IMPRESA SICURA
I nuovi strumenti per la Sicurezza Informatica offerti dal PID

PUNTO IMPRESA DIGITALE MAREMMA E TIRRENO – 19 SETTEMBRE 2022

CAMERA DI COMMERCIO
MAREMMA E TIRRENO

punto impresa digitale

AGENDA

- Introduzione: il lato oscuro del digitale per le imprese
- Il ruolo del PID in tema di Cyber security
- Il nuovo servizio **Check-up Sicurezza Informatica per le PMI**
  - PID Cyber Check
  - Cyber Exsposure Index (CEI)
- Gli altri servizi offerti dal Punto Impresa Digitale in breve
- Q&A

punto impresa digitale

INTRODUZIONE

Il lato oscuro del digitale per le imprese

Internet ha introdotto **grandi opportunità di ampliamento del *business*** e di visibilità della propria impresa su nuovi mercati; la **grande facilità con cui vengono create soluzioni tecnologiche a supporto del *business*** è un incredibile stimolo per la crescita delle imprese.

Di contro, questa grande semplicità ha aumentato sensibilmente la quantità di rischi a cui le imprese sono esposte, dagli **attacchi *cyber***, alle **truffe telematiche**, al **furto di identità** e molti altri.

Il rischio informatico

Il **rischio informatico** è un rischio di tipo operativo associato alle perdite economiche inflitte ad un organizzazione dalla mancata **confidenzialità**, **disponibilità** o **integrità** di informazioni e/o sistemi informativi propri o di terzi.

La sua origine può essere:

- **Accidentale**: si tratta di eventi che si verificano indipendentemente dalla volontà di tutti i soggetti coinvolti (es. spegnimento dei server)
- **Deliberata**: evento che deriva da azioni volontarie da parte di soggetti che hanno scopi personali di varia natura (es. fughe di dati)

- **CONFIDENZIALITA'**: garanzia che i sistemi forniscano l'informazione solo a chi è autorizzato ad ottenerla;
- **DISPONIBILITA':** garanzia che l'informazione sia accessibile solo a chi può accedervi ;
- **INTEGRITA':** garanzia che l'informazione sia conservata in forma inalterata.

Esempi di attacco informatico

PHISHING

Il **phishing** inizia con una e-mail che sembra provenire da un mittente affidabile e che invece contiene link malevoli volti a convincere la vittima a fornire dati riservati

MALWARE

Un **software** progettato per arrecare danni al sistema che «infetta». Si può trattare o meno di un virus

RANSOWARE

Virus che prende il controllo del computer di un utente ed esegue la crittografia dei dati, quindi chiede un riscatto per ripristinarne il normale funzionamento

Studio di ENISA su Cyber security e PMI

Agenzia europea per la Cyber security

Le PMI offrono ai cyber criminali un buon rapporto valore/rischio: molte PMI forniscono servizi a organizzazioni più grandi e **possono consentire di attaccare le organizzazioni più grandi attraverso la supply chain**. Ogni impresa per quanto piccola sia infatti ha:

RETE INFORMATICA

COMPUTER

POSTA ELETTRONICA

FORNITORI E CLIENTI

Tutti questi canali sono esposti al rischio di attacchi e possono diventare oggetto di interesse da parte di attori malevoli.

Studio di ENISA su Cyber security e PMI

Agenzia europea per la Cyber security

Le SFIDE che sono chiamate ad affrontare le PMI sono le seguenti:

1. Scarsa consapevolezza della sicurezza informatica fra il personale
2. Protezione inadeguata delle informazioni critiche
3. Mancanza di budget adeguati
4. Mancanza di specialisti o di capacità adeguati in materia di cyber security
5. Mancanza di adeguate linee guida per le PMI
6. SHADOW IT: spostamento del lavoro in ambienti ICT fuori dal controllo delle imprese

Come proteggersi?

Un'efficacie strategia di ***Cyber security*** richiede un'analisi delle **minacce**, delle **vulnerabilità** e dei **rischi** associati all'impiego di sistemi informativi nonché l'attuazione di **adeguate e specifiche misure difensive**.

Quando si parla di misure difensive occorre distinguere:

- **Misure di prevenzione**: agiscono riducendo la probabilità di realizzazione di una minaccia
- **Misure di protezione**: agiscono riducendo la gravità del danno prodotto da un attacco o da un crimine informatico

- **MINACCIA:** potenziale capacità di un'azione di arrecare un danno sfruttando le vulnerabilità dell'infrastruttura;
- **VULNERABILITA'**: debolezza di un sistema di sicurezza che può essere sfruttata per arrecare un danno.

..Raccomandazioni di processo

AUDIT PERIODICI

UTILIZZO DI ACCESSI CENTRALIZZATI E CORRETTA GESTIONE DELLE PASSWORD

PATCH ED AGGIORNAMENTI SOFTWARE REGOLARI E AUTOMATIZZATI

PROTEZIONE DEI DATI PERSONALI

PIANIFICAZIONE E RISPOSTA AGLI INCIDENTI DI SICUREZZA

La maggioranza degli incidenti e cyber attacchi è causata da **errori umani**.

..Raccomandazioni tecniche

- **SICUREZZA DELLE RETI**: soprattutto attraverso firewall
- **ANTIVIRUS**: su tutti i dispositivi e endpoint
- Strumenti di **protezione della posta elettronica**
- **CRITTOGRAFIA**: applicata a più livelli possibili, utilizzando VPN per le connessioni
- **MONITORAGGIO DELLA SICUREZZA**
- **SICUREZZA FISICA** degli ambienti e dei dispositivi utilizzati
- **BACKUP** sicuri, il più possibile separati, regolari e crittografati

REGOLA 3 – 2 – 1

Conservare 3 copie dei dati, archiviarle in 2 archivi diversi e avere almeno 1 backup esterno al perimetro aziendale

IL RUOLO DEL PID IN TEMA DI CYBERSECURITY

CAMERA DI COMMERCIO
MAREMMA E TIRRENO

punto
impresa
digitale

IL SUPPORTO DEL PID MAREMMA E TIRRENO

Le imprese maggiormente esposte al **rischio di attacco informatico** sono accomunate da tre fattori:

SCARSA ATTENZIONE ALLA DIFESA DIGITALE

POCA CONSAPEVOLEZZA DEI PROPRI RISCHI CYBER

BASSI INVESTIMENTI IN FORMAZIONE E DIFESA DIGITALE

Le risposta del **PUNTO IMPRESA DIGITALE**

CHECKUP
Sicurezza IT

EVENTI INFO - FORMATIVI

STRUMENTI DI ANALISI DEL RISCHIO INFORMATICO

MISURA A – BANDO A SOSTEGNO DELLA DIGITALIZZAZIONE

CAMERA DI COMMERCIO MAREMMA E TIRRENO

punto impresa digitale

EVENTI INFO - FORMATIVI

Volendo diffondere la **cultura del digitale**, ogni anno il PID Maremma e Tirreno organizza vari corsi di formazione.

