

# Come ottenere il Report di sicurezza informatica PID Cyber-Check 2.0

Guida a cura del Punto Impresa Digitale Maremma e Tirreno



CAMERA DI COMMERCIO  
MAREMMA E TIRRENO



pd  
punto  
impresa  
digitale

# Premessa

PID Cyber-Check è un test di self-assessment rapido e gratuito che aiuta l'impresa, attraverso alcune domande on line, ad avere una primissima valutazione del suo livello di rischio di subire un attacco informatico.

Al termine del test viene generato un **Report** che indica gli eventuali rischi a cui l'impresa può andare incontro.

Lo scopo dello strumento è quello di offrire un modo semplice e veloce per effettuare un **self-assessment** dei cyber rischi e **ottimizzare gli investimenti in cyber sicurezza**.



DITEC  
CONSORZIO PER L'INNOVAZIONE  
TECNOLOGICA



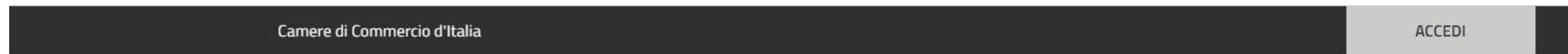
START4.0





# Accedi alla piattaforma nazionale del PID

PID Cyber Check è disponibile online su [www.puntoimpresadigitale.camcom.it](http://www.puntoimpresadigitale.camcom.it) nella sezione "Gli Strumenti di assessment per le imprese"



Seguici su:



[News](#) [Docuweb 4.0](#) [Approfondimenti](#) [Rassegna web](#) [Covid-19 - ripartenza Digitale](#)



Cosa sono i **Punti Impresa Digitale** e il Network Impresa 4.0

Dove sono i **Punti Impresa Digitale**

I servizi dei **Punti Impresa Digitali**

Gli **Strumenti di assessment** per le imprese

I **voucher digitali 4.0**

I servizi "**digitali**" delle Camere di Commercio

Premio **TOP of the PID**

Clicca su "Gli strumenti di assessment per le imprese"



# Assessment Checkup Sicurezza IT per le imprese

PID Cyber Check è disponibile online su  
[www.puntoimpresadigitale.camcom.it](http://www.puntoimpresadigitale.camcom.it)

Assessment Checkup Sicurezza IT per le imprese

CHECKUP Sicurezza IT

I PID offrono un servizio specifico per aiutare l'impresa a capire i **rischi informatici** ai quali è esposta: dagli attacchi cyber, alle truffe telematiche, al furto di identità e molto altro. Questo aiuta l'impresa a capire se sta tutelando i propri dati ma anche quelli di clienti e fornitori, utilizzando misure e strumenti appropriati. Conoscere tempestivamente queste situazioni e quali punti di accesso o vulnerabilità sono già a conoscenza degli hackers informatici, aiuta concretamente un imprenditore anche sprovvisto di competenze tecnologiche, a fare il primo passo verso una **maggiore sicurezza della sua struttura**.

SCOPRI DI PIÙ

Assessment delle competenze digitali

DIGITAL SKILL VOYAGER

Digital Skill Voyager è il nuovo strumento per la valutazione delle competenze digitali rivolto a studenti e lavoratori e, più in generale, a tutti coloro che cercano uno strumento specifico per misurare le proprie competenze digitali e per valorizzarle sul mercato del lavoro.

SCOPRI DI PIÙ

Clicca su "Scopri di più"

Assessment Checkup Sicurezza IT per le imprese

I PID offrono un servizio specifico per aiutare l'impresa a capire i **rischi informatici** ai quali è esposta: dagli attacchi cyber alle truffe telematiche passando dal furto di identità e molto altro. Questo aiuta l'impresa a capire se sta tutelando i propri dati, ma anche quelli di clienti e fornitori, utilizzando misure e strumenti appropriati. Conoscere tempestivamente queste situazioni e quali punti di accesso o vulnerabilità sono già a conoscenza degli hackers informatici, aiuta concretamente un imprenditore anche sprovvisto di competenze tecnologiche, a fare il primo passo verso una **maggiore sicurezza della sua struttura**. In questa direzione, il nuovo servizio di **assessment sulla "Sicurezza Informatica"** offerto **alle imprese** prevede due differenti strumenti di analisi:

CHECKUP Sicurezza IT PID Cyber Check

**PID Cyber Check**

È un test molto rapido di circa 30 domande che consente una prima auto-valutazione del livello di rischio di un attacco informatico al quale l'impresa è esposta.

