WELCOME TO OUR COMPANY

CYBERSECURITY AND PRIVACY

CYBERSECURITY

La cybersecurity, ovvero, **protezione fisica e virtuale degli asset aziendali è un'insieme di processi, procedure e soluzioni tecnologiche in grado di proteggere la tua rete** e i tuoi sistemi critici dagli attacchi digitali.

Con l'aumento esponenziale **dei dati e del numero** di persone che lavorano e si connettono ovunque, gli hacker hanno **sviluppato metodi sofisticati e nuove tecniche per ottenere l'accesso alle risorse,** rubare i dati, eludere i sistemi di rilevamento, sabotare le aziende.

Ogni anno il numero di attacchi aumenta!

Un **programma di cybersecurity efficace include persone, processi e soluzioni tecnologiche** che, insieme, riducono **il rischio di interruzioni dell'attività, perdite finanziarie e danni di immagine dovuti a un attacco.**

ATTACCHI CYBER IN AUMENTO: I NUMERI

Il Rapporto Clusit 2023 (uscito a marzo 2023), non lascia dubbi: è necessario attivare le giuste misure difensive.
Nel 2022 si sono registrati più attacchi cyber, con un **aumento del 21% nel mondo rispetto all'anno precedente**

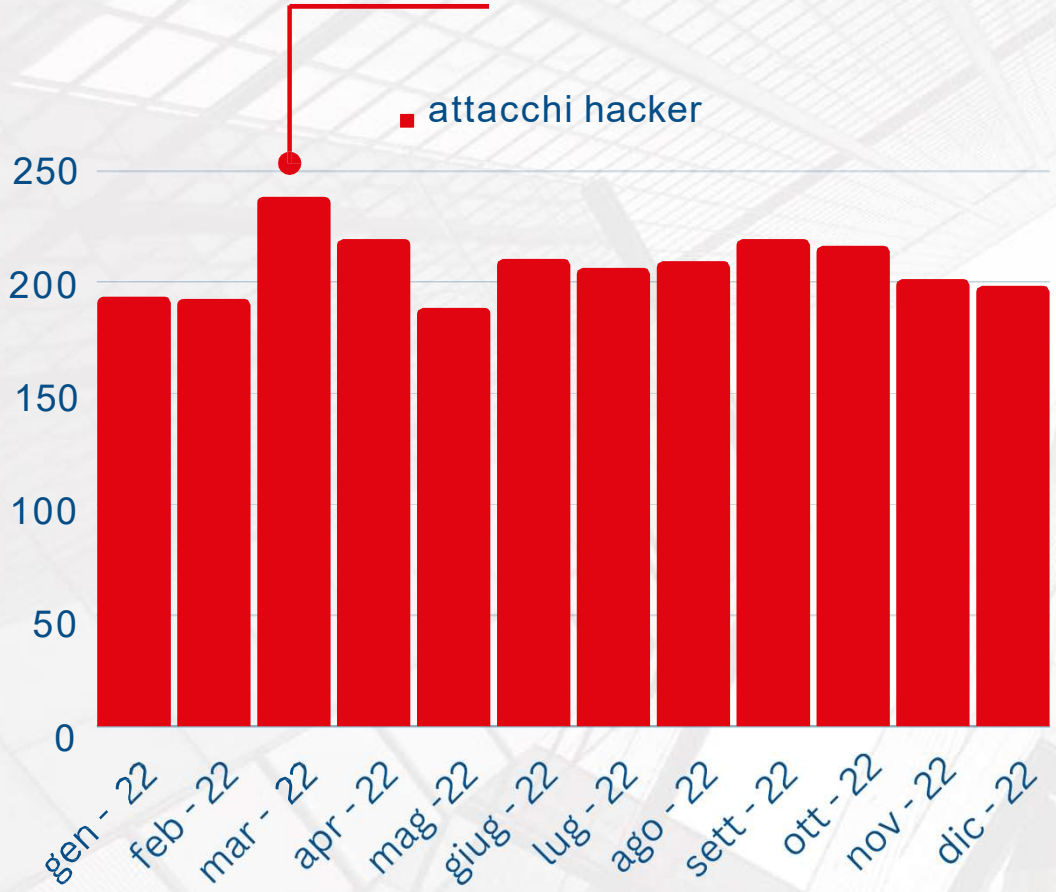
I dati principali:

- A livello planetario, sono stati registrati **2.489 attacchi gravi nel 2022 (+21% rispetto al 2021)**
- Media mensile di attacchi: **207** (picco a marzo legato al conflitto Russo-Ucraino - molti ricercatori definiscono come "guerra cibernetica diffusa")
- Per quanto riguarda l'**Italia**, sono 188 gli attacchi andati a segno, registrando un **+169% rispetto all'anno precedente**
- L'**Italia riceve il 7,6% degli attacchi globali**, dato ben superiore rispetto al 3,4% registrato nell'anno prima.
- L'**83% dei 188 attacchi andati a segno** hanno portato a **conseguenze di gravità elevata o critica.**

Fonte: Rapporto Clusit 2023 per la cyber security

I NUMERI

Il picco di Marzo e Aprile è in corrispondenza dell'inizio delle ostilità tra Russia e Ucraina.



