



Cybersecurity e PMI

Proteggere la continuità, rafforzare la filiera

La sicurezza digitale come capacità
di lavorare, crescere e mantenere la fiducia.

LA PROPOSTA DI HERMES CENTRO STUDI EUROPEO

Un percorso proporzionato per individuare le priorità, verificare la ripartenza e rendere documentabile l'affidabilità della PMI.

01

CONTINUITÀ OPERATIVA

02

FIDUCIA DI FILIERA

03

RISULTATI VERIFICABILI

01 / LA SITUAZIONE

Se si ferma il sistema, si può fermare il business

La sicurezza digitale riguarda ordini, incassi, consegne e relazioni con i clienti.

Un ordine da confermare, un pagamento da verificare, una macchina che dipende da un gestionale: molte attività di una PMI attraversano sistemi digitali e servizi esterni. Quando uno di questi collegamenti viene meno, la difficoltà può raggiungere il magazzino, la produzione e il cliente. Il problema entra così nel conto economico e nella reputazione dell'impresa.

Nel primo semestre 2026 il monitoraggio nazionale registra 2.171 eventi cyber, contro 1.474 nello stesso periodo del 2025: un aumento di circa il 47%. Sono eventi osservati nel perimetro del monitoraggio, non il numero complessivo delle PMI attaccate né una misura della probabilità che ciascuna impresa subisca un incidente.

Un investimento nella capacità di continuare

Proteggersi significa ridurre esposizioni evitabili e sapere come gestire un'interruzione. Accessi controllati, dati recuperabili e responsabilità riconoscibili possono aiutare a contenere gli impatti e a riprendere le attività. La continuità rende inoltre più credibile il rapporto con clienti e partner.

LA DIAGNOSI DI HERMES CENTRO STUDI EUROPEO

Per molte PMI la distanza da colmare è fra strumenti acquistati e capacità organizzativa di utilizzarli, verificarli e mantenerli. La proposta collega sicurezza, continuità e relazioni di filiera attraverso un percorso proporzionato alle attività dell'impresa.

Hermes Centro Studi Europeo è pronta a discutere con le imprese e le loro rappresentanze come trasformare questa esigenza in priorità operative e in una proposta di accompagnamento da portare ai decisori pubblici.

La sicurezza va organizzata. Il divario dimensionale è visibile.

Dati 2024 sulle imprese dei settori coperti dalla rilevazione, pubblicati nel gennaio 2025.

Imprese con documenti sulla sicurezza ICT



Documenti relativi a misure, pratiche o procedure di sicurezza ICT. Microimprese sotto i 10 addetti escluse. Elaborazione dei dati istituzionali riportati nei riferimenti.

La differenza è di 48,6 punti percentuali. Avere documenti non dimostra da solo l'efficacia della protezione; rende però osservabile una componente della formalizzazione. Il dato invita a rafforzare il collegamento fra responsabilità, procedure e attività effettivamente svolte.

Altre misure anno 2024	Imprese 10+	Grandi 250+
Backup separato dei dati	79,5%	95,8%
Valutazione del rischio ICT	36,9%	80,6%
Test di sicurezza ICT	31,8%	78,9%

La colonna 10+ comprende anche le grandi imprese: non è una misura esclusiva delle PMI. Le voci possono coesistere e non vanno sommate. I dati descrivono adozione dichiarata, senza certificare qualità o aggiornamento delle misure.

DAL PRESIDIO ALLA CAPACITÀ

Il valore nasce dalla combinazione: un backup deve poter essere ripristinato; una procedura deve avere responsabili e contatti utilizzabili; un test deve generare correzioni. Il percorso proposto rende verificabili questi passaggi.

Essere affidabili aiuta a lavorare insieme

La sicurezza delle relazioni dipende anche dai collegamenti fra imprese.