"PID Cyber Check" non fornisce indicazione circa i presidi da mettere in atto per proteggere l'impresa da attacchi cyber, ma permette di focalizzare gli eventuali rischi a cui si può andare in contro restituendo anche una stima del danno economico derivante dai possibili attacchi. Il servizio è gratuito, potrà essere realizzato dall'impresa in completa autonomia e al termine verrà prodotto un report personalizzato elaborato sulla base delle risposte fornite al test.

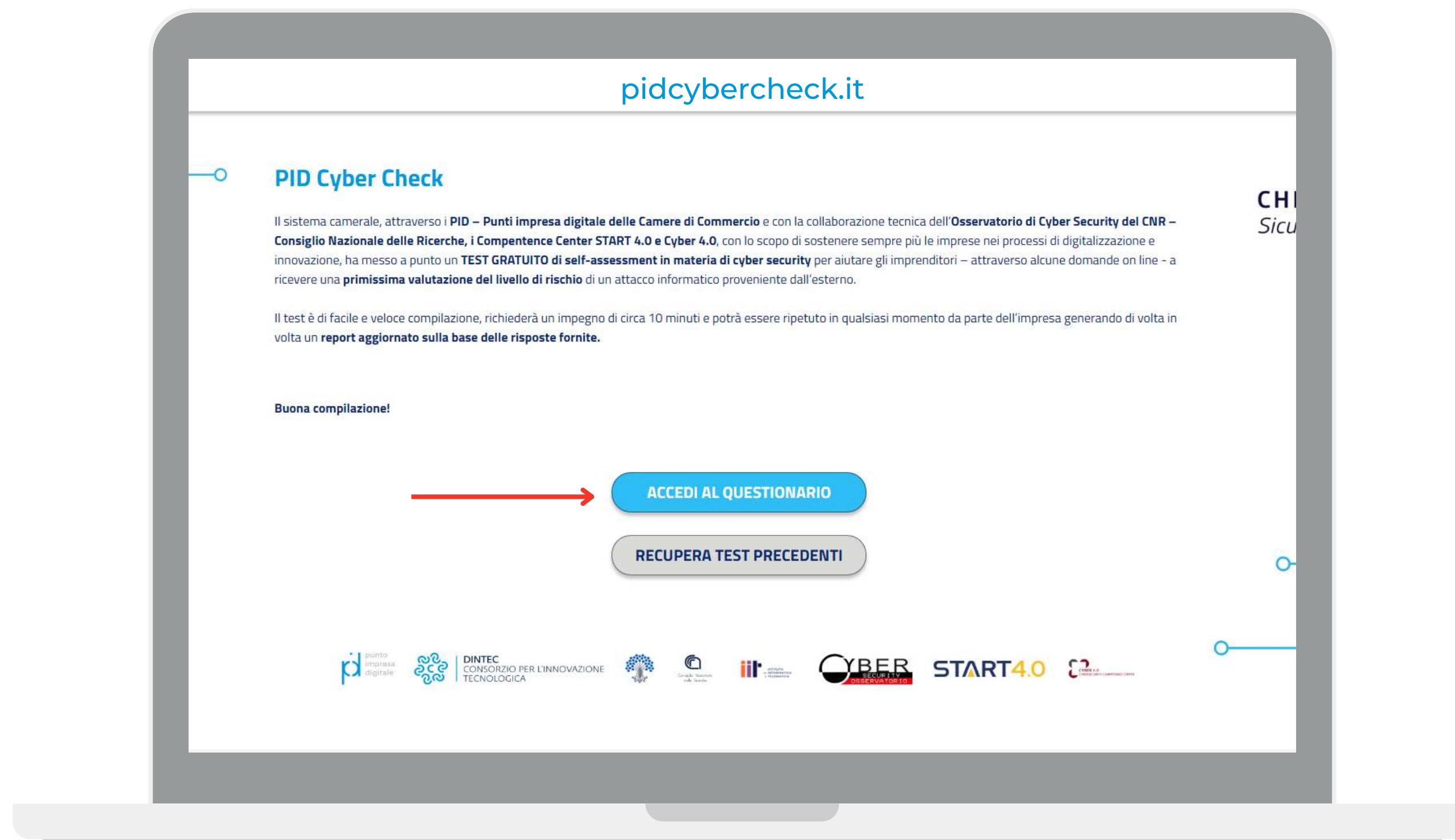
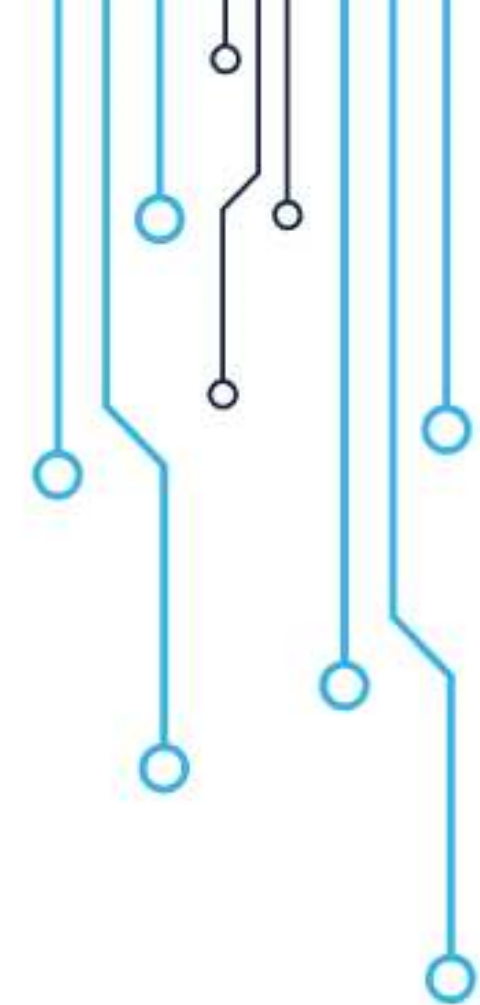
Clicca **qui** per vedere un'anteprima del report di cyber security oppure **qui** per accedere ed effettuare il "PID Cyber Check".

