VIGILIA

CYBERSECURITY PER LE PMI

STRATEGIE PRATICHE PER LA RESILIENZA

2025 REPORT

www.vigiliacyber.com

Indice

01 Introduzione: la nuova normalità della minaccia cyber per le PMI

Negli ultimi anni, il panorama della cybersecurity è cambiato radicalmente. Quella che un tempo era percepita come una minaccia relegata alle grandi multinazionali o alle istituzioni governative è diventata una realtà quotidiana e tangibile per aziende di ogni dimensione, incluse le Piccole e Medie Imprese (PMI) che costituiscono la spina dorsale del tessuto economico italiano.
Questo whitepaper nasce dall' esperienza sul campo di supporto quotidiano a centinaia di PMI nella propria strategia digitale, da cui sono state osservate da vicino l'evoluzione delle minacce, le vulnerabilità ricorrenti e, soprattutto, quelle che possono essere considerate le strategie vincenti – rispetto a quelle che non funzionano – nel contesto specifico delle realtà aziendali con risorse limitate.

L'obiettivo dunque non è quello di spaventare, ma di condividere lezioni apprese, fornire un quadro realistico del contesto attuale e, soprattutto, offrire spunti pratici e strategie attuabili per rafforzare la postura di sicurezza e costruire la cyber resilienza della vostra azienda. Vedremo come le minacce globali impattano direttamente le PMI italiane, quali settori sono più a rischio secondo i dati più recenti (Rapporto Clusit 2025), come affrontare la sfida emergente della sicurezza OT (Operational Technology) e, infine, cinque consigli pratici ispirati anche ai principi della nuova direttiva NIS2, per gestire il rischio cyber in modo efficace e sostenibile.
La cybersecurity non è più solo una questione tecnica, ma un elemento strategico fondamentale per la continuità del business e la competitività. Affrontarla con consapevolezza e pragmatismo è il primo passo verso un futuro digitale più sicuro.

02 Il Contesto Globale delle Minacce: non solo un problema per le grandi aziende

Il cybercrime è diventato un'industria globale multimiliardaria, altamente organizzata e in continua evoluzione. Gli attaccanti sono sempre più sofisticati, utilizzano strumenti avanzati e tattiche diversificate per colpire i loro bersagli. È fondamentale comprendere che le PMI non sono immuni, anzi.

L'evoluzione del Cybercrime: ransomware, phishing e oltre

Il ransomware continua a essere una delle minacce più devastanti, capace di bloccare intere operazioni aziendali chiedendo riscatti esorbitanti: per esempio, nei primi 5 mesi del 2025 il gruppo ransomware Akira ha reso noto circa 300 vittime. Le tecniche di phishing diventano sempre più mirate e convincenti (spear-phishing), sfruttando l'ingegneria sociale per ingannare i dipendenti e ottenere credenziali di accesso o installare malware. Assistiamo inoltre all'aumento di attacchi che sfruttano Vulnerabilità di sistemi esposti dove i criminali sfruttano tecnologie o piattaforme non correttamente aggiornate come punto iniziale di accesso.

La Supply Chain come vettore d'attacco

Un trend in forte crescita è l'attacco alla catena di fornitura (Supply Chain Attack). I cybercriminali non colpiscono direttamente l'obiettivo finale, ma compromettono un fornitore (spesso una PMI considerata un anello debole) per poi propagare l'attacco ai propri clienti. Questo rende essenziale valutare non solo la propria sicurezza, ma anche l'interconnessione e la condivisione di dati con i propri fornitori.

L'Intelligenza Artificiale: arma a doppio taglio

L'avvento dell'Intelligenza Artificiale (IA) generativa sta rivoluzionando molti settori, ma offre anche nuovi strumenti ai cybercriminali. La generative AI può essere usata per creare email di phishing estremamente realistiche, generare malware polimorfico più difficile da rilevare, automatizzare la ricerca di vulnerabilità su larga scala e persino creare deepfake per campagne di disinformazione o truffe. Allo stesso tempo, offre potenti strumenti anche per la difesa, ma la corsa agli armamenti è in pieno svolgimento.