Per il 2022 sono stati attivati due percorsi formativi diversi, uno volto ad incrementare le **competenze digitali di base**, l'altro pensato per aumentare la conoscenza delle **tecnologie abilitanti** previste dal Piano Transizione 4.0

STRUMENTI DI ANALISI DEL RISCHIO INFORMATICO

CAMERA DI COMMERCIO
MAREMMA E TIRRENO

punto
impresa
digitale

BANDO PER L'EROGAZIONE DI CONTIRBUTI A SOSTEGNO DELLA DIGITALIZZAZIONE

Risorse stanziate: € 280.000,00

Beneficiari: PMI delle province di Grosseto e Livorno

Spese: sostenute dal 1° gennaio 2022

Termine per la presentazione delle domande: 30 novembre 2022

Presentazione della domanda: tramite piattaforma dal sito *www.registroimprese.it*

CAMERA DI COMMERCIO MAREMMA E TIRRENO

punto impresa digitale

TRE MISURE DI INTERVENTO ALTERNATIVE

MISURA A
PID 4.0

MISURA B
Strumentazione digitale

MISURA C
Prevenzione crisi d'impresa

CAMERA DI COMMERCIO MAREMMA E TIRRENO

punto impresa digitale

MISURA A: PID 4.0

FINALITA': promuovere l'utilizzo di servizi o soluzioni focalizzati sulle nuove competenze e tecnologie digitali nell'ambito delle attività previste dal **Piano Transizione 4.0**

ENTITA' DEL CONTRIBUTO: pari al **70% delle spese** nette effettivamente sostenute e ammissibili, fino ad un **massimo di € 6.000,00**

INVESTIMENTO MINIMO: € 3.000,00

SPESE AMMISSIBILI

- **Acquisto di beni strumentali materiali ed immateriali** (min il 70% delle spese ammissibili) funzionali all'introduzione delle tecnologie abilitanti dell'Elenco 1 ed eventualmente di una o più tecnologie dell'Elenco 2 di cui al Piano Transizione 4.0
- **Servizi di consulenza e/o formazione** (max il 30% delle spese ammissibili)

MISURA A: PID 4.0

Elenco 1	Elenco 2
Robotica avanzata e collaborativa	Sistemi di pagamento mobile e/o via Internet
Interfaccia uomo-macchina	Sistemi fintech
Manifattura additiva e stampa 3D	Sistemi EDI, electronic data interchange
Prototipazione rapida	Geolocalizzazione
Internet delle cose e delle macchine	Tecnologie per l'in-store customer experience
Cloud, High Performance Computing - HPC, fog e quantum computing	System integration applicata all'automazione dei processi
Soluzioni di cyber security e business continuity	Tecnologie della Next Production Revolution (NPR)
Big data e analytics	Programmi di digital marketing
Intelligenza artificiale	Soluzioni tecnologiche per la transizione ecologica
Blockchain	Connettività a Banda Ultralarga
Soluzioni tecnologiche per la navigazione immersiva, interattiva e partecipativa	Sistemi per lo smart working e il telelavoro
Simulazione e sistemi cyberfisici	Sistemi di e-commerce
Integrazione verticale e orizzontale	Soluzioni tecnologiche digitali per l'automazione del sistema produttivo e di vendita
Soluzioni tecnologiche digitali di filiera per l'ottimizzazione della supply chain	
Soluzioni tecnologiche per la gestione e il coordinamento dei processi aziendali con elevate caratteristiche di integrazione delle attività	

IL NUOVO SERVIZIO CHECK UP SICUREZZA INFORMATICA PER LE PMI

CAMERA DI COMMERCIO
MAREMMA E TIRRENO

punto
impresa
digitale

STRUMENTI DI ANALISI DEL RISCHIO INFORMATICO

CAMERA DI COMMERCIO
MAREMMA E TIRRENO

punto
impresa
digitale

IL PID CYBER CHECK

CAMERA DI COMMERCIO
MAREMMA E TIRRENO

punto
impresa
digitale

PID CYBER CHECK

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 informatico**.

Al termine del test viene generato un **Report** che indica gli eventuali rischi a cui l'impresa può andare incontro e fornisce una **stima del danno economico** derivante dai possibili attacchi.

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.