Una PMI può essere collegata ai clienti attraverso portali, documenti condivisi, credenziali o accessi di assistenza. Sono connessioni utili al business, ma richiedono regole chiare. Un disservizio o un accesso compromesso possono coinvolgere informazioni e processi che appartengono a più organizzazioni.

Rendere leggibile ciò che si fa

Clienti e committenti possono chiedere informazioni sulla gestione degli accessi, sulla continuità e sulla risposta agli incidenti. Una risposta documentata riduce ambiguità e rende il confronto più concreto. Non garantisce l'aggiudicazione di un contratto, ma può sostenere la valutazione dell'affidabilità del fornitore.

Evitare richieste indistinte

Questionari ripetuti e clausole poco proporzionate possono pesare soprattutto sulle imprese minori. La soluzione dovrebbe aiutare a distinguere le evidenze necessarie dai duplicati e a concordare richieste coerenti con il servizio fornito e con il rischio effettivo.

Relazione	Aspetto da chiarire
Cliente e fornitore	Informazioni condivise, accessi concessi e comunicazione degli incidenti.
Impresa e gestore IT	Compiti, tempi di intervento e responsabilità sul ripristino.
Direzione e personale	Regole di utilizzo, segnalazione e autorizzazione delle operazioni.

SICUREZZA COME FIDUCIA DOCUMENTABILE

La PMI può rafforzare il proprio posizionamento mostrando come governa i collegamenti essenziali e come prepara la continuità. La proposta rende questo patrimonio più facile da costruire e aggiornare, senza diffondere dettagli tecnici sensibili.

04 / IL QUADRO NORMATIVO

Obblighi diretti e richieste di filiera: distinzioni che contano

La verifica del perimetro viene prima dell'attribuzione degli adempimenti.

Il decreto legislativo n. 138/2024 recepisce la direttiva NIS2 e disciplina i soggetti essenziali e importanti secondo criteri e fattispecie specifici. Essere una PMI o fornire un cliente soggetto NIS non comporta automaticamente l'inclusione nel medesimo perimetro.

Per i soggetti direttamente interessati, le misure di gestione dei rischi comprendono dimensioni tecniche, operative e organizzative. La catena di approvvigionamento e i rapporti con i fornitori assumono rilievo nell'analisi del rischio. Per un fornitore fuori perimetro possono quindi sorgere richieste contrattuali, da distinguere dagli obblighi normativi direttamente applicabili.

Situazione	Verifica da effettuare
Soggetto NIS	Inquadramento, comunicazioni ricevute, obblighi e termini pertinenti.
Fornitore di un soggetto NIS	Clausole, accessi, criticità del servizio ed evidenze richieste.
Impresa fuori perimetro	Continuità, protezione dei dati e ulteriori obblighi applicabili al caso.

Le scadenze non sono uguali per tutti

Il calendario va ricostruito attraverso le determinazioni ACN e le comunicazioni del singolo soggetto. Le disposizioni del 2026 distinguono i nuovi inserimenti dai soggetti già presenti nel 2025. Non è corretto attribuire a tutte le PMI un'unica scadenza di ottobre.

LA PROPOSTA NON SOSTITUISCE GLI ADEMPIMENTI

Il percorso qui descritto è una proposta di accompagnamento. Per chi ha obblighi già applicabili, le attività devono essere organizzate nel rispetto dei termini pertinenti. Una prova o un fascicolo interno non equivalgono a una certificazione NIS.

Un percorso di resilienza proporzionato alla PMI

La soluzione di Hermes Centro Studi Europeo collega priorità aziendali ed evidenze operative.

Hermes Centro Studi Europeo propone un percorso di resilienza per PMI e filiere: analizzare le attività essenziali, definire un piano proporzionato, accompagnarne l'attuazione con competenze specialistiche e verificare la capacità di ripartenza. È una proposta progettuale, non un incentivo già istituito.