Clicca su "qui" in basso



# Accedi al questionario

In caso di prima compilazione clicca su "Accedi al questionario"  
altrimenti inserisci il **Codice di recupero** per recuperare il test precedente





# Registrati al "PID Cyber Check"

Inserisci le informazioni richieste, acconsenti al trattamento dei dati e clicca su "Inizia"

**INFORMAZIONI SULL'ORGANIZZAZIONE**

Ragione Sociale \*

CF/ Partita IVA dell'impresa \*

Stato \*

Regione \*

Provincia \*

Email di contatto \*

**Informativa dati personali**

Ho preso visione dell'INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI ai sensi dell'articolo 13 del Reg. UE 679/2016 e sul trattamento dei dati per le finalità previste dalla mappatura, sollevando DINTEC Srl (Consorzio per l'Innovazione Tecnologica) da ogni responsabilità sui contenuti di terze parti, e obbligandosi a mantenere indenne DINTEC Srl da tutti i danni che dalla pubblicazione di tali contenuti potranno derivare.

L'interessato ha dichiarato di aver preso visione dell'informativa di cui sopra, esprime il consenso per il trattamento dei dati connessi alle seguenti finalità:

- \* Acconsento al trattamento dei miei dati personali per finalità di registrazione/adesione al PID-Cybercheck, e realizzazione dell'auto-assessment.
- Acconsento al trattamento dei miei dati personali per la finalità di invio di comunicazioni informative su ulteriori iniziative promosse da Unioncamere sul tema.
- Acconsento al trattamento dei miei dati personali per l'invio di comunicazioni informative su ulteriori e diverse iniziative promosse dalla CCIAA/PID competente territorialmente sul tema.