CHECKUP Sicurezza IT

PID Cyber Check

Consiglio Nazionale delle Ricerche

CYBER SECURITY OSSERVATORIO

ISTITUTO DI INFORMATICA E TELEMATICA

START4.0

CAMERA DI COMMERCIO MAREMMA E TIRRENO

punto impresa digitale

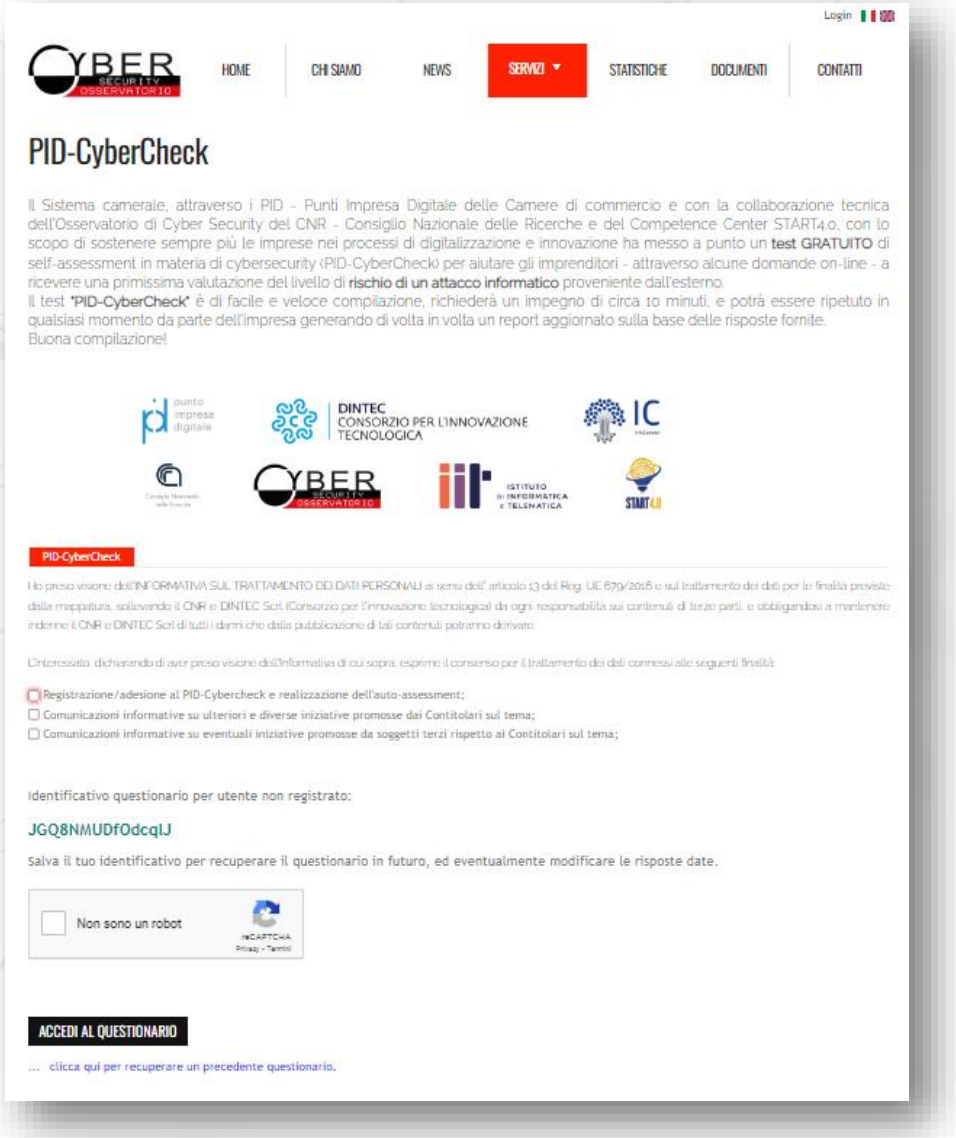
COME RICHIEDERLO?

Per accedere alla compilazione del **PID Cyber Check** occorre collegarsi a:

WWW.CYBERSECURITYOSSERVATORIO.IT

Selezionare *Registrazione/adesione al PID Cybercheck e realizzazione dell'auto-assessment*

