
Quills

Quills

Quills è il nostro servizio per la cybersecurity

NEXiD è una **digital company** che accompagna le aziende nei processi di **trasformazione digitale**, from vision to execution.

Quills è un servizio modulare di Nexid che aiuta le organizzazioni a definire e gestire efficacemente le strategie di mitigazione dei rischi associati all'uso delle tecnologie dell'informazione, garantendo la conformità con normative, regolamenti e standard del settore.

NEXiD

Digital Xperiences

Quills

Perché la cybersecurity è fondamentale?

La sicurezza informatica o cybersecurity, riguarda **la difesa di reti, sistemi e software dagli attacchi digitali.** Questi attacchi mirano ad accedere, modificare o distruggere informazioni sensibili, estorcere denaro agli utenti o interrompere i processi aziendali normali.

Implementando misure di sicurezza robuste, la cybersecurity **aiuta a proteggere i dati contro le minacce esterne, garantendo la confidenzialità, l'integrità e la disponibilità delle informazioni**.

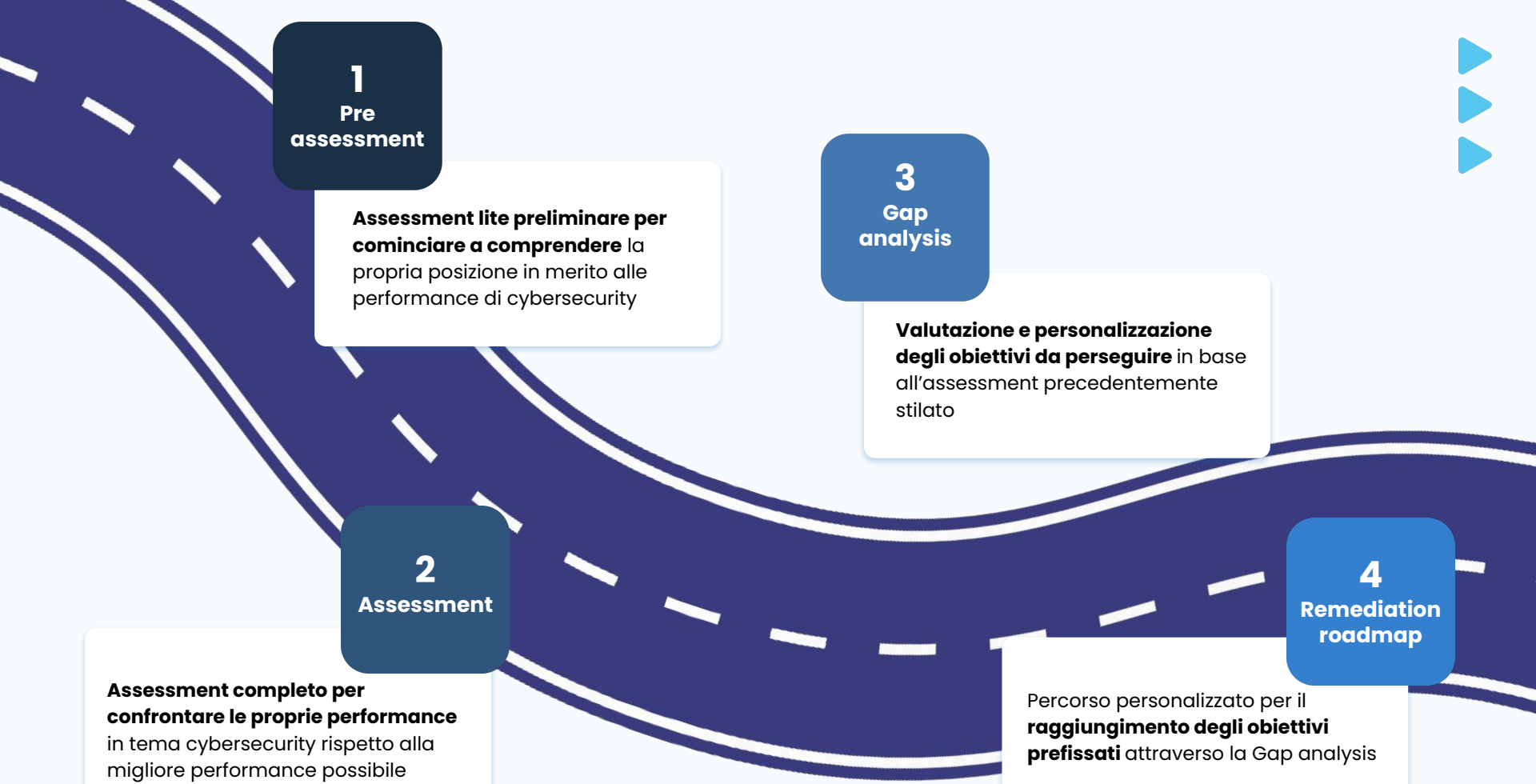
Quills

Come lo facciamo?

Attraverso il nostro questionario di pre-assessment **gratuito e senza impegno**, potrai cominciare a comprendere le tue performance nell'ambito della cybersecurity.

Successivamente su richiesta sarà possibile effettuare un vero e proprio **assessment di rischio**, che copre tutte le tematiche necessarie al raggiungimento della conformità con i principali **framework di settore** (ISO 27001, ISO 22301, NIST, COBIT, ITIL).

Verrà quindi stilata una **Remediation Roadmap su misura del cliente**, con una dettagliata pianificazione delle best practices da implementare suddivise per ambito.



1 Pre assessment

Assessment lite preliminare per cominciare a comprendere la propria posizione in merito alle performance di cybersecurity

2 Assessment

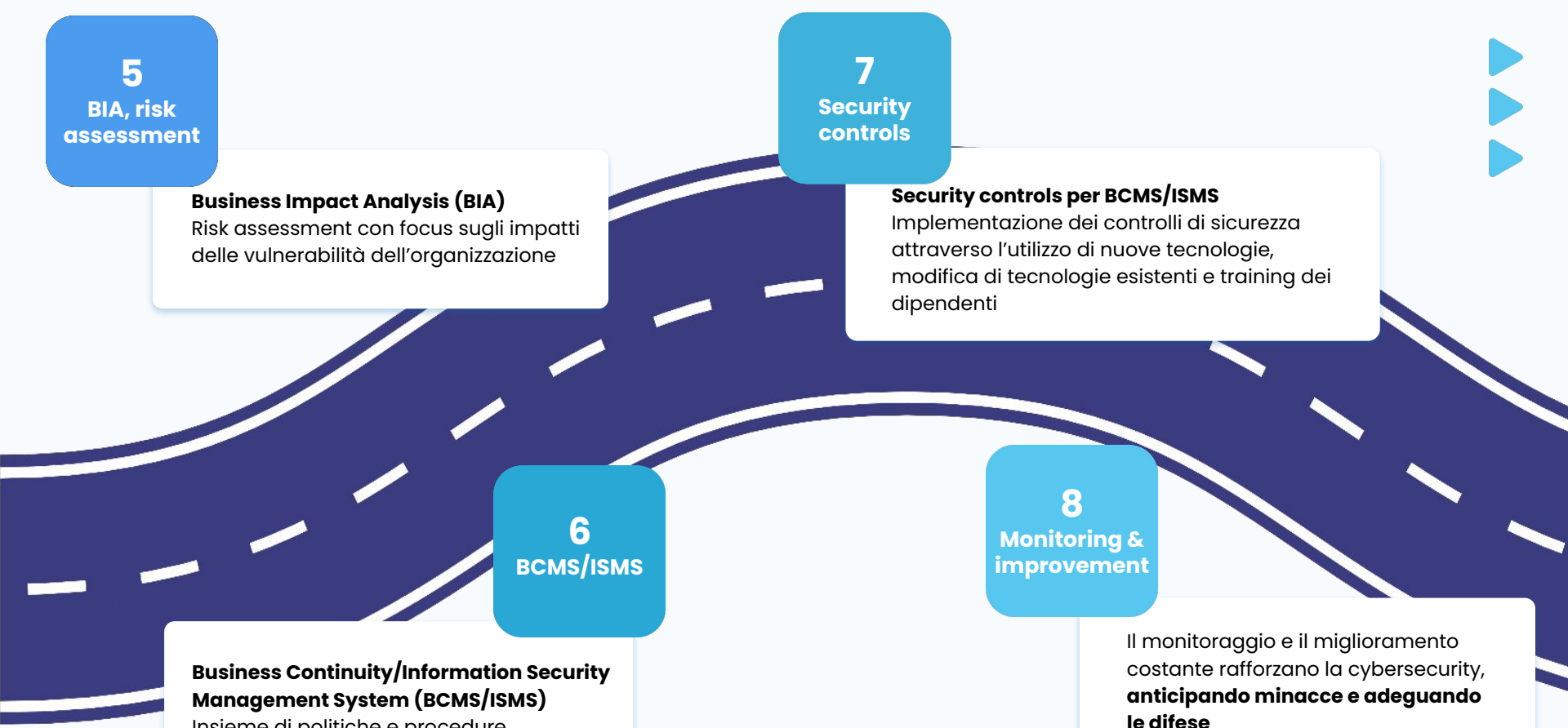
Assessment completo per confrontare le proprie performance in tema cybersecurity rispetto alla migliore performance possibile