Perché le PMI sono nel mirino

- Contrariamente a un pensiero diffuso, le PMI sono bersagli molto attraenti per diversi motivi:
- Porta d'accesso: Possono essere utilizzate come trampolino per colpire aziende più grandi (Supply Chain Attack).
- Risorse percepite come limitate: Gli attaccanti presumono (spesso a ragione) che le PMI abbiano investito meno in sicurezza rispetto alle grandi corporation, rendendole bersagli "più facili".
- Dati preziosi: Anche le PMI gestiscono dati sensibili (clienti, dipendenti, know-how) che hanno valore sul mercato nero.
- Impatto operativo: Un attacco riuscito può avere conseguenze devastanti sulla continuità operativa di una PMI, aumentando la probabilità che venga pagato un riscatto.

Ignorare queste minacce non è più un'opzione.
Ogni azienda, indipendentemente dalla dimensione, deve considerare la cybersecurity una priorità strategica.

03 Oltre la difesa: abbracciare la cyber resilienza

Nell'attuale panorama, dove la probabilità di subire un incidente informatico è sempre più alta, la sola difesa perimetrale non è più sufficiente. È necessario adottare un approccio più olistico e dinamico: la Cyber Resilienza.

Cos'è la Cyber Resilienza?

La cyber resilienza non è semplicemente la capacità di *prevenire* un attacco, ma la capacità di un'organizzazione di *anticipare*, *resistere*, *recuperare e adattarsi* a incidenti informatici significativi, minimizzandone l'impatto sul raggiungimento dei propri obiettivi di business primari. Significa essere preparati all'inevitabile, saper rispondere rapidamente ed efficacemente quando un incidente accade, e imparare dall'esperienza per migliorare continuamente.

Imparare dai Leader: Lezioni dal Cyber Resilience Compass (World Economic Forum)

Il World Economic Forum (WEF), in collaborazione con esperti globali, ha sviluppato il "Cyber Resilience Compass", un framework che identifica le pratiche chiave per costruire resilienza. Analizzando le esperienze di aziende leader che hanno affrontato gravi incidenti, possiamo trarre lezioni preziose anche per le PMI:

- **Caso Studio Mærsk (Colpita da NotPetya nel 2017):** Decisioni Basate sul Rischio Quantificato. Mærsk ha trasformato la sua gestione del rischio traducendo l'impatto potenziale degli incidenti in termini economici ("dollari persi"). Questo ha facilitato il dialogo con il board e il CFO, assicurando i fondi necessari per la trasformazione della sicurezza. Lezione per le PMI: Anche una valutazione qualitativa dei rischi (Alto, Medio, Basso) legata ai processi di business critici aiuta a prioritizzare gli investimenti e a comunicare l'importanza della sicurezza in termini comprensibili al management.

- **Caso Studio PETRONAS:** La Trasformazione Guidata dalla Leadership. Di fronte a una crescente digitalizzazione e al ruolo di infrastruttura critica, la leadership di PETRONAS ha reso la cyber resilienza una priorità strategica fin dall'inizio, guidando un programma pluriennale focalizzato su governance, difesa, identità, sicurezza OT ed education. Lezione per le PMI: Il commitment della direzione è fondamentale. Anche in una PMI, la sicurezza deve essere vista come un fattore abilitante del business, non solo un costo IT.

Applicare la Resilienza nelle PMI

Costruire resilienza non richiede necessariamente budget enormi. Si tratta di adottare una mentalità proattiva: identificare cosa è veramente critico per il business, capire i rischi principali, implementare controlli essenziali (MFA, backup testati, monitoraggio vulnerabilità e patching), preparare un piano di risposta semplice ma chiaro, formare i dipendenti sui comportamenti sicuri e, soprattutto, considerare la sicurezza un processo continuo di miglioramento.