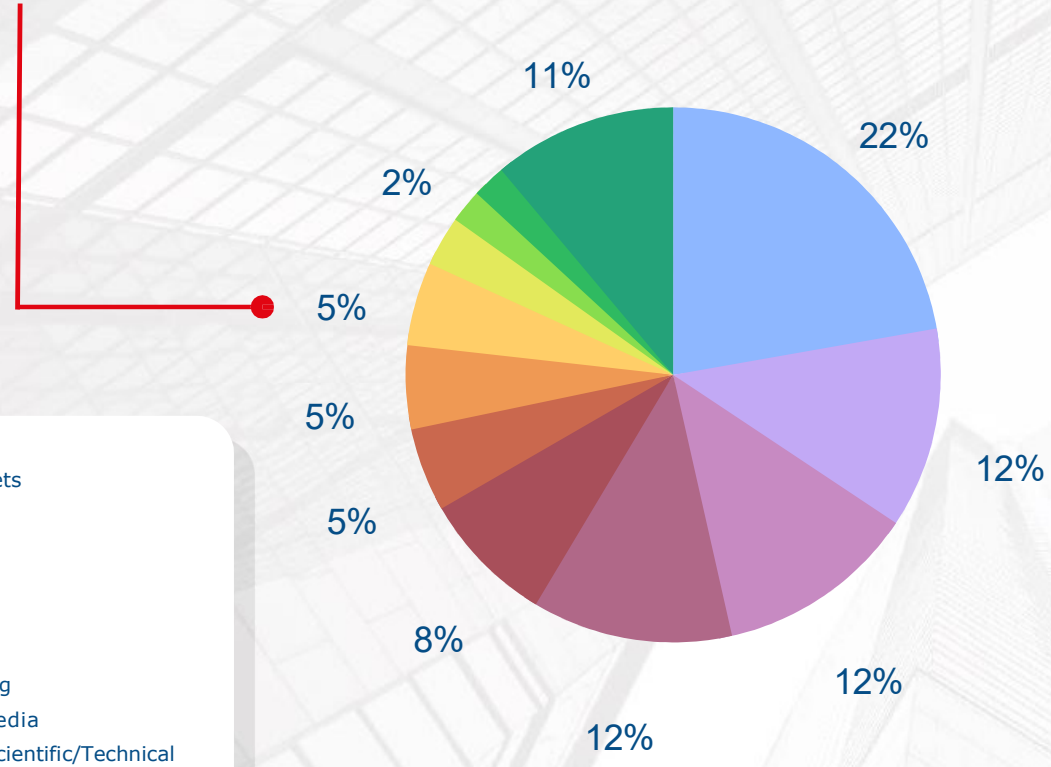
Gli **obiettivi** alla base degli attacchi hacker analizzati sono:

- Cybercrime (82% che sale al 93% in Italia)
- Spionaggio e sabotaggio (11%)
- Information warfare (4%)
- Attivismo (3%)

238

***Il numero degli attacchi** registrati a marzo,
rappresentano il record assoluto registrato fino ad ora

LE VITTIME



I settori più attaccati **in Italia** sono:

- **Settore governativo**

20%

- **Manifatturiero**

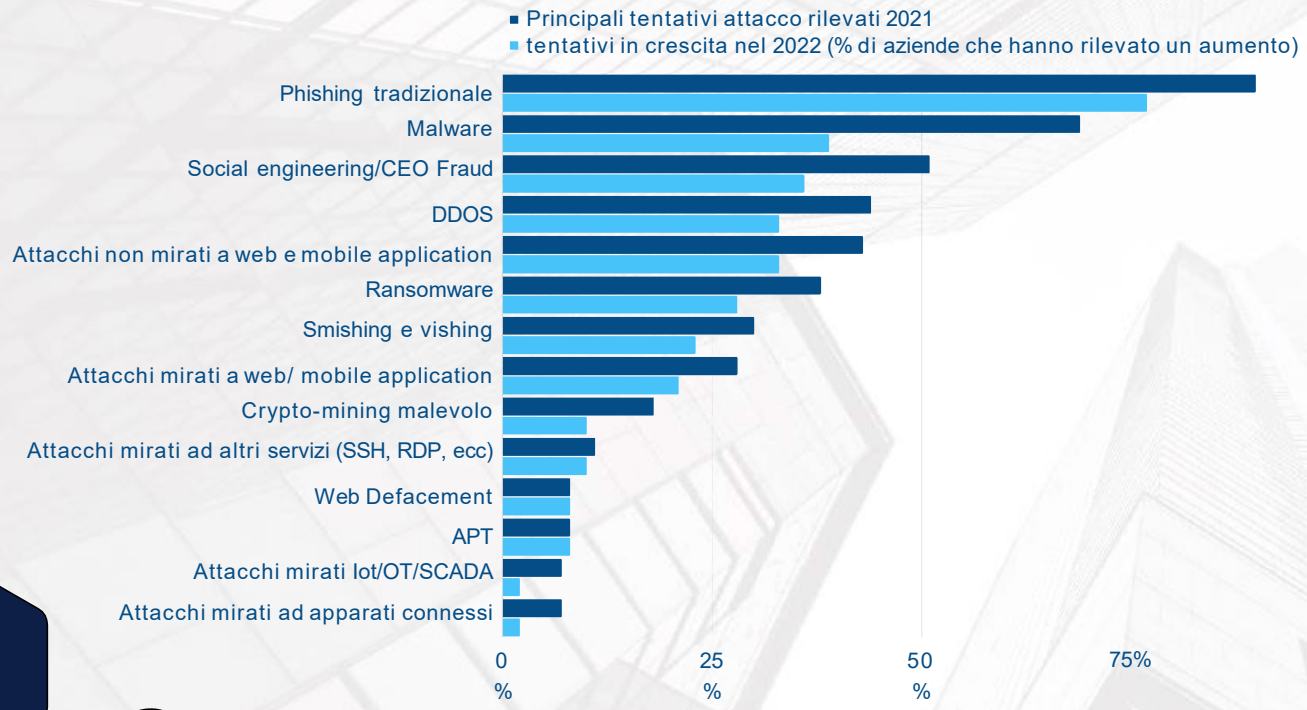
19%

188

*Gli attacchi andati a segno in Italia registrando un **+169% rispetto all'anno precedente.**

Fonte: Rapporto Clusit 2023 per la cyber security

QUALI I PRINCIPALI ATTACCHI NEL MONDO



Le **tecniche di attacco** più utilizzate dai cybercriminali sono:

- **Phishing/Social Engineering** (77%)
- **Malware (in Italia rappresenta il 36% degli attacchi,** mentre nel resto del mondo la percentuale è molto più bassa)
- DDos (39%)
- Sfruttamento delle vulnerabilità
- Furto d'identità/credenziali

Fonte Barometro Cybersecurity, NetConsulting cube, 2023

URGENTE LA GOVERNANCE DELLA CYBERSECURITY

Recita il rapporto CLUSIT:

"Le minacce informatiche continueranno a rappresentare una sfida per la sicurezza [...], le organizzazioni dovranno continuare a investire in ***tecnologie di sicurezza avanzate*** *e in* ***programmi di formazione****".*

Viste le tante conseguenze degli attacchi alla sicurezza – interruzione del servizio, danneggiamento di impianti e asset, riduzione nei livelli di produttività, perdita di dati e informazioni, danno reputazionale, calo delle performance – aziende ed enti devono essere impegnate a mettere in atto azioni strategiche volte a mitigare gli impatti delle minacce.

Diventa quindi sempre più critico indirizzare le tematiche di cybersecurity da un punto di vista strategico e organizzativo prevedendo formazione, persone, processi e soluzioni tecnologiche.

DA DOVE PARTIRE?

Definire **cosa abbiamo di prezioso** da proteggere sul Cyberspazio

Misurare la sicurezza informatica implica l'identificazione, la valutazione e il monitoraggio di vari aspetti della sicurezza per garantire che le risorse digitali siano protette in modo efficace e che le politiche aziendali siano rispettate.

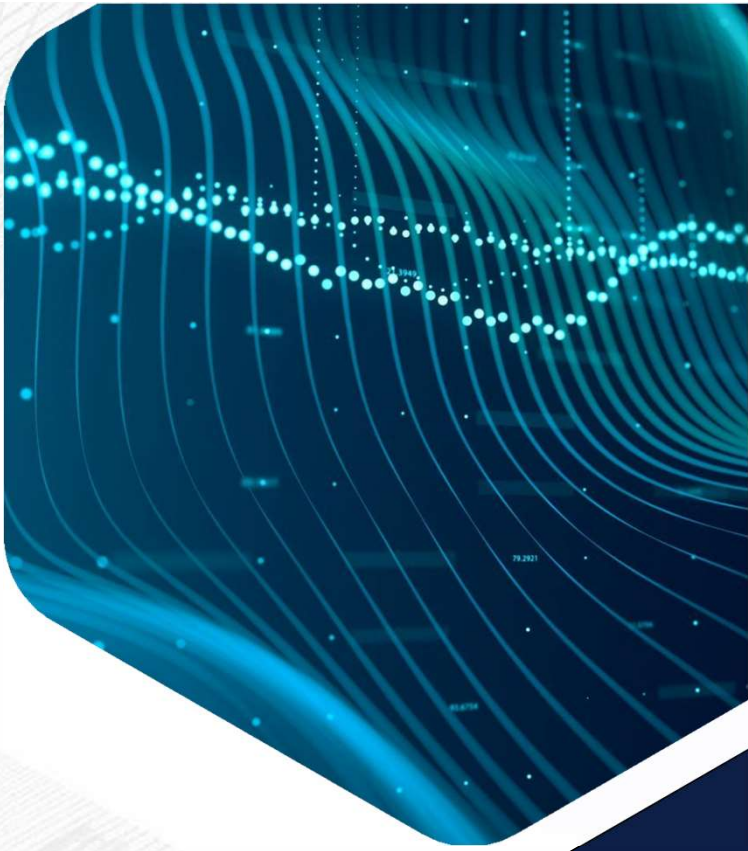
Individuare le principali Minacce a cui siamo esposti (Sicurezza e compliance)

DA DOVE PARTIRE?