Capire che cosa deve continuare

Il punto di partenza è il business: quali servizi devono essere ripristinati per primi, quanto tempo può essere tollerato e quali dipendenze esterne esistono. Questa lettura permette di ordinare gli interventi e di evitare acquisti scollegati dalle priorità.

Collegare direzione e competenze tecniche

Il percorso individua un responsabile aziendale e coinvolge i fornitori informatici pertinenti. Hermes Centro Studi Europeo può contribuire all'analisi organizzativa, al piano di intervento e al raccordo con professionisti qualificati; le verifiche tecniche richiedono specialisti e autorizzazioni appropriate.

Verificare e mantenere

Il risultato è un piano con attività, responsabilità, costi e prove. La verifica comprende il ripristino di un servizio prioritario e un'esercitazione organizzativa. L'aggiornamento diventa parte della gestione, soprattutto quando cambiano persone, sistemi o fornitori.

IL VALORE AGGIUNTO

La PMI ottiene una lettura comprensibile delle proprie priorità e un percorso attuabile per rafforzare la continuità. Le evidenze possono sostenere anche il confronto con i committenti, entro un perimetro di condivisione concordato.

06 / DALLA PROPOSTA AL LAVORO

Preparare la ripartenza prima che serva

Ogni presidio acquista valore quando risponde a un’esigenza del processo.

Priorità	Intervento da valutare	Evidenza utile
Accessi	Riesame degli account e delle autorizzazioni; autenticazione adeguata.	Ruoli, verifiche periodiche e revoca degli accessi non necessari.
Aggiornamenti	Inventario dei sistemi e gestione delle correzioni.	Responsabilità e tempi di intervento secondo criticità.
Recupero dei dati	Copie separate e protette; prove di ripristino.	Esito, durata e limitazioni della prova autorizzata.
Risposta	Contatti, ruoli e procedure di gestione dell’interruzione.	Esiti dell’esercitazione e azioni da completare.

Queste aree non costituiscono un elenco esaustivo di conformità. La selezione dipende da attività, infrastrutture e rischio. In particolare, una copia disponibile non dimostra che l’intero servizio possa ripartire: applicazioni, credenziali, configurazioni e dipendenze devono essere considerate nella prova.

Esercitarsi senza compromettere la produzione

Le verifiche vanno pianificate in condizioni controllate, con autorizzazioni e responsabilità definite. Gli esiti devono indicare che cosa è stato provato, che cosa resta fuori e quali interventi sono necessari. Le attività tecniche non devono creare un’interruzione evitabile.

UNA CULTURA DELLA SEGNALAZIONE

Il personale deve sapere a chi rivolgersi davanti a una richiesta sospetta o a un’anomalia. Formazione breve, pertinente e ripetuta può aiutare a rendere utilizzabili le procedure, senza attribuire alle persone una responsabilità indistinta per ogni incidente.

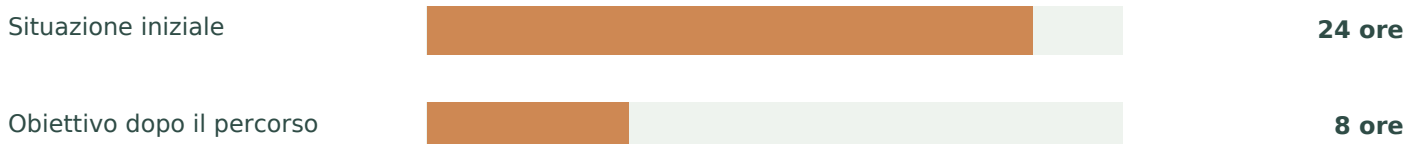
07 / MISURARE LA RIPARTENZA

Il tempo di recupero può diventare un obiettivo concreto

Simulazione illustrativa: nessun risultato reale o riduzione garantita del rischio.

Si consideri una PMI che dipenda da un servizio digitale prioritario. In una simulazione, il tempo necessario a ripristinare quel servizio passa da 24 a 8 ore. La differenza è di 16 ore, pari a una riduzione del 66,7%. È un obiettivo ipotetico da verificare con prove comparabili.