04 Il panorama italiano: settori nel mirino (Dati Clusit 2025)

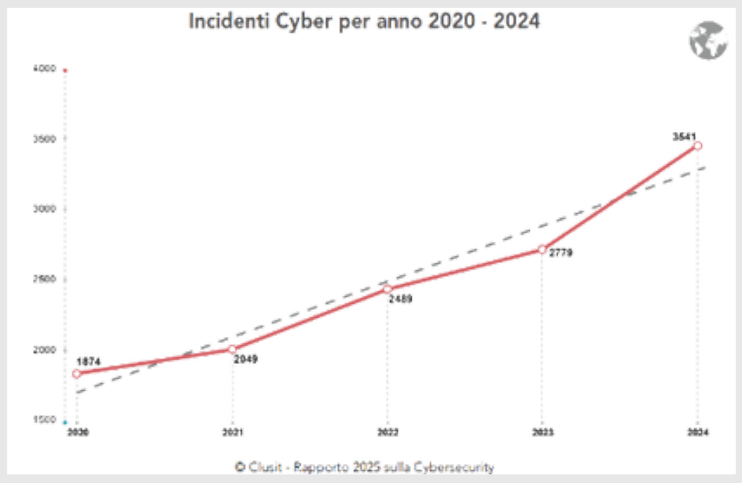
Comprendere quali settori sono più bersagliati dagli attacchi cyber in Italia fornisce un contesto prezioso per valutare il proprio livello di rischio, specialmente se la vostra azienda opera in uno di questi ambiti o fa parte della loro catena di fornitura. Il Rapporto Clusit 2025 offre uno spaccato aggiornato della situazione.

Analisi dei settori più colpiti

Secondo i dati presentati nel Rapporto Clusit 2025 (relativi agli incidenti noti del 2024 a livello globale, Italia inclusa, e con focus specifico sull'Italia):

- **Multiple Targets (18% globale):** Gli attacchi che colpiscono simultaneamente organizzazioni in settori diversi rimangono prevalenti, spesso tramite campagne massive (phishing, malware distribuito su larga scala) che non discriminano il bersaglio ma mirano a massimizzare il numero di vittime con il minimo sforzo.
- **Governativo/Militare/Forze dell'Ordine (13% globale, in aumento in Italia):** Questi settori sono target primari per spionaggio, hacktivism a sfondo geopolitico e tentativi di disruption. La crescente digitalizzazione della PA italiana la rende un bersaglio sempre più attraente.
- **Sanità (13% globale,+18.9% in Italia rispetto al 2023):**

  Il valore elevatissimo dei dati sanitari sul mercato nero e la criticità dei servizi rendono questo settore estremamente vulnerabile al ransomware e alle esfiltrazioni di dati. L'impatto di un blocco operativo qui è particolarmente grave.



Fonte: Rapporto Clusit 2025 sulla Cyber Security in Italia e nel mondo

- **Manifatturiero (in crescita significativa in Italia, 16% degli attacchi italiani nel 2024):** La crescente interconnessione degli impianti (Industria 4.0, convergenza IT/OT) espone il settore a rischi di spionaggio industriale, sabotaggio e ransomware che possono bloccare la produzione. L'Italia, con il suo forte tessuto manifatturiero, è particolarmente esposta.
- **Altri settori rilevanti:** Il Rapporto Clusit evidenzia anche una significativa pressione su settori come Financial/Insurance (sebbene in calo rispetto agli anni precedenti, forse per effetto di normative come DORA), Education, News/Multimedia (protagonista di un attacco specifico su larga scala in Italia nel 2024) e Transportation/Storage.

Implicazioni per le PMI e la catena di fornitura

La consapevolezza del settore di appartenenza e delle relative minacce è il primo passo per una strategia di difesa mirata.

Questi dati hanno implicazioni dirette per le PMI:

- **Rischio Diretto:** Se la vostra PMI opera in uno dei settori più colpiti (es. manifatturiero, sanità, servizi per la PA), il vostro livello di rischio intrinseco è più elevato.
- **Rischio Indiretto (Supply Chain):** Anche se non operate direttamente in questi settori, potreste essere fornitori di aziende di questo tipo. Come discusso, la supply chain è un vettore d'attacco primario. La compromissione di una PMI fornitrice può essere il mezzo per colpire un cliente più grande e strategico. È quindi fondamentale che anche le PMI valutino la sicurezza dei propri partner e vengano a loro volta valutate dai propri clienti.

05 La Convergenza IT/OT: una sfida cruciale per il manifatturiero (e non solo)

Una delle tendenze tecnologiche più significative degli ultimi anni, con profonde implicazioni per la cybersecurity, è la crescente **convergenza tra Information Technology (IT) e Operational Technology (OT)**.

Questo fenomeno è particolarmente rilevante per le PMI del settore manifatturiero, ma riguarda anche molte altre realtà (energia, trasporti, building automation, etc.).