Avere chiara **la nostra Propensione al Rischio**

Individuare le soluzioni migliori in termini di rapporto costo-beneficio per le nostre esigenze (prodotti e servizi di sicurezza)

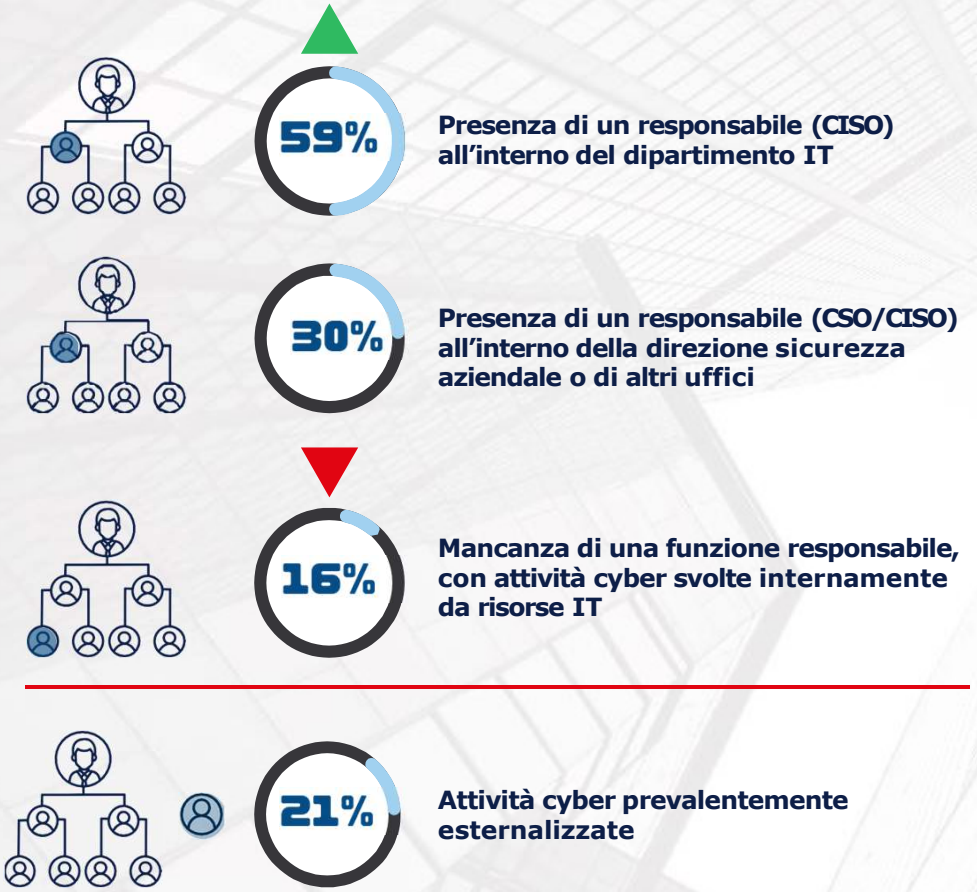
Investire molto sulla Consapevolezza dei nostri dipendenti (qualsiasi strumento implementeremo sarà inutile se non usato correttamente)



GLI ELEMENTI CHIAVE DELLA STRATEGIA

Attualmente com è organizzata la vostra azienda per la governance e la gestione della cybersecurity?

Valori %, risposte multiple



PROCEDURE CONSIGLIATE DI CYBERSECURITY: Chief Information Security Officer

Il "Chief Information Security Officer (CISO)" è un ruolo chiave per la gestione dei rischi di sicurezza informatica in un'organizzazione.
Il CISO agisce come un architetto, sviluppando e allineando le misure tecniche per affrontare i rischi e raggiungere gli obiettivi ell'organizzazione.

Cresce, infatti, la quota di aziende che ha dichiarato di aver nominato un Ciso, all'interno della divisione IT, con responsabilità della governance e della gestione delle tematiche di sicurezza.

Fonte Barometro Cybersecurity, NetConsulting cube, 2023

PROCEDURE CONSIGLIATE DI CYBERSECURITY

L'Identity and Access Management (IAM)

è fondamentale per garantire l'accesso appropriato alle risorse al momento giusto.

Cryptographic Standards and Validation

comprende operazioni come la creazione di chiavi e firme digitali, specifiche e processi per garantire la sicurezza e l'affidabilità di sistemi informatici e dati.