Non sono un robot

[Esci senza salvare](#) [Inizia](#)

2024® Lifetronic [Impostazioni cool](#)



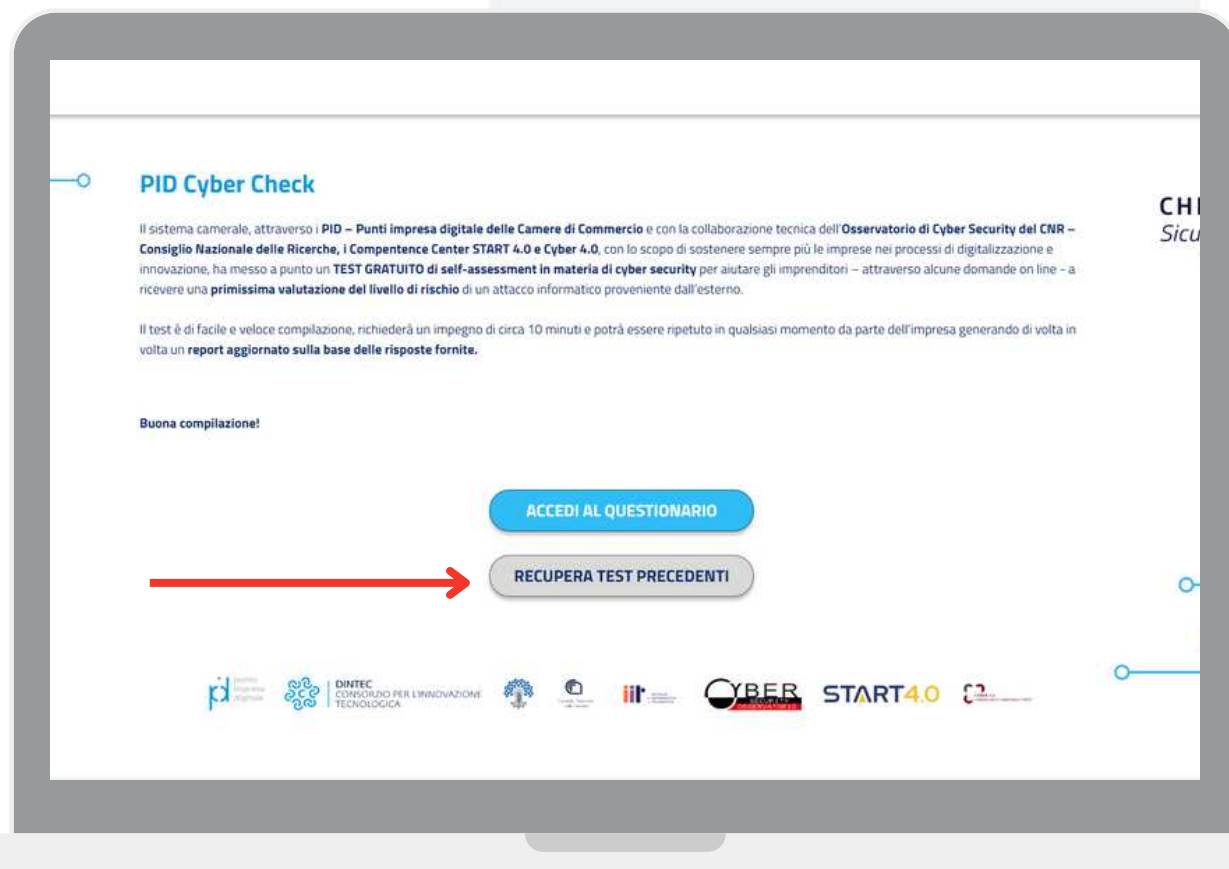
# Ricevi mail con il Codice di recupero del questionario

Dopo aver effettuato la registrazione, riceverai una mail con il Codice che potrai utilizzare per recuperare il questionario una volta concluso e aggiornarlo

