DIFESA DIGITALE

WHITEPAPER OPERATIVO PER PMI E AZIENDE ITALIANE

Guida alla Cyber Resilienza 2026

Come costruire protezione, continuità e governance in un panorama di minacce sempre più complesso.

Questa guida offre un modello pratico per valutare, rafforzare e governare la sicurezza digitale della tua organizzazione con un approccio strutturato e sostenibile. È pensata per imprenditori, manager, CIO, IT e responsabili della sicurezza che devono affrontare il 2026 con metodo e consapevolezza.

Difesa Digitale
ISGroup S.r.l.

Versione 1.0
2026

INDICE

Un percorso pratico per costruire resilienza

INTRODUZIONE

Perché la resilienza è il nuovo requisito minimo

La trasformazione digitale ha ampliato le opportunità di crescita per le aziende italiane, ma ha anche aumentato la loro esposizione a minacce sempre più sofisticate.

Nel 2026 la sicurezza non può più essere considerata un insieme di controlli tecnici. Deve diventare un elemento strutturale del business: la resilienza digitale.

Questa guida nasce con tre obiettivi fondamentali:

1. Fornire un approccio pratico per avviare o migliorare la resilienza digitale, indipendentemente dal livello di maturità attuale.
2. Rendere comprensibili concetti complessi, traducendo temi tecnici in indicazioni utili per imprenditori, direzioni aziendali, responsabili IT e figure operative.
3. Offrire un modello replicabile, applicabile alle PMI italiane che devono proteggere dati, continuità e reputazione in un contesto competitivo e regolamentato.

Sicurezza IT e Cyber Resilienza: qual è la differenza?

La sicurezza IT è focalizzata sugli strumenti: antivirus, firewall, backup, patching. La cyber resilienza è focalizzata sul funzionamento del business anche in presenza di attacchi o incidenti.

Sicurezza IT	Cyber Resilienza
Protegge i sistemi	Protegge continuità, dati e reputazione
Approccio tecnico	Approccio organizzativo e tecnico
Reattiva	Preventiva, misurabile, governata
Limitata all'IT	Coinvolge direzione, processi e persone

INTRODUZIONE

Le aziende resilienti prevedono il rischio, riducono l'impatto di un incidente, mantengono continuità operativa e dimostrano sicurezza a clienti e partner.

CAPITOLO 1

Il panorama delle minacce 2026

Il 2026 segna una fase di ulteriore intensificazione del cyber-crime. Le minacce sono più veloci, automatizzate e capaci di operare su larga scala grazie all'uso dell'intelligenza artificiale.

Per le PMI questo significa una cosa: non serve essere un bersaglio di interesse per subire un attacco. Basta essere vulnerabili.

1. Ransomware AI-driven, estorsione multipla e supply chain

Il ransomware rimane la minaccia più distruttiva per le aziende italiane. Gli attacchi moderni combinano automazione, doppia o tripla estorsione e compromissione dei fornitori.

- AI-driven: automazione nella ricerca di vulnerabilità e nella fuga laterale.
- Doppia e tripla estorsione: cifratura, pubblicazione dei dati e pressione su clienti e fornitori.
- Supply chain attack: compromissione di piccoli fornitori per raggiungere aziende più grandi.

2. Compromissioni di identità cloud e Microsoft 365

Il cloud è il cuore operativo di molte PMI. Gli attaccanti puntano sulle identità per accedere a dati strategici, muoversi lateralmente e mantenere persistenza.

- Abuso di sessioni non protette.
- MFA assente o configurato in modo debole.
- Condivisioni esterne non controllate.
- Regole malevole nelle caselle di posta.

CAPITOLO 1

3. Phishing mirato verso ruoli finanziari

Il phishing non è più generico o facilmente riconoscibile. Crescono gli attacchi verso CFO, contabilità e procurement, con email che replicano clienti, fornitori o banche e richieste di pagamento fraudolente.

CAPITOLO 1

Esposizione digitale e limiti dei modelli tradizionali

4. Exploit su tecnologie obsolete o esposte

Un numero crescente di attacchi sfrutta software non aggiornato, VPN legacy senza MFA, firewall con configurazioni obsolete e servizi accessibili da Internet senza protezioni adeguate.

5. Visibilità dell'esposizione digitale

Molte aziende non conoscono con precisione quali servizi espongono verso l'esterno, quali versioni software utilizzano, quali dati sono reperibili online e quali credenziali sono state compromesse nel tempo.

La cyber resilienza richiede di monitorare costantemente l'esposizione, identificare superfici attaccabili e correggere rapidamente le configurazioni deboli.