Formazione

È importante implementare un programma di formazione sulla sicurezza informatica per aumentare la consapevolezza e la comprensione dei vantaggi della gestione del rischio informatico e della mitigazione delle vulnerabilità a tutti i livelli.

Piattaforme Affidabili

Richiede tecnologie di sicurezza e privacy per proteggere utenti e dati, compresa la crittografia.

PROCEDURE CONSIGLIATE DI CYBERSECURITY

Ingegneria della privacy

Definita da NIST come una specialità che fornisce linee guida per ridurre i rischi legati alla privacy e prendere decisioni informate sull'allocazione delle risorse e il controllo dei sistemi informativi

Gestione integrata del rischio aziendale (ERM)

La gestione integrata del rischio aziendale (ERM) è un approccio sistemico che considera aspetti finanziari e non finanziari e Permette di identificare, valutare e gestire il rischio.

Reti Affidabili

promuovere ricerca, standardizzazione e adozione di tecnologie per migliorare sicurezza, privacy, robustezza e prestazioni dei sistemi di rete.

LE NOSTRE SOLUZIONI

SERVIZI

As-a-Service" (AaS) è un acronimo originato con il cloud computing, inizialmente con Software-as-a-Service (SaaS). Security as a Service permette di integrare servizi di protezione da attacchi informatici nell'infrastruttura aziendale tramite abbonamenti.

- **Ciso as a Service**
- **Vulnerability Assessment Service**
- **Cyber Security as a Service**
- **Digital Transformation as a Service**
- **Disaster Recovery as a Service**
- **Virtual Desktop Infrastructure as a Service**

CISO AS A SERVICE (CISOaaS)

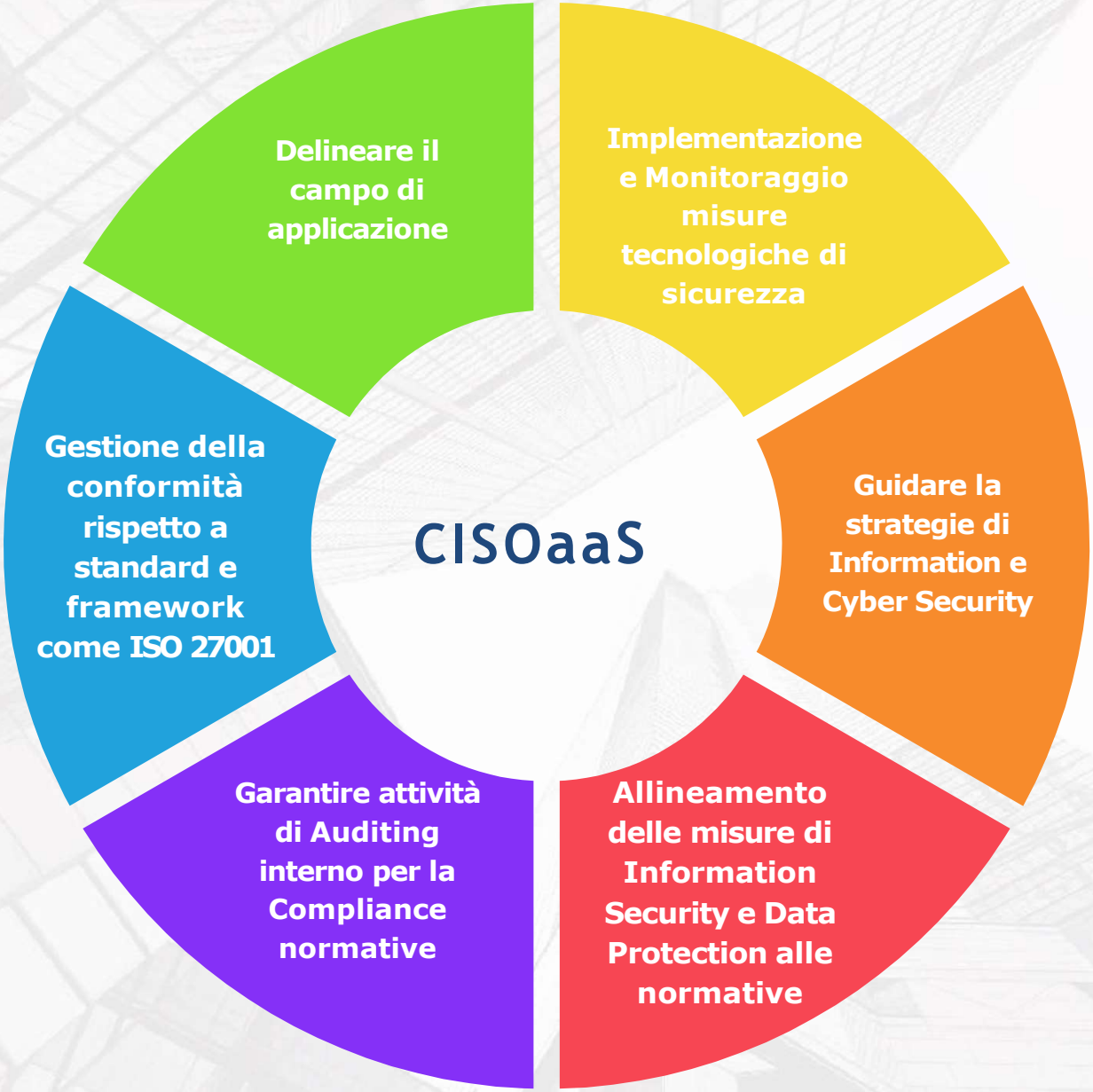
What

Il CISO è il responsabile della sicurezza informatica in azienda, definisce la visione strategica e implementa programmi per proteggere gli asset informativi e limitare i rischi legati alle tecnologie digitali.