Codice recupero questionario >

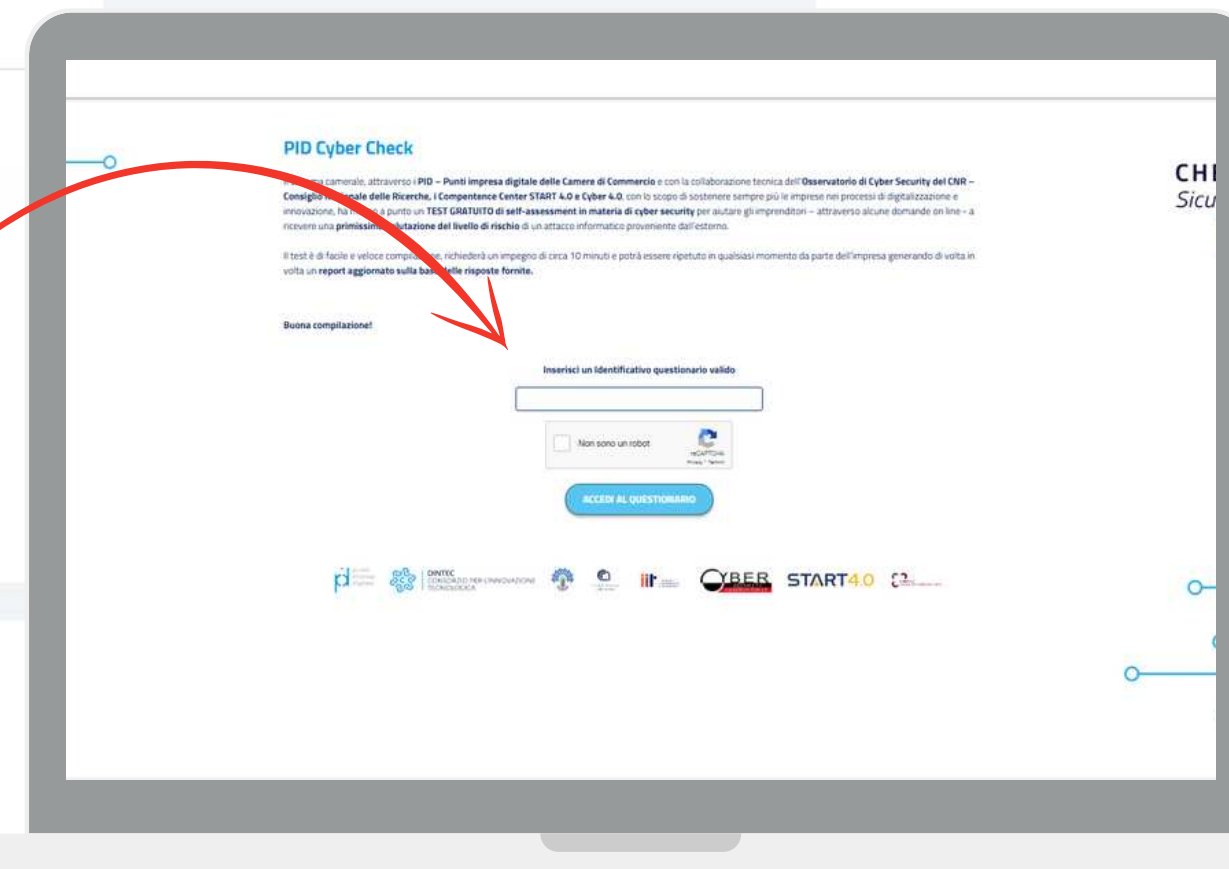
no-reply@pidcybercheck.it  
a me

È stato generato un ID Compilazione per questo questionario e inviato via mail all'indirizzo specificato, che potrai utilizzare in futuro per recuperare il questionario e per modificare le risposte date.



Gentile  
grazie per aver iniziato la compilazione di un questionario. di seguito il codice per recuperare quest'ultimo: **678f62da4b19c4eadfc543cc**

Cordiali Saluti  
PidCyberCheck.





# Calcola il rischio

Dopo aver risposto a tutte le domande  
clicca su “Concludi” in basso a destra

CHECKUP Scanner 4.0

DETECT, RESPOND AND RECOVER

Quali strumenti di protezione dalle minacce informatiche vengono utilizzati sui dispositivi (es. smartphone, desktop, laptop, server, etc.)? \*

- Endpoint Security Solution (inclusi antivirus, firewall, gestione delle vulnerabilità, ecc.)
- Solo antivirus (anche gratuito o incluso nel sistema operativo);
- Nessuna delle precedenti;

Quali sono le procedure/sistemi che vengono utilizzati per bloccare l'installazione di utility/tools/mobile apps non consentite sui dispositivi mobili/non mobili (sono consentite risposte multiple)? \*

- Procedure scritte (ad esempio nella policy aziendale sulla cybersecurity);
- Meccanismi automatici per la verifica/monitoraggio dell'installazione;
- Nessuna delle precedenti;

La sua impresa ha previsto delle procedure di scansione delle vulnerabilità? \*

- Sì, scansioni di vulnerabilità vengono effettuate regolarmente e si applicano su tutto il sistema (e.g., servers, cloud, end points, other network devices, etc.)
- Sì, scansioni di vulnerabilità vengono effettuate regolarmente ma si applicano solo per componenti critiche del sistema (e.g., servers e risorse cloud )
- Sì, le scansioni di vulnerabilità vengono eseguite occasionalmente
- No, l'impresa non ha mai eseguita scansioni delle vulnerabilità.