6. Perché i modelli tradizionali non bastano più

Firewall, antivirus e backup sono necessari, ma non sufficienti. Le minacce attuali richiedono un approccio guidato dal rischio, capacità di rilevare comportamenti anomali, governance e processi, protezione basata sull'identità e risposta strutturata agli incidenti.

La resilienza digitale non è una questione di tecnologia. È un modello operativo.

CAPITOLO 2

I pilastri della Cyber Resilienza

La resilienza digitale nasce da pratiche organizzative, controlli tecnici e capacità operative che lavorano in modo coordinato.

1. Governance

Ruoli, responsabilità, processi decisionali, revisione periodica delle priorità di sicurezza.

2. Identità e accessi

MFA, privilegio minimo, ciclo di vita degli account, protezione degli amministratori.

3. Protezione dei dati

Backup separati e protetti, cifratura, retention, classificazione dei dati.

4. Continuità operativa

BCP, piano di risposta agli incidenti, procedure per ransomware, blackout e compromissioni cloud.

5. Detection & Response

Rilevazione di anomalie, monitoraggio di accessi sospetti, escalation chiare e risposta rapida.

6. Security culture

Formazione continua, simulazioni di phishing, processi semplici di segnalazione e responsabilizzazione.

Questi pilastri non vanno implementati tutti insieme. Devono essere affrontati in modo progressivo, misurabile e coerente con il rischio aziendale.

> La resilienza non è una tecnologia. Non è un software. È un modello operativo e deve essere gestito come tale.

CAPITOLO 3

Come valutare il livello di resilienza

Prima di migliorare la resilienza, un'azienda deve capire a che punto si trova oggi. La valutazione richiede un modello semplice, domande chiave e capacità di riconoscere segnali di fragilita operativa.

Il modello di maturità in 5 livelli

Livello 1 - Initial

Nessuna governance, processi assenti o informali, sicurezza gestita quasi solo dall'IT.

Livello 2 - Repeatable

Alcune pratiche sono ripetute nel tempo, ma non sono documentate ne integrate nel business.

Livello 3 - Defined

Esistono policy, ruoli e processi; il rischio viene valutato; la direzione e coinvolta.

Livello 4 - Managed

La sicurezza e misurata, monitorata e coordinata; esiste un piano di miglioramento annuale.

Livello 5 - Optimized

La resilienza e integrata nel funzionamento aziendale, con capacità avanzate di detection, risposta e governance.

La maggior parte delle PMI italiane si colloca tra il Livello 1 e il Livello 3.

CAPITOLO 3

Self-assessment rapido

Il modo più veloce per capire il livello di resilienza e rispondere a cinque domande, ognuna riferita a un pilastro della sicurezza.

1. Governance: abbiamo ruoli e responsabilità documentati?
2. Identità: MFA e attivo per tutti?
3. Dati: i backup sono verificati e isolati?
4. Continuity: esiste un piano di risposta agli incidenti?
5. Detection: abbiamo visibilità su accessi sospetti e configurazioni critiche?

Indicatori di debolezza tipici delle PMI

- Dipendenza totale da IT esterno, senza controllo interno ne governance.
- Assenza di un inventario aggiornato di dispositivi, applicazioni, utenti e servizi cloud.
- Configurazioni cloud non controllate, con MFA non obbligatorio, condivisioni aperte e log non raccolti.
- Mancanza di monitoraggio su accessi, log centralizzati, rilevazione comportamentale e alert.

Come interpretare i risultati

- Molte risposte negative: priorità alta. L'azienda deve costruire basi solide.
- Risposte miste: priorità media. I processi esistono, ma sono ancora poco strutturati.
- Quasi tutte positive: priorità strategica. Serve concentrarsi su miglioramento continuo.

Sapere dove si e oggi permette di decidere dove andare domani.

CAPITOLO 4

Le priorità immediate per il 2026

Non tutte le aziende possono affrontare subito un programma completo di cyber resilienza. Esistono però interventi minimi e ad alto impatto che riducono significativamente il rischio in 90 giorni.

1. Protezione delle identità

MFA ovunque: email, VPN, applicazioni aziendali, sistemi cloud e strumenti gestionali. A questo va affiancata una revisione degli accessi privilegiati per identificare account amministrativi, ridurre permessi eccessivi ed eliminare credenziali dimenticate.

2. Protezione email

Devono essere attivi filtri anti-phishing avanzati, capaci di riconoscere domini simili, link malevoli e spoofing dell'identità. Gli allegati sconosciuti devono essere aperti in ambiente isolato.

3. Hardening del cloud

Per Microsoft 365 e Google Workspace servono MFA obbligatorio, Conditional Access dove disponibile, limitazione dei privilegi, blocco del forwarding esterno, restrizioni sulle condivisioni e log di sicurezza attivi.