Comprendere le Differenze tra IT e OT
Tradizionalmente, IT e OT erano mondi separati:

- **IT (Information Technology):** Riguarda i sistemi usati per gestire dati e informazioni (computer, server, reti aziendali, email, applicazioni gestionali). Le priorità sono classicamente Confidentiality, Integrity, Availability (CIA).

- **OT (Operational Technology):** Riguarda i sistemi hardware e software usati per monitorare e controllare processi fisici (macchinari industriali, PLC, SCADA, sensori). Le priorità sono storicamente invertite: Availability, Integrity, Confidentiality (AIC). La sicurezza fisica e la continuità operativa sono la priorità.

La convergenza vede questi due mondi sempre più interconnessi: i dati dai sistemi OT vengono inviati ai sistemi IT per analisi (es. manutenzione predittiva), e i sistemi IT vengono usati per gestire e configurare i sistemi OT. Questo porta enormi benefici in termini di efficienza e innovazione, ma apre anche nuove superfici d'attacco.

Vulnerabilità Specifiche dell'OT

Gli ambienti OT presentano sfide di sicurezza uniche:

01. Sistemi legacy

Molti sistemi OT sono progettati per durare decenni e utilizzano sistemi operativi e protocolli obsoleti e non più supportati, per i quali le patch di sicurezza non sono disponibili.

02. Priorità operativa

La necessità di garantire l'operatività 24/7 spesso rende difficile applicare patch o implementare misure di sicurezza che potrebbero richiedere fermi macchina.

03. Protocolli insicuri

Molti protocolli di comunicazione OT non sono stati progettati con la sicurezza by design e mancano di autenticazione o crittografia.

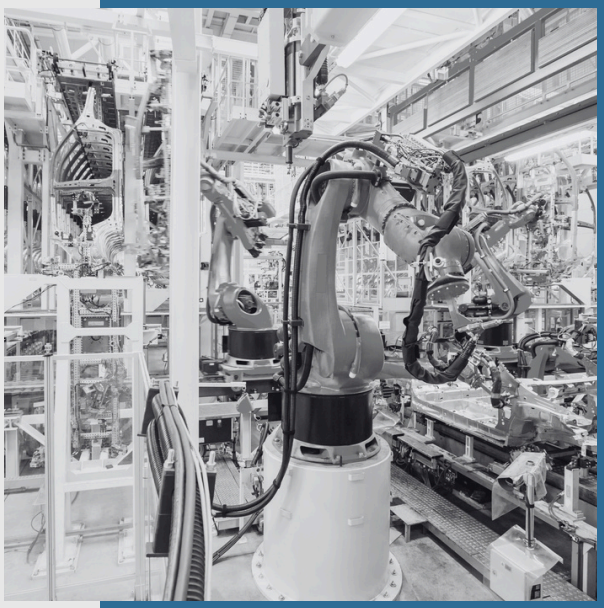
04. Conoscenze specifiche

La sicurezza OT richiede competenze che combinano conoscenze IT, OT e di processo industriale, spesso difficili da reperire.

05. Impatto fisico

Un attacco cyber a un sistema OT può avere conseguenze fisiche dirette (blocco produzione, danno a macchinari, rischi per la sicurezza dei lavoratori o per l'ambiente).

Strategie di Sicurezza per Ambienti Ibridi



Per le PMI manifatturiere, investire nella sicurezza OT non è un lusso, ma una necessità per proteggere il cuore produttivo dell'azienda.

Proteggere ambienti convergenti IT/OT richiede un approccio specifico:

- **Segmentazione della Rete:** Isolare rigorosamente le reti OT dalle reti IT tramite firewall e zone demilitarizzate (DMZ) è fondamentale per impedire che una compromissione in IT si propaghi all'OT (e viceversa).
- **Controllo Accessi Specifico:** Implementare controlli di accesso granulari (privilegio minimo) e MFA anche per gli accessi ai sistemi OT, specialmente quelli remoti.
- **Monitoraggio Dedicato:** Utilizzare strumenti di monitoraggio della sicurezza specifici per OT, capaci di comprendere i protocolli industriali e rilevare anomalie specifiche di quell'ambiente.
- **Gestione Vulnerabilità Adattata:** Applicare patch dove possibile, ma anche implementare controlli compensativi (es. Virtual Patching, Intrusion Prevention Systems - IPS) dove il patching diretto è rischioso.
- **Collaborazione IT/OT:** Creare team e processi che favoriscano la collaborazione tra i responsabili della sicurezza IT e gli ingegneri di processo/automazione OT.