Flaggare *Non sono un robot*



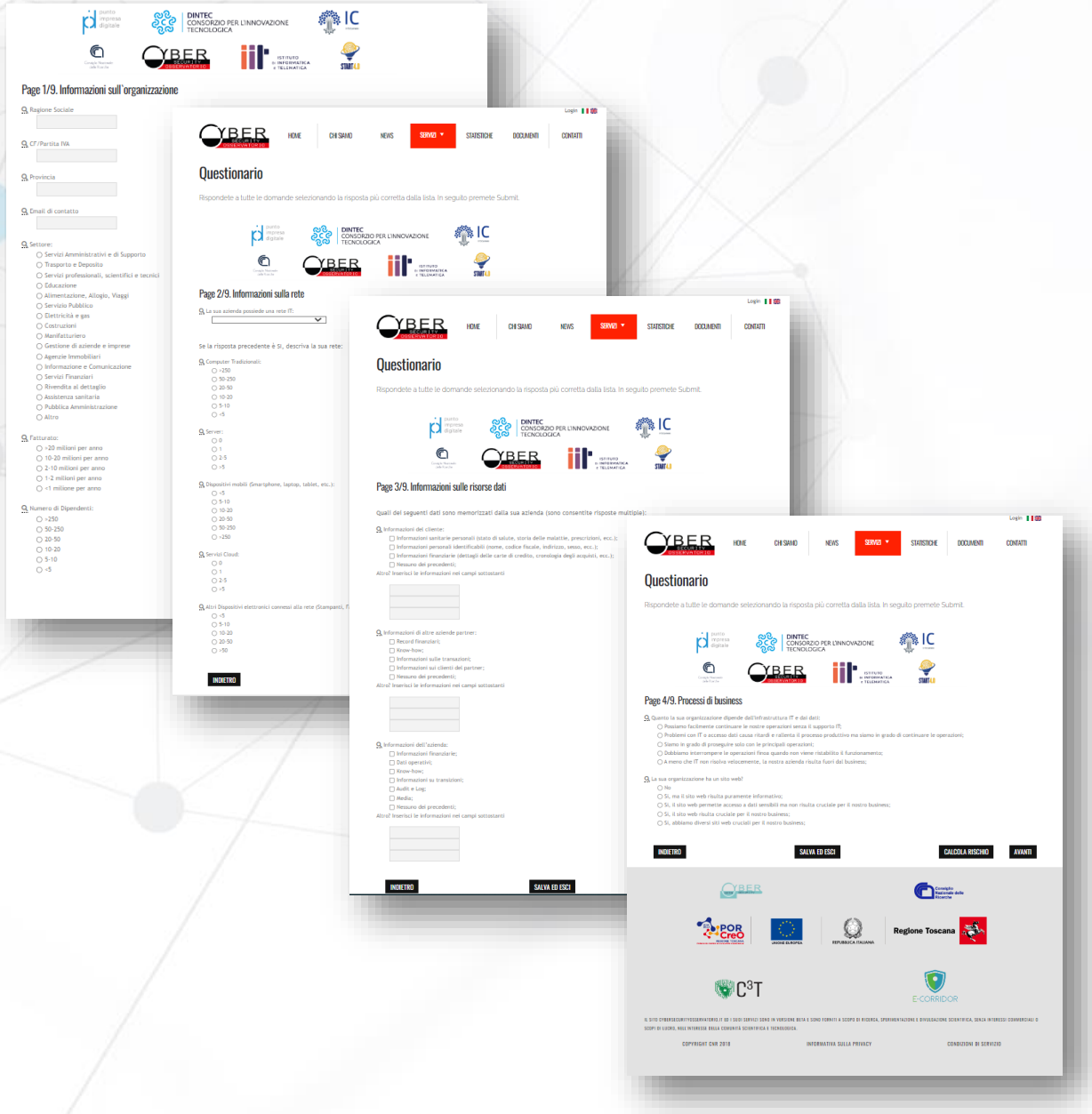
CAMERA DI COMMERCIO MAREMMA E TIRRENO

punto impresa digitale

QUESTIONARIO

Nella prima parte del questionario vengono poste domande che fanno riferimento agli **aspetti descrittivi dell'impresa e ai suoi assets**

- **Informazioni sull'organizzazione**
- **Informazioni sulla rete**
- **Informazioni sulle risorse dati**
- **Processi di business**



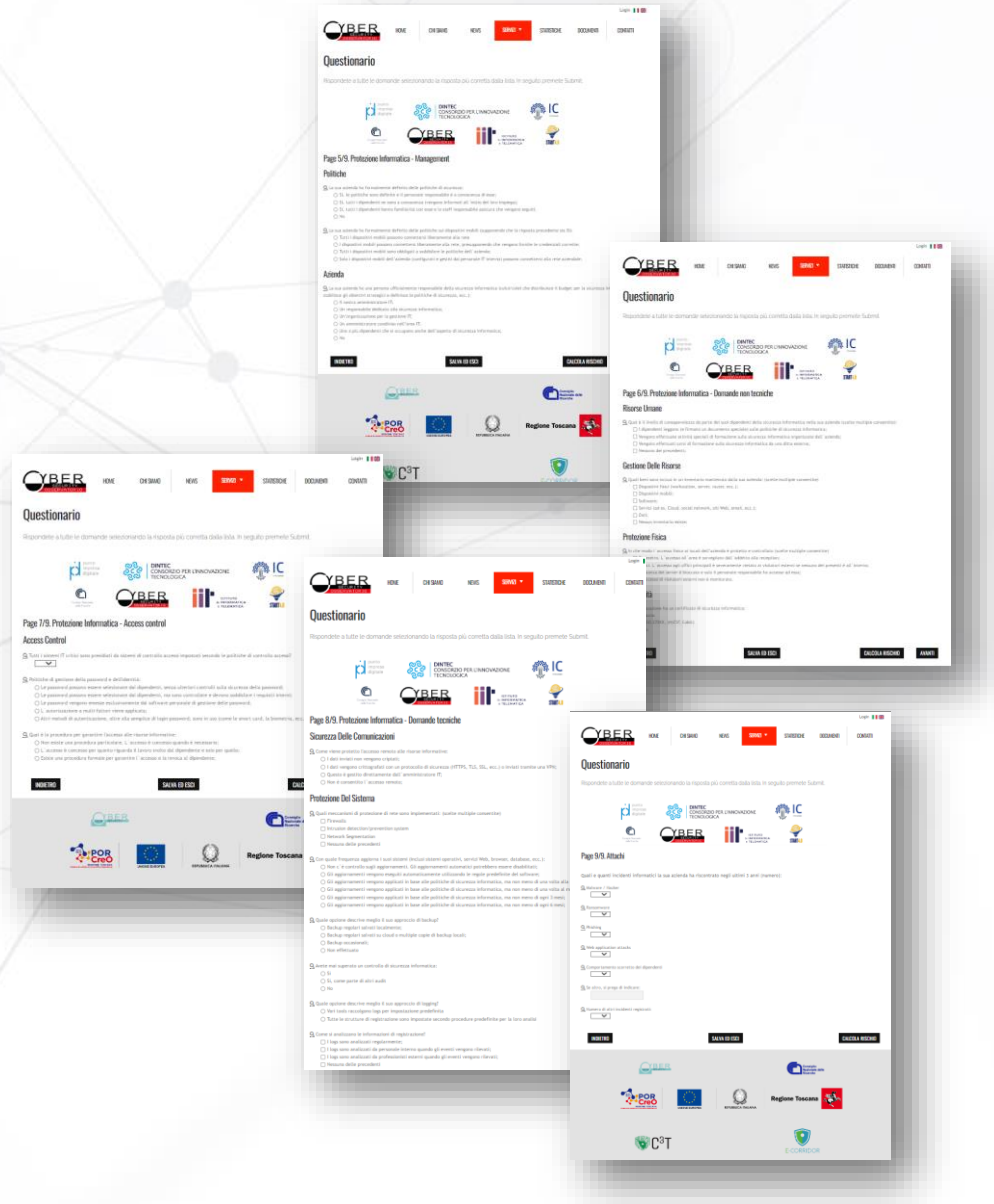
CAMERA DI COMMERCIO MAREMMA E TIRRENO

punto impresa digitale

QUESTIONARIO

Nella seconda parte del questionario le domande riguardano i **controlli di sicurezza**

- **Protezione Informatica – Domande non tecniche**
- **Protezione informatica – Domande Tecniche**
  - Access Control
  - Sicurezza delle Comunicazioni
  - Protezione del Sistema
  - Attacchi