4. Aggiornamenti e patching critico

La finestra di sfruttamento delle vulnerabilità pubbliche e spesso di pochi giorni. Occorre aggiornare sistemi operativi, firewall, VPN, apparati di rete e applicazioni esposte a Internet.

CAPITOLO 4

Azioni ad alto impatto in 90 giorni

5. Backup offline verificati

Un backup non verificato e un backup che forse funziona. La resilienza si costruisce con procedure di ripristino testate e controllate.

- Verificare l'integrità dei backup.
- Assicurarsi che almeno una copia sia offline o immutabile.
- Testare un ripristino completo almeno una volta al trimestre.

6. Test di sicurezza

Un Vulnerability Assessment permette di identificare servizi esposti, configurazioni deboli, software obsoleti e vulnerabilità critiche. Le simulazioni di phishing aiutano a valutare il comportamento degli utenti e a identificare reparti da formare con priorità.

Roadmap concreta e sostenibile

Implementare queste sei aree in 90 giorni permette di ridurre il rischio reale di attacco, prevenire compromissioni di identità ed email, migliorare la postura cloud, garantire la sopravvivenza dei dati e creare le basi per un programma di resilienza più ampio.

Non serve trasformare l'azienda da un giorno all'altro. Serve iniziare dalle priorità giuste.

CAPITOLO 5

Il modello Individua – Correggi – Certifica

La resilienza non si costruisce con interventi isolati. Richiede un metodo operativo pensato per PMI che hanno bisogno di controllo, visibilità e continuità senza creare un reparto interno complesso.

1. Individua

Comprendere il rischio e il primo passo per ridurlo.

- **Valutazione del rischio:** analisi di processi, dati, sistemi, fornitori e modalità operative.
- **Penetration Test:** simulazioni controllate di attacco su applicazioni e sistemi critici.
- **Threat Exposure Study:** analisi di servizi esposti, credenziali compromesse, informazioni disponibili online e superfici attaccabili.

2. Correggi

Le vulnerabilità identificate vengono affrontate con interventi mirati e sostenibili.

- Remediation guidata, con priorità basate sulle conseguenze di business.
- Hardening di infrastruttura e cloud.
- Definizione dei processi minimi di sicurezza: accessi, aggiornamenti, backup, incident response e fornitori.

CAPITOLO 5

Dimostrare la sicurezza

3. Certifica

Dimostrare la sicurezza diventa un vantaggio competitivo. Le PMI affrontano sempre più spesso questionari di sicurezza, audit dei fornitori e richieste tecniche dai clienti esteri.

Preparazione a NIS2, ISO 27001 e DORA

- Comprendere gli obblighi.
- Colmare i gap rispetto agli standard.
- Definire un sistema di gestione della sicurezza coerente.
- Redigere documentazione e policy richieste.

Supporto agli audit di clienti e supply chain

Il percorso Individua - Correggi - Certifica permette di superare le verifiche con chiarezza, documentazione coerente e un sistema di sicurezza dimostrabile.

Il metodo permette all'azienda di capire dove e vulnerabile, intervenire con priorità corrette, dimostrare il proprio livello di sicurezza e costruire una resilienza misurabile nel tempo.

CAPITOLO 6

Costruire un Security Program sostenibile

La cyber resilienza non si ottiene con interventi isolati. Richiede un Security Program strutturato, continuo e misurabile, capace di evolvere con il business e con le minacce.

Roadmap annuale

Una roadmap efficace deve essere basata sul rischio, progressiva, misurabile e bilanciata tra aspetti tecnici e organizzativi.

Q1 - Fondamenta

MFA, revisione accessi, baseline cloud, policy minime, test iniziali.

Q2 - Rafforzamento

Hardening infrastruttura, segmentazione rete, miglioramento backup e ripristino.

Q3 - Governance

Risk assessment formale, piano di risposta agli incidenti, formazione e simulazioni phishing.

Q4 - Certificazione e audit

Preparazione NIS2 e ISO 27001, audit interni, revisione completa dei KPI.

CAPITOLO 6

KPI essenziali per direzione e board

Le direzioni aziendali non devono analizzare log o dettagli tecnici. Devono verificare indicatori chiave che descrivono lo stato della sicurezza in modo semplice.

- **Percentuale utenti con MFA attivo**
- **Vulnerabilità critiche aperte e chiuse**
- **Tempo medio di applicazione delle patch critiche**
- **Incidenti rilevati e incidenti evitati**
- **Percentuale dipendenti che superano i test phishing**
- **Esposizione digitale: asset esposti e credenziali compromesse**

CAPITOLO 6

Priorità, vCISO e integrazione operativa

Scegliere le priorità in base al rischio

Un Security Program sostenibile parte da una domanda semplice: "Quale rischio stiamo riducendo?" Le priorità devono considerare impatto sul business, probabilita di accadimento, esposizione attuale, obblighi normativi e dipendenza da fornitori esterni.