06 5 Consigli Pratici per la strategia cyber nelle PMI (Ispirati alla NIS2)

La Direttiva Europea NIS2 (recepita in Italia con D.Lgs. 138/2024) stabilisce nuovi standard di cybersecurity per le entità "essenziali" e "importanti". Sebbene molte PMI potrebbero non rientrare direttamente nell'obbligo normativo nell'immediato, i principi e le misure richieste rappresentano delle best practice fondamentali per qualsiasi organizzazione che voglia gestire seriamente il rischio cyber. Ecco 5 aree chiave su cui concentrarsi, con consigli pratici adattati alla realtà delle PMI:

1. Conoscere sé stessi e i propri rischi (Gestione del Rischio - Rif. NIS2 Art. 21)

- **Principio:** Non puoi proteggere ciò che non conosci. Devi capire quali sono i tuoi asset digitali critici e quali rischi corrono.
- **Consigli Pratici per PMI:**
  - **Inventario Semplificato:** Mappa almeno i dispositivi chiave (server, PC critici, NAS), le applicazioni fondamentali (gestionale, CRM, posta elettronica) e dove risiedono i dati più importanti (clienti, contratti, progetti). Non dimenticare eventuali sistemi OT.
  - **Identifica i Processi Critici:** Quali attività sono vitali per far funzionare l'azienda? Quali sistemi IT/OT le supportano?
  - **Valutazione Rischi Pragmatica:** Chiediti: "Cosa succederebbe se il gestionale fosse bloccato da ransomware? E se le email dei commerciali venissero compromesse? E se il PLC principale si fermasse?". Valuta l'impatto (operativo, finanziario, reputazionale) e la probabilità (anche basandoti su questo whitepaper o notizie di settore). Concentrati sui 3-5 rischi maggiori.

2. Implementare Misure Tecniche e Organizzative Proporzionate (TOMs - Rif. NIS2 Art. 21)

- **Principio:** Adottare difese adeguate al rischio identificato, coprendo aspetti tecnici, procedurali e umani. La proporzionalità è chiave per le PMI.
- **Consigli Pratici per PMI:**

  - **Fondamentali dell'Accesso:** Password robuste e uniche, Multi-Factor Authentication (MFA) almeno per accessi esterni (VPN, email cloud) e amministratori. Gestione utenti (creazione/rimozione tempestiva).
  - **Protezione di Base:** Antivirus/EDR aggiornato su tutti i dispositivi, firewall perimetrale correttamente configurato, patching regolare di sistemi operativi e applicazioni critiche.
  - **Backup, Backup, Backup (e Test!):** Backup regolari dei dati critici, seguendo la regola 3-2-1 (3 copie, 2 supporti diversi, 1 offline/esterno).
    Fondamentale: testare periodicamente il ripristino. Un backup non testato è quasi inutile.
  - **Segmentazione (anche Semplice):** Se possibile, separare la rete Wi-Fi ospiti da quella aziendale. Se c'è un ambiente OT, separarlo rigorosamente dalla rete IT.

3. Prepararsi all'Incidente (Risposta e Segnalazione - Rif. NIS2 Art. 23)

- **Principio:** Un incidente accadrà. Avere un piano, anche semplice, su cosa fare riduce il panico, i tempi di recupero e i danni.
- **Consigli Pratici per PMI:**
  - **Piano di risposta minimo:** Chi chiamare (tecnico interno/esterno, MSSP)? Quali sono i primi passi (isolare la macchina? staccare la rete?)? Chi deve essere informato internamente? Scrivilo, anche poche righe.
  - **Contatti utili:** Tieni a portata di mano i contatti del tuo supporto IT/MSSP, del fornitore del gestionale, e magari un riferimento per consulenza legale/privacy in caso di data breach.
  - **Consapevolezza e segnalazione:** Anche se non soggetta a NIS2, una PMI deve segnalare un data breach al Garante Privacy (GDPR) se c'è rischio per i diritti degli interessati. Sapere a chi rivolgersi è importante.