Vantaggi

- ***Assesment della sicurezza***, gestione e supervisione
- Definizione delle policy politiche e procedure di sicurezza informatica
- **Analisi del cyber rischio** e definizione delle architetture
- Identificazione delle minacce
- Monitoraggio della sicurezza e **adozione di misure preventive**
- Risposta agli incidenti coordinando le indagini, le attività e limitando i danni
- Promuove una **cultura di sicurezza** all'interno dell'azienda, migliora la consapevolezza
- Ottimizzazione le risorse indirizzandole in modo efficiente
- Adozione di nuove tecnologie in funzione delle nuove minacce e delle tecnologie emergenti

LE NOSTRE SOLUZIONI



VULNERABILITY ASSESSMENT as a Service (VAaaS)

What

Il VA ha lo scopo di **valutare la sicurezza del sistema informativo aziendale** e di **individuare vulnerabilità** per adottare le contromisure necessarie.

Vantaggi:

- **Aumento della consapevolezza** sulla sicurezza.
- **Riduzione del rischio** a livelli minimi.
- Continuità operativa garantita con una solida politica di prevenzione.
- **Conformità Normativa** e ai requisiti di sicurezza
- **Rapporto Dettagliato delle vulnerabilità** scoperte, consentendo all'azienda di prendere decisioni
- Protezione della reputazione aziendale essenziale, poiché danni all'immagine sono difficili da recuperare.
- La fiducia dei clienti è fortemente influenzata dalla reputazione aziendale
- **Risparmio a Lungo Termine** prevenendo costi significativi associati a incidenti di sicurezza

LE NOSTRE SOLUZIONI

CYBERSECURITY as a Service (CSaaS)