CAMERA DI COMMERCIO MAREMMA E TIRRENO

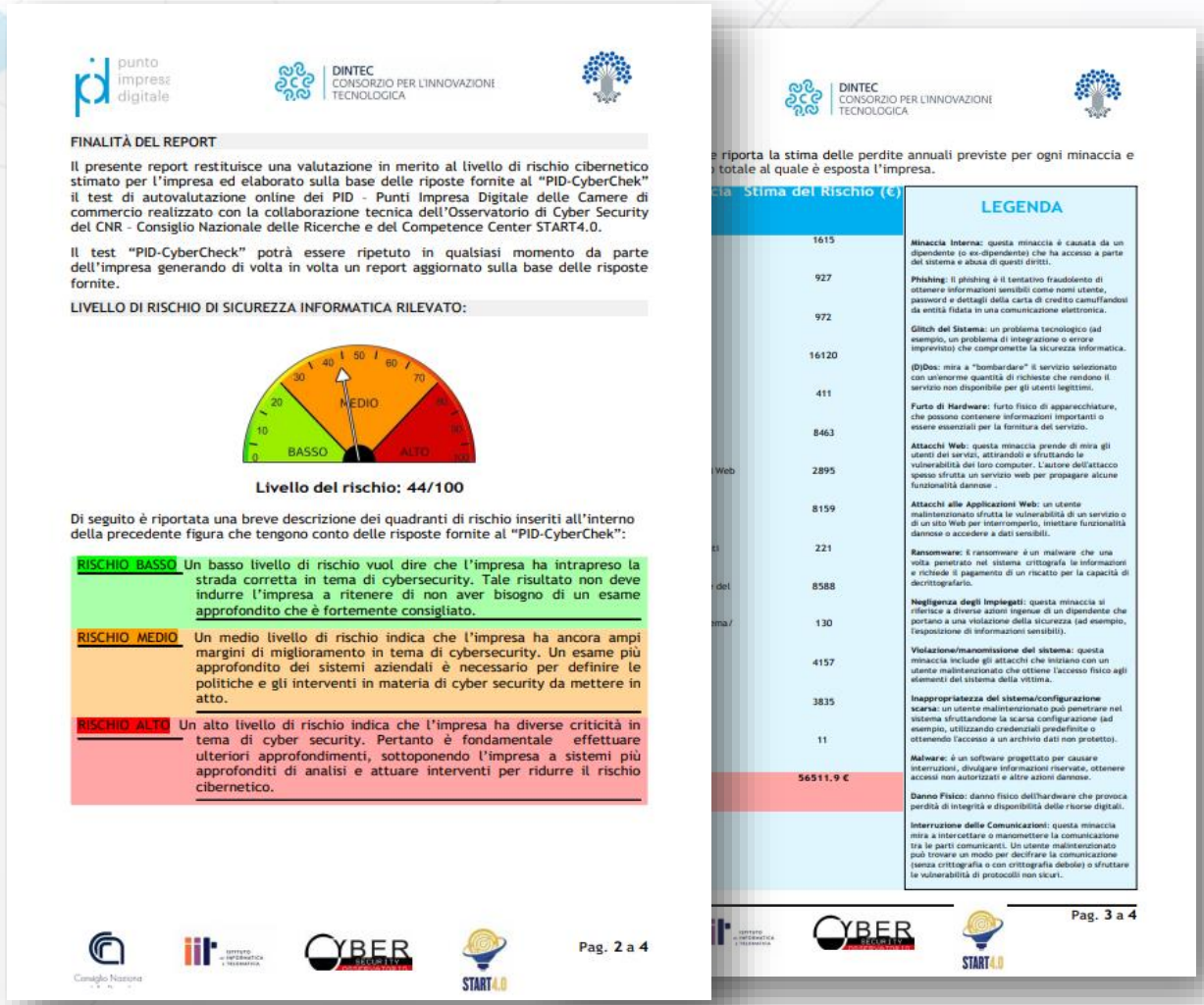
punto impresa digitale

REPORT FINALE

Al termine del questionario l'imprenditore riceve per email il **Report** che restituisce la valutazione in merito al **livello di rischio cibernetico stimato per l'impresa** e la **stima dei danni economici** subiti in caso di attacco.

Il livello di rischio potrà essere: **basso**, **medio** **o** **alto**.

Il PID-CyberCheck potrà poi essere ripetuto in qualsiasi momento generando di volta in volta un Report aggiornato.



punto impresa digitale

DINTEC
CONSORZIO PER L'INNOVAZIONE TECNOLOGICA

FINALITÀ DEL REPORT

Il presente report restituisce una valutazione in merito al livello di rischio cibernetico stimato per l'impresa ed elaborato sulla base delle riposte fornite al "PID-CyberChek" il test di autovalutazione online dei PID - Punti Impresa Digitale delle Camere di commercio realizzato con la collaborazione tecnica dell'Osservatorio di Cyber Security del CNR - Consiglio Nazionale delle Ricerche e del Competence Center START4.0.

Il test "PID-CyberCheck" potrà essere ripetuto in qualsiasi momento da parte dell'impresa generando di volta in volta un report aggiornato sulla base delle risposte fornite.

LIVELLO DI RISCHIO DI SICUREZZA INFORMATICA RILEVATO:

Livello del rischio: 44/100

Di seguito è riportata una breve descrizione dei quadranti di rischio inseriti all'interno della precedente figura che tengono conto delle risposte fornite al "PID-CyberChek":

RISCHIO BASSO	Un basso livello di rischio vuol dire che l'impresa ha intrapreso la strada corretta in tema di cybersecurity. Tale risultato non deve indurre l'impresa a ritenere di non aver bisogno di un esame approfondito che è fortemente consigliato.
RISCHIO MEDIO	Un medio livello di rischio indica che l'impresa ha ancora ampi margini di miglioramento in tema di cybersecurity. Un esame più approfondito dei sistemi aziendali è necessario per definire le politiche e gli interventi in materia di cyber security da mettere in atto.
RISCHIO ALTO	Un alto livello di rischio indica che l'impresa ha diverse criticità in tema di cyber security. Pertanto è fondamentale effettuare ulteriori approfondimenti, sottoponendo l'impresa a sistemi più approfonditi di analisi e attuare interventi per ridurre il rischio cibernetico.

Pag. 2 a 4

DINTEC
CONSORZIO PER L'INNOVAZIONE TECNOLOGICA

riporta la stima delle perdite annuali previste per ogni minaccia e totale al quale è esposta l'impresa.