4. Proteggere la Supply Chain (Sicurezza della Catena di Fornitura - Rif. NIS2 Art. 21)

- **Principio:** La tua sicurezza dipende anche da quella dei tuoi fornitori chiave (IT, software gestionali, servizi cloud, ma anche materie prime se impattano la produzione digitale).
- **Consigli Pratici per PMI:**
  - **Mappa dei fornitori critici:** Identifica i 3-5 fornitori la cui indisponibilità o compromissione avrebbe l'impatto maggiore sul tuo business.
  - **Due Diligence Semplice:** Quando scegli un nuovo fornitore IT o cloud, chiedi informazioni basilari sulle sue pratiche di sicurezza (certificazioni? gestione patch? backup?).
  - **Clausole Contrattuali:** Se possibile, includi nei contratti con fornitori critici (specialmente IT/software) clausole minime sulla sicurezza, sulla notifica in caso di incidenti che ti riguardano e sulla gestione dei dati alla fine del contratto.

5. Promuovere una Cultura della Sicurezza (Governance e Formazione - Rif. NIS2 Art. 20 & 21)

- **Principio:** La cybersecurity non è solo un problema dell'IT, ma riguarda tutti. La consapevolezza dei dipendenti è la prima linea di difesa. La direzione deve dare l'esempio.
- **Consigli Pratici per PMI:**
  - **Coinvolgimento direzione:** Il titolare o il management deve capire l'importanza della cyber sicurezza e supportare le iniziative (anche piccole) e i budget necessari.
  - **Formazione essenziale:** Organizza almeno una volta l'anno una breve sessione formativa (anche interna o con materiale online gratuito) sui rischi principali (phishing, password, uso sicuro dispositivi). Rendi consapevoli i dipendenti che loro sono un obiettivo.
  - **Policy semplici e chiare:** Definisci poche regole base sull'uso accettabile degli strumenti aziendali, sulla gestione delle password e su come segnalare eventi sospetti. Assicurati che siano comunicate e comprese.

Implementare questi consigli non elimina il rischio, ma lo riduce significativamente e pone le basi per una gestione più matura e resiliente della cybersecurity nella vostra PMI.

07 Conclusioni
Un percorso continuo verso la sicurezza

Il panorama della cybersecurity è innegabilmente complesso e in costante mutamento. Le minacce sono reali, sofisticate e, come abbiamo visto, non risparmiano le Piccole e Medie Imprese italiane, anzi, spesso le vedono come bersagli ideali.

Tuttavia, la consapevolezza è il primo passo verso la protezione. Comprendere il contesto globale e italiano, riconoscere le sfide specifiche del proprio settore (incluso l'emergente ambito OT) e abbracciare il concetto di cyber resilienza sono elementi fondamentali per costruire una difesa efficace.

Come abbiamo illustrato attraverso le lezioni tratte dal WEF Cyber Resilience Compass e i cinque consigli pratici ispirati alla NIS2, rafforzare la sicurezza non significa necessariamente stanziare budget proibitivi. Significa piuttosto adottare un approccio metodico e proporzionato:

- Conoscere i propri asset, processi critici e rischi principali.
- Proteggere con misure tecniche e organizzative fondamentali e ben gestite (MFA, patching, backup testati sono irrinunciabili).
- Prepararsi a rispondere agli incidenti con piani semplici ma chiari.
- Estendere lo sguardo alla sicurezza dei fornitori chiave.
- Coinvolgere tutta l'organizzazione, dalla direzione ai singoli dipendenti, nella creazione di una cultura della sicurezza.

Non siete soli in questo percorso. come MSSP, il nostro ruolo è proprio quello di supportarvi, fornendo competenze, strumenti e servizi scalabili per aiutarvi a navigare le complessità della sicurezza digitale e a concentrarvi sul vostro core business.

Investire oggi in cybersecurity e resilienza non è solo un modo per mitigare i rischi, ma un investimento strategico per garantire la continuità, la reputazione e il futuro successo della vostra impresa nell'economia digitale.

Proteggi oggi il futuro della tua azienda i rischi informatici non aspettano. Pianificare un assessment strutturato è il primo passo per mettere in sicurezza il tuo business.

Con **Vigilia Cyber**, analizziamo a fondo la tua esposizione alle minacce digitali, identifichiamo le vulnerabilità e costruiamo con te un piano solido per affrontare ogni sfida.

Richiedi ora una prima consulenza gratuita scrivendo a:
info@vigiliacyber.com