3 Gap analysis

Valutazione e personalizzazione degli obiettivi da perseguire in base all'assessment precedentemente stilato

4 Remediation roadmap

Percorso personalizzato per il **raggiungimento degli obiettivi prefissati** attraverso la Gap analysis



5
BIA, risk assessment

Business Impact Analysis (BIA)
Risk assessment con focus sugli impatti delle vulnerabilità dell'organizzazione

6
BCMS/ISMS

Business Continuity/Information Security Management System (BCMS/ISMS)
Insieme di politiche e procedure necessarie per mitigare i rischi identificati

7
Security controls

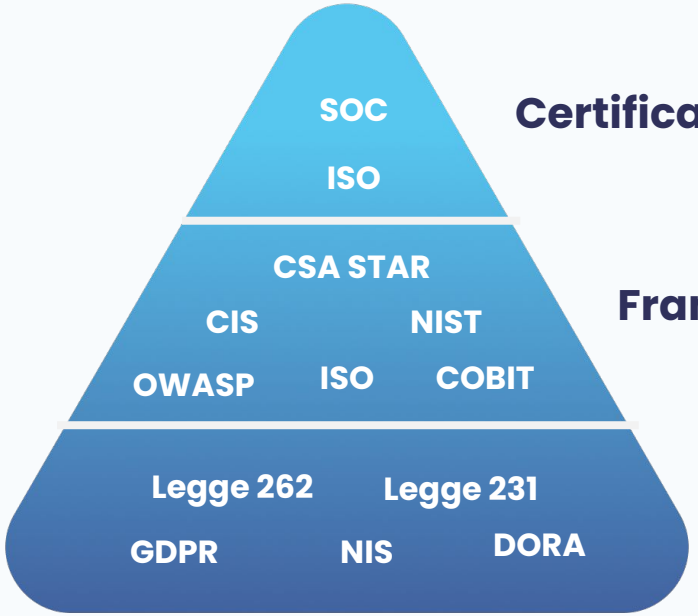
Security controls per BCMS/ISMS
Implementazione dei controlli di sicurezza attraverso l'utilizzo di nuove tecnologie, modifica di tecnologie esistenti e training dei dipendenti

8
Monitoring & improvement

Il monitoraggio e il miglioramento costante rafforzano la cybersecurity, **anticipando minacce e adeguando le difese**

Qual è la normativa? Ci sono dei framework di riferimento?

In questa suddivisione, è importante notare che mentre le normative sono obbligatorie e legalmente vincolanti, i "frameworks" e le "best practices" offrono linee guida e raccomandazioni che, sebbene non obbligatorie, sono ampiamente riconosciute e adottate per migliorare la sicurezza e la governance IT.



Certificazioni

Frameworks & Best practices

Normative

Vai al glossario

Cosa tenere in considerazione?