Stima del Rischio (€)
1615
927
972
16120
411
8463
2895
8159
221
8588
130
4157
3835
11
56511.9 €

LEGENDA

Minaccia Interna: questa minaccia è causata da un dipendente (o ex-dipendente) che ha accesso a parte del sistema e abusa di questi diritti.

Phishing: il phishing è il tentativo fraudolento di ottenere informazioni sensibili come nomi utente, password e dettagli della carta di credito camuffandosi da entità fidata in una comunicazione elettronica.

Glitch del Sistema: un problema tecnologico (ad esempio, un problema di integrazione o errore imprevisto) che compromette la sicurezza informatica.

(D)Dos: mira a "bombardare" il servizio selezionato con un'enorme quantità di richieste che rendono il servizio non disponibile per gli utenti legittimi.

Furto di Hardware: furto fisico di apparecchiature, che possono contenere informazioni importanti o essere essenziali per la fornitura del servizio.

Attacchi Web: questa minaccia prende di mira gli utenti dei servizi, attirandoli e sfruttando le vulnerabilità del loro computer. L'autore dell'attacco spesso sfrutta un servizio web per propagare alcune funzionalità dannose .

Attacchi alle Applicazioni Web: un utente malintenzionato sfrutta le vulnerabilità di un servizio o di un sito Web per interromperlo, iniettare funzionalità dannose o accedere a dati sensibili.

Ransomware: il ransomware è un malware che una volta penetrato nel sistema crittografa le informazioni e richiede il pagamento di un riscatto per la capacità di decrittografarle.

Negligenza degli Impiegati: questa minaccia si riferisce a diverse azioni ingenue di un dipendente che portano a una violazione della sicurezza (ad esempio, l'esposizione di informazioni sensibili).

Violazione/manomissione del sistema: questa minaccia include gli attacchi che iniziano con un utente malintenzionato che ottiene l'accesso fisico agli elementi del sistema della vittima.

Inappropriatezza del sistema/configurazione scarsa: un utente malintenzionato può penetrare nel sistema sfruttandone la scarsa configurazione (ad esempio, utilizzando credenziali predefinite o ottenendo l'accesso a un archivio dati non protetto).

Malware: è un software progettato per causare interruzioni, divulgare informazioni riservate, ottenere accessi non autorizzati e altre azioni dannose.

Danno Fisico: danno fisico dell'hardware che provoca perdita di integrità e disponibilità delle risorse digitali.

Interruzione delle Comunicazioni: questa minaccia mira a intercettare o manomettere la comunicazione tra le parti comunicanti. Un utente malintenzionato può trovare un modo per decifrare la comunicazione (senza crittografia o con crittografia debole) o sfruttare le vulnerabilità di protocolli non sicuri.

Pag. 3 a 4

CAMERA DI COMMERCIO MAREMMA E TIRRENO

punto impresa digitale

L'INDICE DI ESPOSIZIONE CYBER (CEI)

CAMERA DI COMMERCIO
MAREMMA E TIRRENO

punto
impresa
digitale

CYBER EXPOSURE INDEX (CEI)

Il **Cyber Exposure Index (CEI)** è un indice che, a partire dal **sito web e dalla casella di posta elettronica aziendale**, misura lo spazio digitale di esposizione agli attacchi cyber di un'impresa attraverso la valutazione di tre fattori principali:

- Quantità dei **servizi esposti** su internet;
- Elenco delle **vulnerabilità** relative ai servizi esposti e sfruttabili dall'esterno;
- **Data leakage** o "fughe di dati" relative ad utenze e password legate all'azienda.

CHECKUP
Sicurezza IT
Cyber Exposure Index

CAMERA DI COMMERCIO MAREMMA E TIRRENO
punto impresa digitale

CEI – SERVIZI ESPOSTI

I servizi esposti sono i servizi accessibili da internet. Descrivono il perimetro, la superficie pubblicamente esposta dell'azienda sulla rete e comprendono una serie di strumenti come: siti web, portali di e-commerce, applicazioni web di gestione di ordini e di condivisione di informazioni con clienti e fornitori.

SUGGERIMENTO

Il quantitativo di servizi esposti non è un problema di per sé, deve essere però **minimizzato** a quanto effettivamente necessario al business aziendale, riducendo così la superficie attaccabile ed i sistemi da aggiornare e controllare.

L'esposizione di servizi su *Internet*, dovrebbe essere oggetto di censimento e la loro realizzazione e manutenzione dovrebbe seguire un **piano regolare di aggiornamento alle ultime versioni disponibili**.

CEI – VULNERABILITA'

Le **vulnerabilità** vengono identificate sul perimetro dei **servizi esposti rilevati** ed evidenziano, tramite una scansione «passiva» e non invasiva, le versioni dei servizi pubblicati dall'azienda che risultano avere delle vulnerabilità note, rispetto ad una **base dati** accessibile globalmente e continuamente aggiornata.

SUGGERIMENTO

L'indice di rischio viene calcolato sulla base della **gravità delle vulnerabilità note** che potrebbero presentare le versioni dei software rilevate ed esposte al pubblico.

Per ridurre questo indice, un'impresa dovrebbe **aggiornare i software vulnerabili**, dando precedenza a tutti i servizi esposti in rete.

CEI – FUGHE DI DATI

I **data leak** sono collezioni di informazioni (informazioni personali, password protette (hash), o addirittura password in chiaro), disponibili sulla rete, relative a persone e aziende. L'origine di queste collezioni di **dati esfiltrati** è riconducibile ad attacchi, perpetrati ai danni di diverse organizzazioni, che hanno permesso il furto da parte di criminali informatici, di informazioni gestite o di proprietà delle organizzazioni colpite.

SUGGERIMENTI

Il data leak va valutato in funzione della **tipologia di informazione rilevata** e, in caso riguardasse credenziali rubate o altri dati sensibili, andranno valutate le opportune contromisure, quali:

- Cambiare le credenziali esposte;
- Assicurarsi di non utilizzare la stessa password su diversi sistemi;
- Assicurarsi che la logica con cui è eventualmente stata costruita la password rubata, non sia utilizzata per le credenziali di altri servizi;
- Assicurarsi che gli account aziendali siano usati solo per finalità lavorative e per servizi legati al business aziendale.