Come si analizzano le informazioni di registrazione (sono consentite risposte multiple)? \*

- Analisi dei dati di registrazione sistematica/periodica;
- Analisi dei dati a seguito di eventi criminali;
- Nessuna analisi dei dati;

E' prevista una procedura per il ripristino dopo un incidente inerente la sicurezza informatica (sono consentite risposte multiple)? \*

- Sì, è stata definita una procedura da seguire a seguito di incidente informatico. Il personale coinvolto è stato appositamente informato. La procedura viene periodicamente testata per verificarne l'efficacia.
- Sì, in caso di incidente il responsabile della sicurezza interviene per attivare risorse specializzate interne o esterne per ripristinare i sistemi.
- No, non è prevista una procedura specifica.

SALVA LE MODIFICHE ED ESCI   ESCI SENZA SALVARE

PAGINA 5/5

\* Obbligatoria

INDIETRO   CONCLUDI

Clicca su “Concludi” per  
terminare il questionario





# Questionario effettuato!

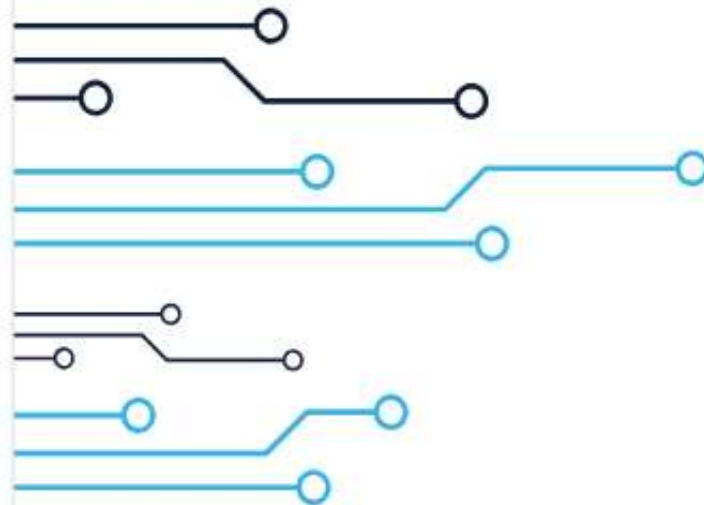
Leggi il Report PID Cyber Check direttamente online oppure scaricalo attraverso il link che riceverai per mail

## Questionario effettuato!

Puoi consultare il report qui di seguito.  
Inoltre, riceverai il link per scaricare il report in formato PDF via e-mail all'indirizzo specificato.



**DITEC**  
CONSORZIO PER L'INNOVAZIONE  
TECNOLOGICA



**CHECKUP**  
Sicurezza IT



**PID**  
Cyber  
Check

**LIVELLO DI RISCHIO DI SICUREZZA INFORMATICA RILEVATO**

25 rischio basso | 75 rischio alto

Livello del rischio: 43/100

Di seguito è riportata una breve descrizione dei quadranti di rischio figura che tengono conto delle risposte fornite al "PID Cyber Check":

- RISCHIO BASSO** - Un basso livello di rischio è intrinsecamente la strada corretta in risultato non deve indurre l'impresario a un esame approfondito.
- RISCHIO MEDIO** - Un medio livello di rischio indica ampi margini di miglioramento esame più approfondito dei sistemi definire politiche e gli interventi mettere in atto.
- RISCHIO ALTO** - Un alto livello di rischio indica criticità in tema di cybersecurity effettuare ulteriori approfondimenti a sistemi più approfonditi di ridurre il rischio cibernetico.

**INDICATORI DI RISCHIO E MITIGAZIONE DELL'IMPRESA**

I grafici, in calce, rappresentano la performance dell'impresa rispetto alle grandezze "Fonti di Rischio" e "Misure di Difesa" che, nel complesso, ricostruiscono la performance dell'organizzazione attraverso il binomio "attacco-difesa" in grado di esplorare il rischio informatico rispetto a diverse dimensioni "strutturali".

