rispetto alle dieci misure dell'articolo 21;
- verificare la registrazione sulla piattaforma ACN, se dovuta, e annotare le scadenze applicabili.

Giorni 31-60: chiudere i varchi tecnici

- attivare l'MFA per tutti gli utenti, amministratori per primi, con politiche di Conditional Access;

- proteggere la posta: record SPF, DKIM e DMARC corretti e politiche anti-phishing di Defender for Office 365;
- verificare i backup di dati e sistemi critici, compresi i dati di Microsoft 365, con almeno un test di ripristino documentato;
- cifrare i dispositivi con BitLocker gestito centralmente da Intune;
- impostare il patching gestito e ridurre i privilegi amministrativi non necessari;
- abilitare audit log e definire una retention adeguata alle esigenze di indagine.

Giorni 61-90: procedure, persone e fornitori

- approvare e comunicare la politica di sicurezza delle informazioni;
- completare l'Incident Response Plan, con scadenze di notifica e contatti, e collaudarlo con una simulazione tabletop;
- creare il registro dei fornitori critici e inserire le prime clausole di sicurezza nei contratti in rinnovo;
- erogare e registrare la formazione, per la direzione e per il personale;
- definire il piano di miglioramento continuo, con riesame trimestrale di rischi e Secure Score.

Fase	Focus	Risultato atteso
Giorni 1-30	Assessment e governance	Perimetro chiarito, referente nominato, registro rischi e gap analysis
Giorni 31-60	Misure tecniche prioritarie	MFA, email security, backup testati, cifratura e patching gestito
Giorni 61-90	Procedure e persone	Policy e IRP approvati, fornitori contrattualizzati, formazione registrata

Il consiglio SynSphere

Non puntate alla perfezione in 90 giorni: puntate alla **difendibilità**. Un percorso documentato, con priorità motivate e date certe, vale più di un progetto ambizioso fermo al 20%. È l'approccio che applichiamo sui **+150 tenant Microsoft 365** che gestiamo: prima le misure che riducono davvero il rischio — MFA, backup, sicurezza della posta — poi tutto il resto, con evidenze scritte a ogni passo.

10. Checklist operativa

La checklist che segue riassume il percorso del white paper in azioni verificabili. Ogni voce dovrebbe avere un responsabile e una data: una casella spuntata senza evidenza dietro non supera un audit. Usatela come base per il riesame trimestrale: la versione datata e firmata di questa lista, confrontata trimestre dopo trimestre, è essa stessa un'evidenza di miglioramento continuo.

Perimetro e governance

- Verificare settore e soglie dimensionali rispetto agli allegati del D.Lgs. 138/2024 e conservare la valutazione scritta

- Completare la registrazione sulla piattaforma ACN, se dovuta, nelle finestre temporali previste
- Nominare un referente per la sicurezza con mandato formale e portare il tema in direzione con cadenza fissa
- Far approvare e verbalizzare dalla direzione la politica di sicurezza e il piano di adeguamento
- Pianificare e registrare la formazione obbligatoria degli organi di gestione

Misure tecniche

- Attivare l'MFA per tutti gli utenti, amministratori inclusi, con politiche di Conditional Access
- Configurare SPF, DKIM e DMARC e le protezioni anti-phishing di Defender for Office 365
- Verificare i backup di dati e sistemi, compreso Microsoft 365, e documentare un test di ripristino
- Cifrare i dispositivi aziendali con BitLocker gestito da Intune
- Impostare il patching gestito e monitorare Secure Score con obiettivi trimestrali
- Limitare e censire gli account con privilegi amministrativi, separandoli dagli account di uso quotidiano
- Abilitare audit log e definire la retention necessaria per le indagini

Continuità operativa

- Mantenere un piano di continuità e disaster recovery aggiornato, con RPO e RTO definiti per i sistemi critici
- Conservare almeno una copia di backup isolata dalle credenziali di amministrazione ordinarie
- Programmare test di ripristino periodici e conservarne gli esiti documentati

Incidenti e notifiche

- Definire i criteri interni per riconoscere un incidente significativo
- Completare l'Incident Response Plan con ruoli, contatti e scadenze di notifica a 24 ore, 72 ore e un mese
- Censire canale, piattaforma e credenziali per la notifica al CSIRT Italia, e custodirli fuori dai sistemi a rischio
- Eseguire almeno una simulazione tabletop all'anno e verbalizzare le lezioni apprese

Supply chain

- Creare e mantenere il registro dei fornitori critici
- Inserire clausole di sicurezza e obblighi di notifica nei nuovi contratti e nei rinnovi
- Governare gli accessi guest e di terze parti con un riesame periodico degli accessi in Entra ID
- Preparare il dossier di risposta ai questionari di sicurezza dei clienti NIS2

Persone

- Erogare la formazione di base a tutto il personale e tenerne il registro firmato
- Avviare campagne di phishing simulato e misurare tasso di clic e tasso di segnalazione
- Formalizzare le procedure di onboarding e di offboarding sicuro degli account e dei dispositivi

Chi è SynSphere

SynSphere Italia è un partner Microsoft specializzato nelle piccole e medie imprese italiane. Dal 2008 affianchiamo le aziende su Microsoft 365, Azure, Dynamics 365, sicurezza informatica e formazione, con sedi operative a Milano (Segrate) e Bolzano.

+150	**+10.000**	**0**
tenant Microsoft 365 gestiti	utenti migrati	downtime medio nelle migrazioni
+5.000	**+800**	**95%**
ore di formazione erogate	professionisti formati	soddisfazione dei corsi

Vuoi una mano sui temi di questo white paper? Parliamone: **synsphere.it/contattaci** · **info@synsphere.com**. Sul sito trovi anche strumenti gratuiti di assessment, toolkit PowerShell, template operativi e il catalogo completo di corsi e certificazioni Microsoft.