La **complessità normativa e la relativa complessità tecnologica** esistente sottolinea la necessità di sviluppare processi, progetti e prodotti che garantiscano un elevato livello di sicurezza. La compilazione di un **assessment** dedicato dà la possibilità di indagare le principali **problematiche** del proprio business, evidenziando le **opportunità** di crescita annesse.

Secure Innovation
"Futuro ma sicuro"

GRC – IT Internal Control System & IT Audit
"Le regole del gioco"

Asset & Vulnerability Management
"Tieni alte le difese"

Access Control Management *Chi siete? … Cosa portate? … Sì, ma quanti siete? … Un fiorino!*

Infrastructure Security & Operations Management
"Admin123 non è una password sicura!"

Third Party Management
"Il tuo fornitore è affidabile?"

Business Continuity and Disaster Recovery
"Morto un server se ne fa un altro"

Incident Management
"Non succede ma se succede…"

Qualche dato?

Mercato italiano

2,1 miliardi di euro

+16% rispetto al 2022

*"Tra le altre tendenze che caratterizzano il panorama delle minacce, si denota **l'aumento degli attacchi di tipologia supply chain**, che si propagano a cascata tra fornitori e clienti"*

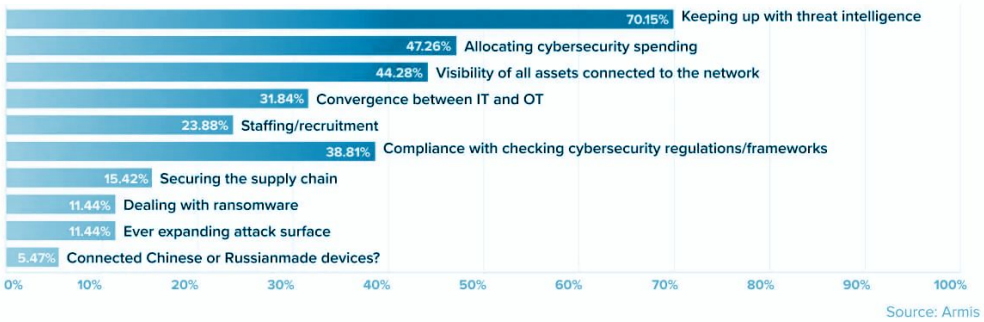
Osservatorio Politecnico

Grandi organizzazioni

+62% di spesa

rispetto al 2022

Le più grandi sfide incontrate dalle aziende in tema di cybersecurity nella prima metà del 2023, secondo il sondaggio di Armis:



Fonti: ANSA - Osservatorio Politecnico - Armis

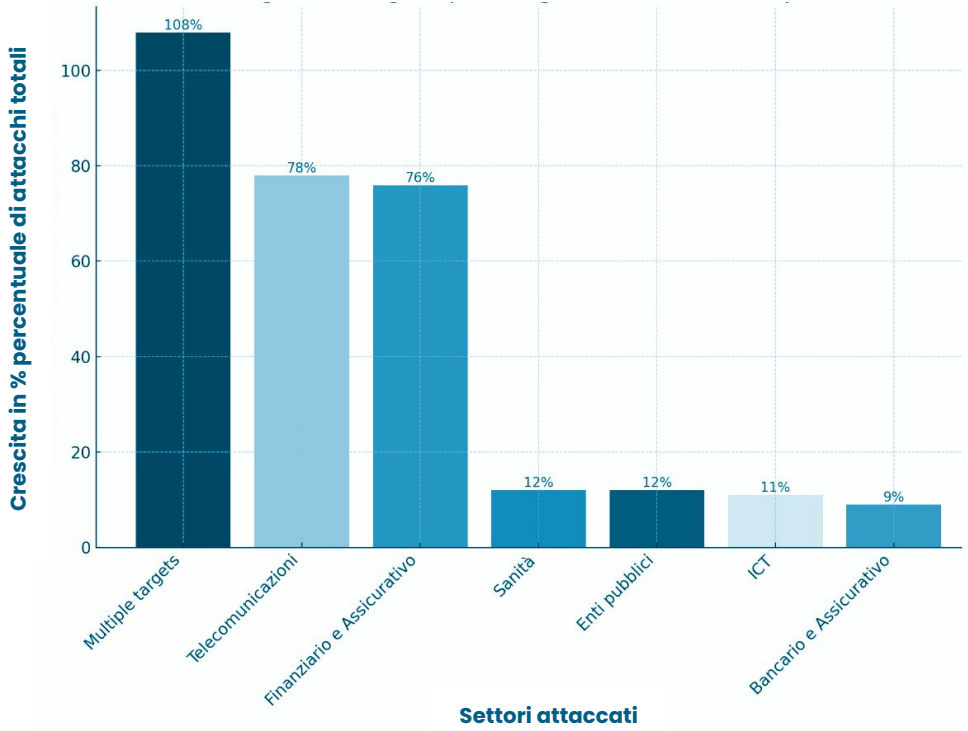
Qualche dato?