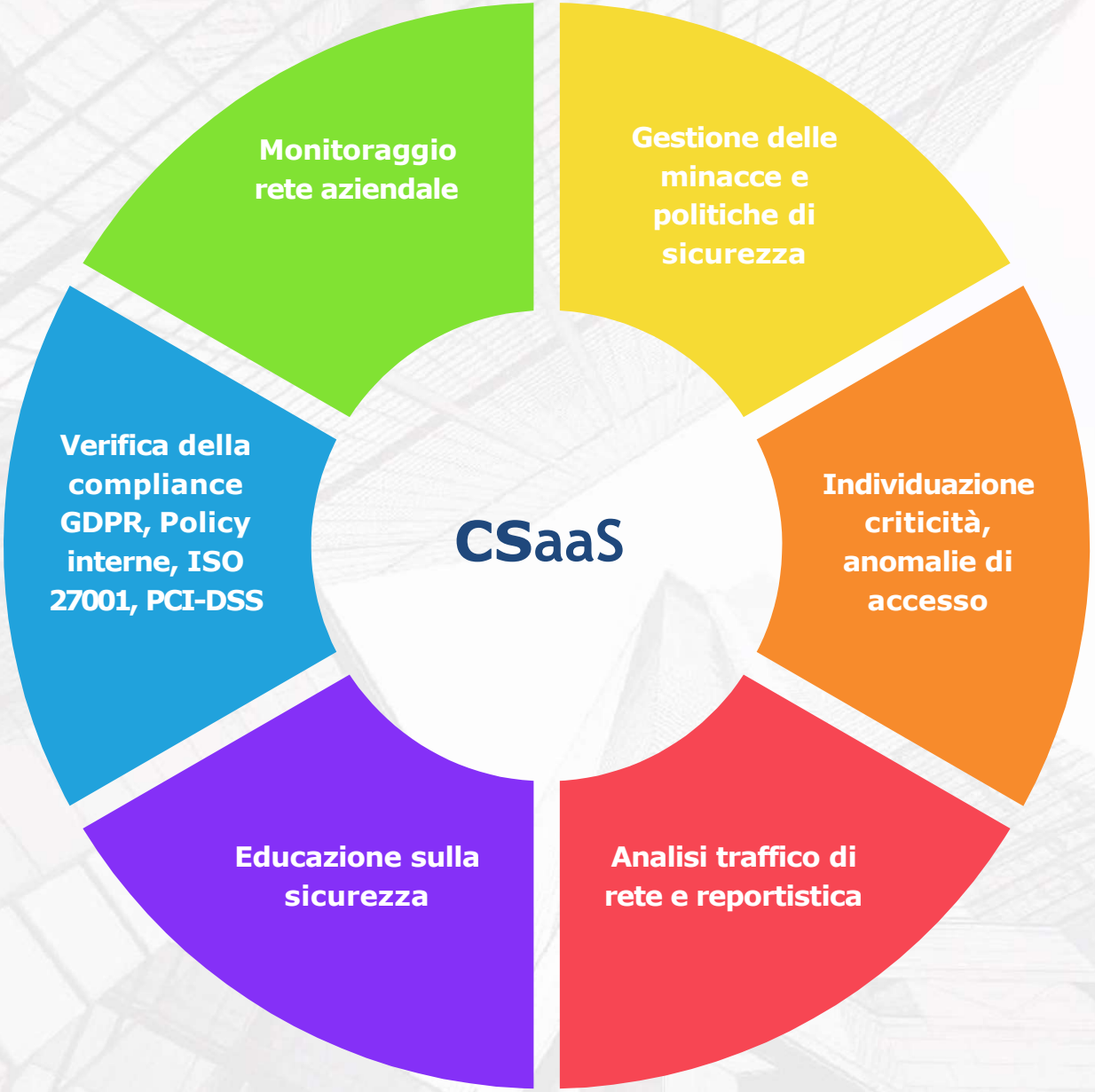
What

La sicurezza informatica è importante per le imprese e richiede risorse specifiche. La cyber security as a service permette all'azienda di concentrarsi sul core business mentre i professionisti gestiscono la protezione dei dati e delle risorse.

Vantaggi

- **Accesso a esperti e professionisti** in sicurezza informatica
- **Risposta aggiornata alle minacce** monitorando costantemente le minacce emergenti e aggiornano le difese
- **Costi flessibili** in base alle proprie esigenze e budget.
- **Risorse scalabili** adattando le risorse di sicurezza informatica in modo rapido ed efficiente.
- **Riduzione dell'Onere** amministrativo e della manutenzione dei sistemi di sicurezza
- **Conformità Normativa**
- **Monitoraggio Costante**
- **Riduzione del Rischio** di violazioni e perdite di dati.
- **Risposta rapida** alle minacce
- **Miglioramento della sicurezza complessiva**
- **Flessibilità e agilità** per adattarsi alle mutevoli esigenze di sicurezza in modo rapido.

LE NOSTRE SOLUZIONI



DIGITAL TRANSFORMATION as a Service (DTaaS)

What

La Digital Transformation richiede una ristrutturazione organizzativa e **l'adozione di soluzioni digitali offrendo** vantaggi in termini di efficienza aziendale. Richiede competenze specifiche per adattarsi al cambiamento tecnologico.

Vantaggi

- **Accesso a competenze specializzate** senza la necessità di assumere personale aggiuntivo.
- **Riduzione dei costi** consentendo alle aziende di gestire i costi in modo più efficiente.
- **Rapida implementazione** accelerando il processo di trasformazione e consentendo di rimanere competitivi sul mercato.
- **Personalizzazione del servizio** rispetto alle esigenze dell'organizzazione
- **Accesso alle ultime tecnologie** e best practice, garantendo che l'azienda rimanga all'avanguardia.
- **Miglioramento della Customer Experience** attraverso l'implementazione di nuove tecnologie e soluzioni.
- **Innovazione continua**
- **Miglioramento dell'efficienza operativa e l'ottimizzazione dei processi e dei flussi di lavoro**

LE NOSTRE SOLUZIONI

DISASTER RECOVERY as a Service (DRAaS)