Quando serve un vCISO

Un vCISO diventa necessario quando l'azienda deve rispondere ad audit della supply chain, sono richieste conformità NIS2, ISO 27001 o DORA, IT non ha competenze specifiche di governance e rischio, oppure la direzione vuole una visione chiara e misurabile.

Integrazione con IT interno e fornitori

Un Security Program funziona solo se integrato con chi gestisce davvero i sistemi.

- IT interno: esegue attività operative.
- Fornitori IT: mantengono infrastrutture e applicazioni.
- Difesa Digitale/ISGroup: governa, orienta, verifica e misura.

Un progetto ha una fine. La resilienza no.

È un ciclo continuo di individuazione dei rischi, miglioramento dei controlli, verifica e adeguamento ai cambiamenti.

CAPITOLO 7

Checklist di resilienza

Questa checklist raccoglie i controlli minimi necessari per stabilire un livello essenziale di resilienza digitale. Usala in riunione con il team IT o con i fornitori per verificare lo stato attuale e identificare rapidamente le priorità.

A. Controlli tecnici

MFA

- MFA attivo per tutti gli utenti.
- MFA obbligatorio per amministratori e accessi remoti.
- MFA configurato anche su applicazioni cloud e VPN.

Backup

- Almeno una copia offline o immutabile.
- Verifica periodica del ripristino.
- Procedure documentate e applicate.

Endpoint Protection

- Antivirus/EDR aggiornato su ogni dispositivo.
- Blocco di comportamenti anomali e ransomware.
- Policy di isolamento macchina compromessa.

CAPITOLO 7

Checklist tecnica e organizzativa

A. Controlli tecnici

Rete segmentata

- Separazione tra rete utenti, server e sistemi critici.
- Accessi minimi tra segmenti.
- VPN configurata con permessi limitati.

Patch Management

- Patch critiche applicate entro 30 giorni, preferibilmente 14.
- Aggiornamenti automatici dove possibile.
- Inventario dei sistemi e relative versioni.

B. Controlli organizzativi

- Policy documentate per accessi, uso risorse, email, cloud, backup, continuità e risposta agli incidenti.
- Ruoli definiti: chi decide, chi esegue e chi verifica.
- Direzione formalmente coinvolta nella sicurezza.
- Procedure minime per incident response, gestione fornitori e change management.

CAPITOLO 7

Monitoraggio e uso della checklist

C. Monitoraggio e detection

- Alert su accessi anomali, tentativi di autenticazione sospetti e attività anomale su Microsoft 365 o Google Workspace.
- Log conservati per almeno 90 giorni, centralizzati o comunque accessibili per analisi rapide.
- Eventi critici monitorati: autenticazioni, modifiche, errori di sistema.
- Vulnerability Assessment almeno una volta l'anno.
- Simulazioni phishing periodiche.
- Revisione trimestrale delle configurazioni cloud e dei permessi.

Come utilizzare questa checklist

- Verifica ogni voce con Si, No o Da verificare.
- Conta quante aree risultano mancanti.
- Le voci No rappresentano le priorità dei prossimi 90 giorni.
- Le voci Da verificare richiedono approfondimento immediato.

Applicata correttamente, questa checklist riduce in modo significativo il rischio operativo di una PMI e crea un punto di partenza solido per costruire resilienza nel lungo periodo.

CONCLUSIONI

La resilienza non è complicata se guidata da un metodo chiaro

La cyber resilienza non è un obiettivo astratto né un percorso riservato alle grandi aziende. Per una PMI, essere resiliente significa avere metodo, priorità chiare e processi essenziali.

Il modello operativo illustrato, basato su governance, protezione delle identità, hardening, detection, continuità e certificazione, offre a qualunque azienda un percorso concreto per iniziare a migliorare la propria sicurezza fin da subito.

Valuta il livello di rischio della tua azienda

Ogni percorso efficace parte da una fotografia iniziale: capire dove sei oggi e quali priorità hanno l'impatto maggiore sul tuo business.

Difesa Digitale mette a disposizione una valutazione gratuita del rischio, progettata per PMI e aziende italiane che vogliono identificare le principali aree di esposizione, definire priorità reali e ottenere un piano d'azione operativo.

Scansiona il QR Code per prenotare la consulenza.

www.difesadigitale.it/consulenza

Termini e Condizioni

Il percorso verso la resilienza inizia con una decisione: mettere la sicurezza del tuo business al centro.