ESPOSIZIONE ALLA MINACCIA	FONTI DI RISCHIO	MITIGAZIONE DEL RISCHIO
ESPOSIZIONE ALLA MINACCIA	ESPOSIZIONE ALLA MINACCIA: Insieme dei fattori che aumentano o diminuiscono la probabilità con cui la minaccia stessa può manifestarsi.	IDENTIFY: Consapevolezza del contesto operativo dell'azienda, compresi gli asset critici per i processi aziendali e i rischi ad essi legati. Questa consapevolezza consente all'organizzazione di allineare
INFRASTRUTTURA	INFRASTRUTTURA: Gestione dei sistemi e delle reti che supportano le operazioni aziendali, garantendo la protezione e l'integrità dei dati e dei servizi (enti).	PROTECT: Conoscenza del contesto operativo dell'azienda, compresi gli asset critici per i processi aziendali e i rischi ad essi legati. Questa consapevolezza consente all'organizzazione di allineare

**STATO ATTUALE DEL PROFILO DI GESTIONE DEL RISCHIO CIBERNETICO DELL'IMPRESA**

Completivamente in base alle tue risposte ti diamo il tuo profilo di gestione del rischio che potrà essere utile per continuare il percorso con i digital promoter della tua camera di commercio, così da individuare come continuare il tuo cammino sulla cybersecurity.

**IN BASE ALLE RISPOSTE FORNITE L'IMPRESA RISULTA ESSERE AL SEGUENTE LIVELLO:**

1° LIVELLO 2° LIVELLO 3° LIVELLO 4° LIVELLO 5° LIVELLO

**PROTEZIONE**

**CONSAPEVOLE**

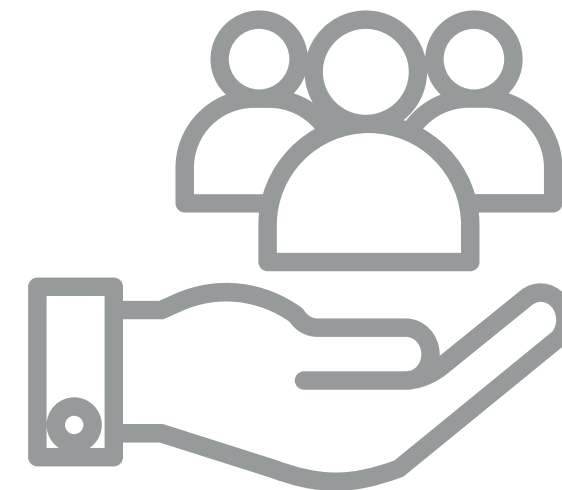
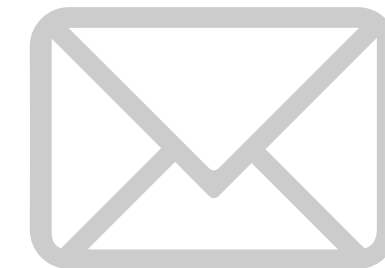
L'organizzazione ha processi interni per gestire il rischio cibernetico, ma non sono estesi a tutta l'organizzazione. La consapevolezza del rischio cibernetico è presente, ma non è accompagnata da processi di gestione diffusi a tutti i livelli organizzativi dell'impresa. La condivisione di strategie sulla cybersecurity con gli stakeholder esterni è principalmente di tipo passivo e occasionale.

18% ESPOSIZIONE ALLA MINACCIA | 41% INFRASTRUTTURA

# Hai bisogno di assistenza?

Invia una mail a [pid@lg.camcom.it](mailto:pid@lg.camcom.it) indicando nel testo:

- Ragione sociale
- Codice fiscale/Partita Iva
- Provincia di riferimento
- Indirizzo e-mail indicato in fase di registrazione al PID Cyber Check
- Problematica da risolvere





CAMERA DI COMMERCIO  
MAREMMA E TIRRENO



pd punto  
impresa  
digitale

# Punto Impresa Digitale Maremma e Tirreno

---



Piazza del Municipio, 48 - LI / V. F.lli Cairoli, 10 - GR



[www.lg.camcom.it](http://www.lg.camcom.it)



[pid@lg.camcom.it](mailto:pid@lg.camcom.it)



0586 231 262



Gruppo | Punto Impresa Digitale Maremma e Tirreno