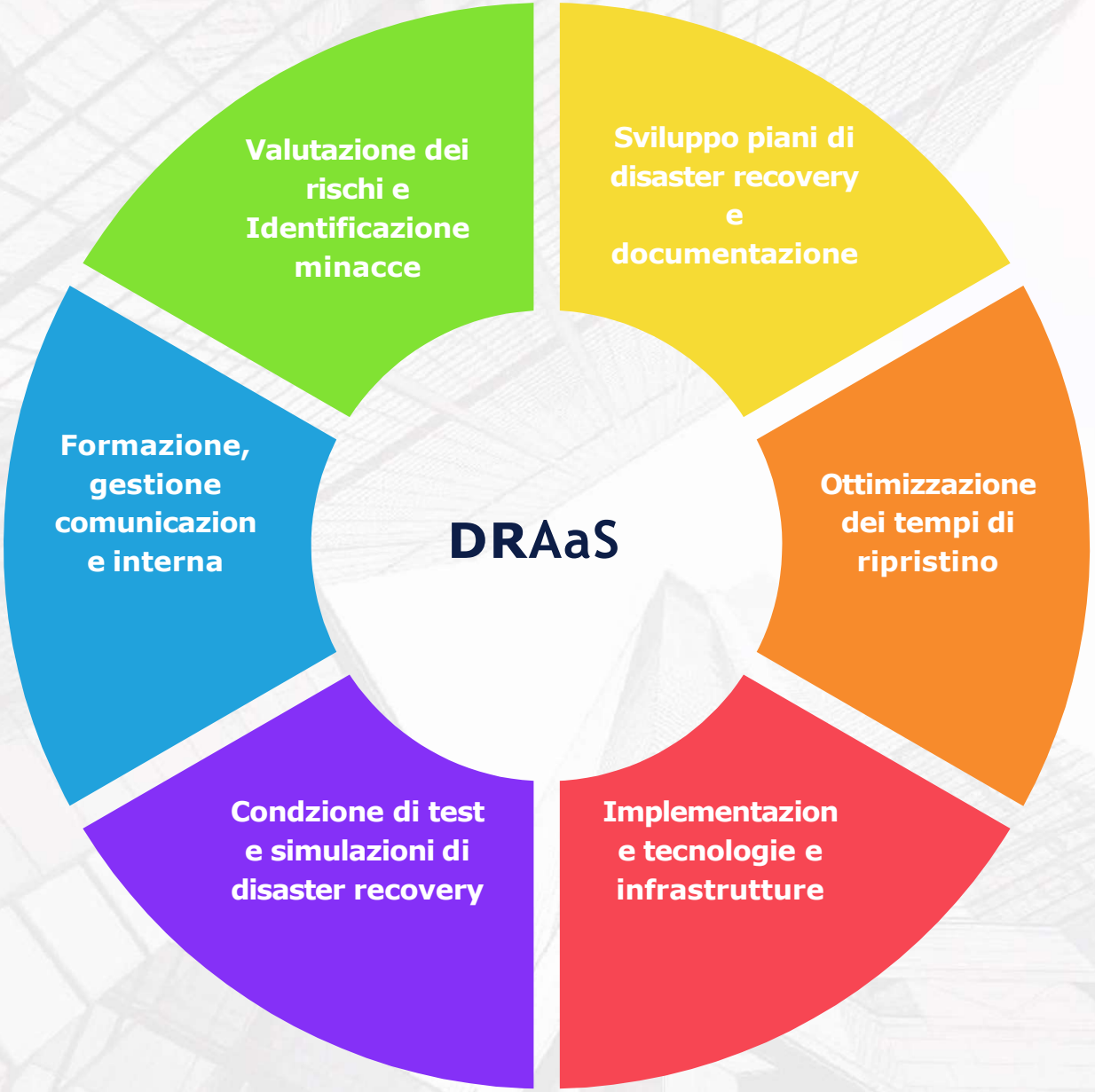
What

Disaster Recovery (DR) protegge dati e applicazioni da interruzioni dovute a varie cause, come calamità naturali e attacchi informatici che causano perdite economiche e danni d'immagine. Il servizio **Disaster Recovery as a Service (DRaaS),** basato su cloud, con un buon equilibrio tra **Recovery Point Objective (RPO) e Recovery Time Objective (RTO), è la soluzione.**

Vantaggi

- **Riduzione dei Downtime** consentendo un ripristino rapido
- **Risparmio sui costi** eliminando la necessità di investire in infrastrutture di disaster recovery
- **Pianificazione delle continuità operativa** garantendo la ripresa delle attività in tempi brevi.
- **Risposta Rapida alle emergenze** e alle minacce,
- **Accesso a expertise** specializzate in tema di sicurezza
- **Riduzione del rischio** di perdite di dati e di interruzioni delle attività
- **Conservazione dei dati** con soluzioni di backup garantendo che i dati siano disponibili
- **Facilità di gestione** consentendo all'azienda di concentrarsi sulle attività principali
- **Pianificazione anticipata** delle situazioni di emergenza, riducendo l'impatto di eventi inattesi

LE NOSTRE SOLUZIONI



VIRTUAL DESKTOP INFRASTRUCTURE as a Service (VDIaaS)

What

L'infrastruttura VDI (Virtual Desktop Infrastructure) consente **l'accesso a sistemi aziendali da vari dispositivi,** evitando la gestione di computer fisici. La VDI esegue carichi di lavoro desktop su server centralizzati ed è ampiamente utilizzata per supportare il lavoro remoto, nelle filiali e per l'accesso a terze parti.

Vantaggi

- **Accesso da qualsiasi luogo** e dispositivo connesso a Internet ai propri desktop
- **Riduzione dei cost**i hardware consentendo all'azienda di risparmiare sui costi di capitale.
- **Agilità e scalabilità** consentendo di espandere o ridurre le risorse in base alle necessità.
- **Massimi livelli di sicurezza** perché i dati sono ospitati in data center sicuri
- **Ideale per lavoratori in smartworking** come supporto
- **Riduzione del rischio** di perdita dei dati con backup pianificabile
- **Facilità di aggiornamenti software** che possono essere effettuati centralmente

LE NOSTRE SOLUZIONI

CONTACT US

+39 347 176 1331

m.lasorsa@pcsoftware.it

Via Pasubio 35, 70125 Bari

www.pcsoftware.doud

THANK YOU