CYBER EXPOSURE INDEX (CEI)

Le **tre diverse dimensioni** che indaga il CEI cercano di riassumere i **vari scenari di attacco** da parte di un attaccante esterno:

SERVIZI ESPOSTI

Più elevato è il numero di servizi raggiungibili su internet, più sistemi e tecniche può sfruttare un attaccante per ottenere un **accesso non autorizzato**.

VULNERABILITA'

Più potenziali vulnerabilità sono sfruttabili da un attaccante, più sarà facile **compromettere il sistema.**

FUGHE DI DATI

Più data leaks sono presenti, più facilmente l'attaccante sarà in grado di ottenere **informazioni sfruttabili per portare a termine un attacco**.

PERCHE' RICHIEDERLO?

L'indice consente di avere una visione dell'**impronta digitale** su internet dell'impresa, al momento in cui viene eseguito e con prospettiva esterna, ad esempio dal punto di vista degli attaccanti. Non va quindi inteso come un'analisi completa della postura di sicurezza, è invece un **ottimo punto di partenza per la valutazione di adeguate strategie di monitoraggio e controllo dell'infrastruttura informatica**, da approfondire e proseguire anche internamente. Inoltre:

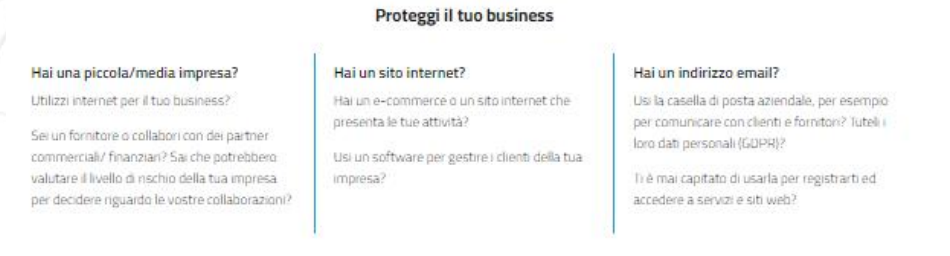
1. Strumento **semplice** ed **immediato**
3. Contiene **informazioni** che sono **già accessibili** dai cyber criminali ma anche da coloro che vogliono valutare il livello potenziale di rischio dell'impresa (es. clienti, banche)
4. Si basa su **tecnologie sofisticate** e su **fonti di altissimo valore (Threat intelligence)**
5. **Prezzo** contenuto grazie al contributo delle Camere di Commercio

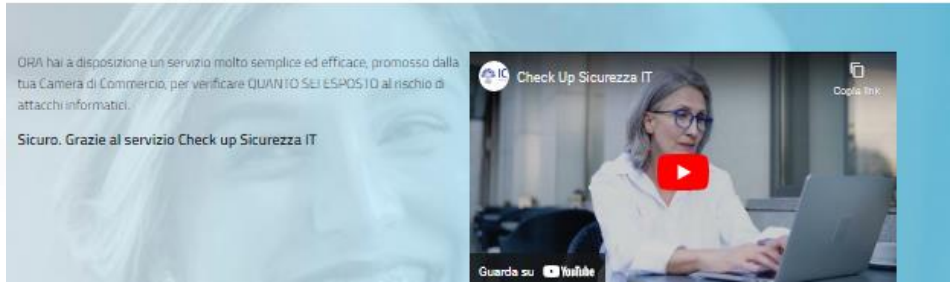
COME RICHIEDERLO?

Per richiedere il **Report CEI** occorre collegarsi a:

WWW.CYBERSECURITY-PMI.INFOCAMERE.IT

Cliccare su *Richiedi il servizio* e registrarsi





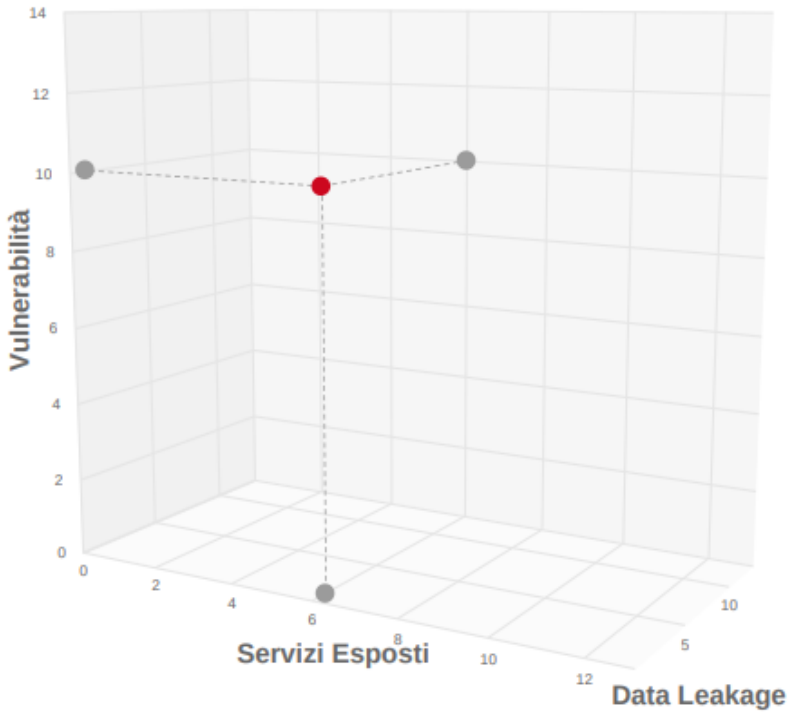
STRUTTURA DEL REPORT

A seguito della richiesta, un pool di esperti conduce l'indagine sulle tre dimensioni che caratterizzano il CEI ed elabora il **Report CEI** il quale si struttura in tre parti:

1. La **parte introduttiva**, in cui vengono spiegati i contenuti e le metodologie di elaborazione delle componenti dell'indice;

2. Il corpo del report che contiene l'**indice** e il **rating** calcolato per ciascuna delle sue componenti, con alcune indicazioni utili per l'azienda;

3. La parte conclusiva che dettaglia tutti gli elementi tecnicamente valutati nell'elaborazione delle tre componenti. Sono **contenuti** molto **tecnici**, utili al personale tecnico di riferimento per l'azienda in analisi.