Ripristino del servizio | scenario illustrativo



Tempi ipotetici riferiti allo stesso servizio e allo stesso perimetro di prova. Non descrivono la frequenza degli incidenti né garantiscono l'esito di un evento futuro.

Se il margine di contribuzione non recuperabile fosse ipotizzato in 1.000 euro per ogni ora di fermo, l'esposizione economica nello scenario passerebbe da 24.000 a 8.000 euro: una differenza condizionata di 16.000 euro per un evento con quelle caratteristiche.

IL SIGNIFICATO ECONOMICO

La differenza è riferita a un singolo scenario, non è un risparmio annuo atteso. Per stimare una perdita attesa servirebbero probabilità e gravità attendibili. Ordini recuperati, costi straordinari e conseguenze contrattuali possono modificare il risultato.

Il valore di 1.000 euro/ora è una semplice ipotesi di calcolo: non un dato medio di settore, un tariffario o un costo standard. La ricostruzione va effettuata con l'impresa, evitando di confondere fatturato e margine perso.

Dimostrare preparazione senza moltiplicare gli adempimenti

La proposta include un fascicolo essenziale, aggiornabile e condivisibile in modo selettivo.

Una PMI può ricevere questionari differenti su aspetti simili. Hermes Centro Studi Europeo propone di organizzare le informazioni in un fascicolo di resilienza: un insieme essenziale di evidenze, da adattare alle richieste pertinenti e da aggiornare quando cambia il contesto.

Contenuto	Finalità
Attività e dipendenze prioritarie	Chiarire che cosa deve continuare e da quali soggetti dipende.
Responsabili e contatti	Rendere attivabile la gestione dell'interruzione.
Prove svolte e azioni aperte	Mostrare ciò che è stato verificato e ciò che resta da completare.
Regole con i fornitori	Concordare accessi, assistenza e comunicazioni pertinenti.

Un linguaggio comune, proporzionato al rischio

Il confronto con il committente dovrebbe specificare le evidenze necessarie, il loro aggiornamento e i limiti della condivisione. Le richieste vanno collegate al servizio fornito. Si riduce così il rischio che la PMI ripeta risposte senza migliorare il presidio effettivo.

Proteggere anche le evidenze

Il fascicolo non deve diventare un archivio indiscriminato di configurazioni o vulnerabilità. Accesso e condivisione richiedono selezione, riservatezza e canali appropriati. L'obiettivo è documentare la gestione, mantenendo protette le informazioni sensibili.

UNA PROPOSTA, NON UN BOLLINO

Il fascicolo non è una certificazione né garantisce la qualificazione del fornitore. Può rendere più ordinato e credibile il confronto, facendo emergere interventi concreti e responsabilità riconoscibili.

09 / LA SPERIMENTAZIONE

Trenta PMI, un metodo da verificare sul campo

Dimensione e calendario proposti: nessun programma pubblico o finanziamento già acquisito.

Hermes Centro Studi Europeo propone una sperimentazione su 30 PMI, raccolte in tre gruppi territoriali o di filiera. Ogni impresa individua un servizio prioritario, ricostruisce le dipendenze e sviluppa un piano. Il livello tecnico viene adattato alla complessità e al rischio del caso.

Fase indicativa	Attività
Primo mese	Analisi delle attività, perimetro normativo e dipendenze.
Mesi 2-3	Priorità, responsabilità e interventi da realizzare.
Mese 4	Prova autorizzata di ripristino ed esercitazione organizzativa.
Successivi 3 mesi	Correzioni, aggiornamento e verifica della continuità del presidio.

Indicatori leggibili

Per tutte le imprese coinvolte si rilevano piani completati, prove effettivamente svolte, tempi osservati e azioni ancora aperte. La valutazione distingue il miglioramento del presidio dagli incidenti osservati: l'assenza di un attacco nel breve periodo non dimostra da sola l'efficacia del percorso.

Risorse coerenti con le attività

Il budget richiede una progettazione specifica. Vanno separati analisi organizzativa, specialisti tecnici, strumenti, formazione e manutenzione. L'eventuale sostegno deve essere ricondotto a misure effettivamente accessibili e alle rispettive regole, senza presumere coperture automatiche.

RISULTATI UTILI ALLA PROGRAMMAZIONE

L'esperienza può mostrare quali ostacoli pesino sulle PMI e quali servizi condivisi offrano utilità. Gli esiti devono includere anche prove non riuscite e difficoltà, tutelando la riservatezza delle imprese.

Dalla sicurezza della PMI alla resilienza del sistema produttivo

Hermes Centro Studi Europeo collega esigenze professionali e proposte ai decisori pubblici.

La continuità delle imprese minori contribuisce alla stabilità delle filiere. Per renderla più accessibile occorre un confronto fra rappresentanze imprenditoriali, amministrazioni competenti, reti dell'innovazione e soggetti specializzati. Le rispettive funzioni devono restare riconoscibili.

Portare una proposta concreta

Hermes Centro Studi Europeo propone di verificare servizi di accompagnamento proporzionati, evidenze riutilizzabili e modalità di sostegno alle prove di ripristino e alla formazione. Il confronto istituzionale dovrebbe partire dai programmi esistenti e individuare gli adeguamenti necessari, senza presupporre una nuova legge.

Affiancare le imprese nell'analisi

Hermes Centro Studi Europeo è pronta a discutere priorità, dipendenze e richieste di filiera, contribuendo alla costruzione del percorso e al raccordo con le competenze tecniche appropriate. L'obiettivo è trasformare un'esigenza spesso percepita come specialistica in un piano comprensibile alla direzione aziendale.

La sicurezza digitale può sostenere l'affidabilità con cui una PMI lavora e si presenta al mercato. Un'organizzazione preparata dispone di criteri per scegliere gli interventi, chiedere evidenze ai propri fornitori e spiegare ai clienti come affronta la continuità.

UN CONFRONTO DA COSTRUIRE INSIEME

Le PMI, le organizzazioni datoriali e i soggetti di filiera interessati sono invitati a contattare Hermes Centro Studi Europeo per approfondire le proprie esigenze di continuità e la soluzione proposta, costruendo insieme un percorso documentato da portare ai decisori pubblici.

11 / RIFERIMENTI VERIFICABILI

Norme, atti e dati istituzionali

Le ipotesi economiche e il progetto pilota sono elaborazioni proposte, distinte dalle evidenze osservate.

ISTAT | Imprese e ICT, anno 2024

Rapporto del 17 gennaio 2025, pagine 2 e 6: documenti e misure di sicurezza. Perimetri distinti fra PMI, grandi e totale 10+.

Apri il riferimento istituzionale

ACN | Operational Summary, primo semestre 2026

Eventi cyber osservati: 2.171 rispetto a 1.474 nel primo semestre 2025. Il dato non misura tutte le imprese attaccate.

Apri il riferimento istituzionale

Italia | Decreto legislativo n. 138/2024

Recepimento NIS2; perimetro, responsabilità e gestione dei rischi, in particolare artt. 3, 23, 24 e 25.

Apri il riferimento istituzionale

ACN | Modalità e specifiche di base NIS

Determinazione n. 379907 del 19 dicembre 2025 e relativi allegati; lettura con gli aggiornamenti applicabili.

Apri il riferimento istituzionale

ACN | Determinazione n. 127434/2026

Disposizioni sui termini per i soggetti inseriti nel 2026 e raccordo con i soggetti già inseriti nel 2025.

Apri il riferimento istituzionale

ENISA | Cybersecurity for SMEs

Guida istituzionale: misure organizzative, protezione e verifica del recupero dei dati.

Apri il riferimento istituzionale