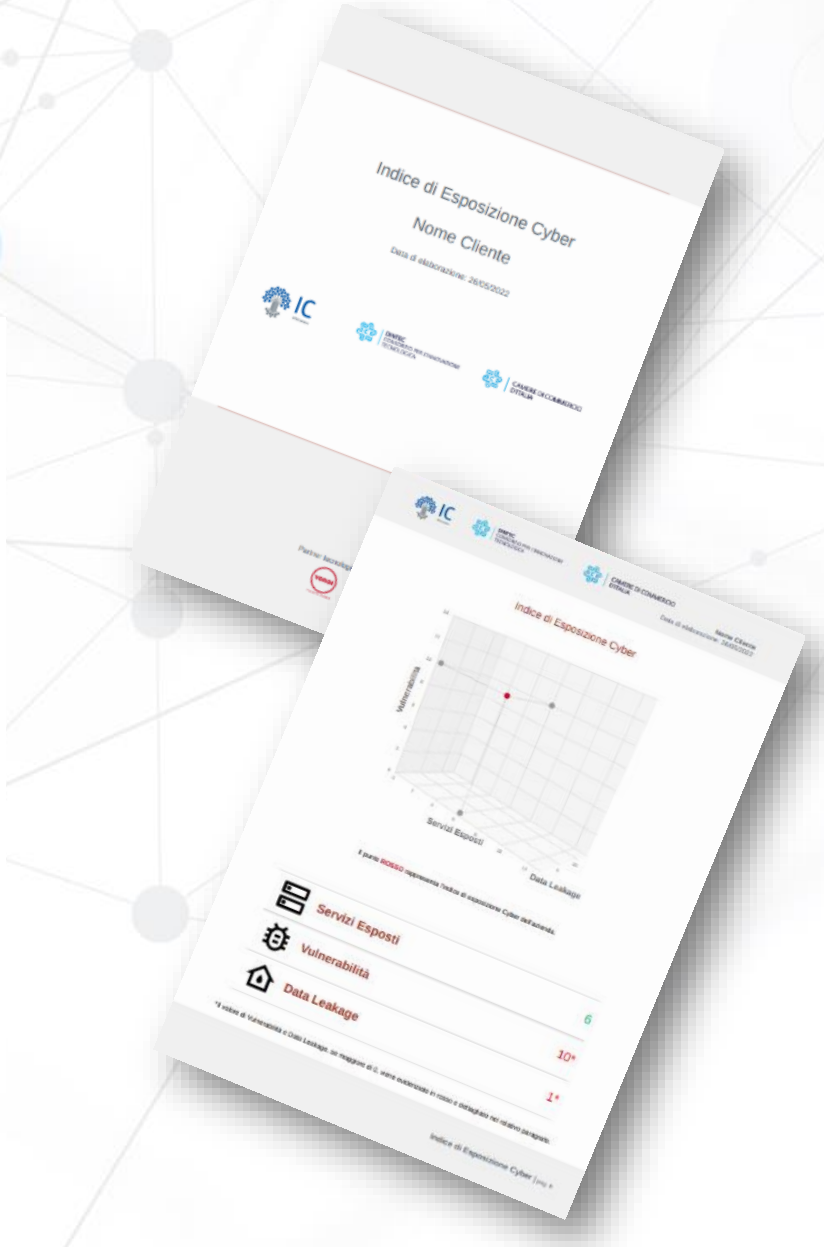


CONSEGNA DEL REPORT

Il **Report CEI** viene consegnato all'impresa dal Digital Promoter dell'Ente in un incontro *one to one* in cui viene fornita una **spiegazione dei risultati**.

Grazie a questo incontro l'imprenditore potrà capire il grado di rischio ed eventualmente porre in atto delle misure di difesa.

Aderendo a questo servizio l'imprenditore avrà diritto alla realizzazione e consegna di un **secondo report** ad una distanza massima di sei mesi dal primo, senza costi aggiuntivi.



CAMERA DI COMMERCIO MAREMMA E TIRRENO

punto impresa digitale

GLI ALTRI SERVIZI DEL PID IN BREVE

CAMERA DI COMMERCIO
MAREMMA E TIRRENO

punto
impresa
digitale

I SERVIZI DEL PID MAREMMA E TIRRENO

FORMAZIONE

- PERCORSO FORMATIVO - DIGITALIZZAZIONE DI BASE
- PERCORSO FORMATIVO - TECNOLOGIE 4.0

CREARE CONSAPEVOLEZZA NELLE IMPRESE

- ASSESSMENT DELLA MATURITA' DIGITALE DELLE IMPRESE
- ASSESSMENT DELLE COMPETENZE DIGITALI
- ASSESSMENT SICUREZZA INFORMATICA

ACCOMPAGNARE ED AIUTARE LE IMPRESE

- ORIENTAMENTO E INDIRIZZAMENTO VERSO IL NETWORK i4.0
- POSSIBILITA' DI OSPITARE IN STAGE UN ESPERTO DIGITALE

SOSTENERE GLI INVESTIMENTI TECNOLOGICI

- BANDO A SOSTEGNO DELLA DIGITALIZZAZIONE

SELFI4.0

ZOOM4.0

DIGITAL SKILL voyager
viaggio nelle competenze digitali

UNIONCAMERE Google

Crescere in Digitale

CAMERA DI COMMERCIO MAREMMA E TIRRENO

punto impresa digitale

IL PROSSIMO APPUNTAMENTO

17 OTTOBRE
ORE 11

- SERVIZI DIGITALI
- SERVIZI DEL PID
- BANDO PER L'EROGAZIONE DI CONTIRBUTI A SOSTEGNO DELLA DIGITALIZZAZIONE

Grazie per l'attenzione!

pid@lg.camcom.it
www.lg.camcom.it

Digital Promoter - Elisabetta Scaturro: 0586 231 262

IL TEAM PID MAREMMA E TIRRENO

Seguici su:

CAMERA DI COMMERCIO
MAREMMA E TIRRENO

punto
impresa
digitale