Mercato italiano

I settori più colpiti

*"Rispetto al primo semestre del 2021, nel 2022, in Italia, si è osservata una crescita significativa nel numero di attacchi gravi in tre categorie: **Multiple targets** (+108%), **Telecomunicazioni** (+78%) e **Finanziario e Assicurativo** (+76%)."*

Kinetikon



Fonti: Kinetikon

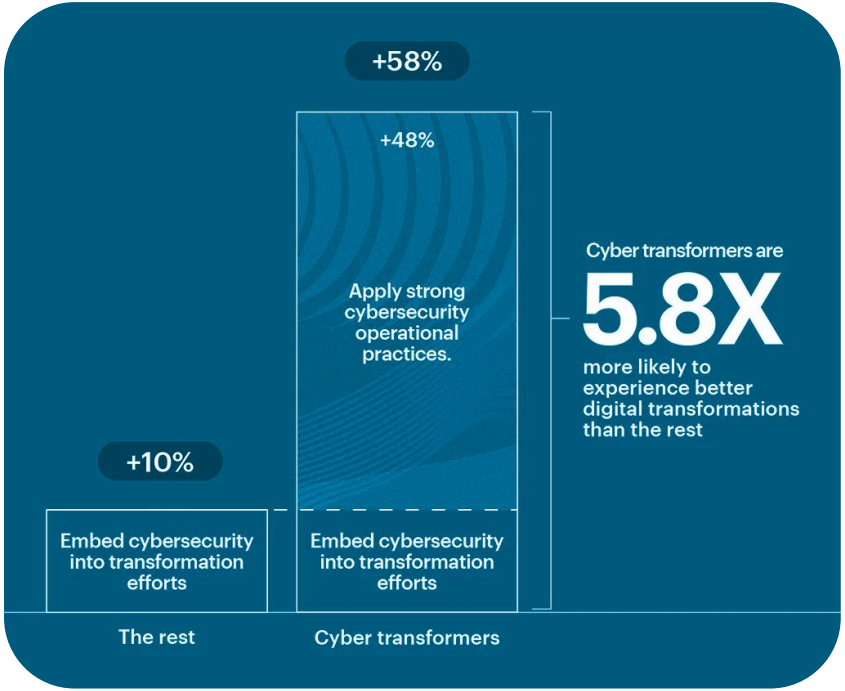
Qualche dato?

Aziende che implementano strategie di cybersecurity

+18% di crescita

"Il mondo è cambiato e la sicurezza informatica sta cambiando con esso. Il desiderio di trasformarsi, più velocemente e con maggiore frequenza, sta spingendo alcune organizzazioni a ***utilizzare la sicurezza informatica come elemento di differenziazione per ottenere risultati aziendali migliori****."*

Accenture



Fonti: Accenture

Quanto costa?

Pre assessment

Gratuito

Form online,
Risultato preliminare

Assessment

Da 1500*€

Assessment completo,
Consulenza alla compilazione,
Gap analysis,
Remediation roadmap

*IVA esclusa

Remediation

Contattaci

Consulenza avanzata personalizzata e gestione di compliance in base alle esigenze del cliente, aderenza alle normative, implementazione framework e best practice

Quills

Compila il nostro **questionario** per identificare lo stato dell'arte della tua azienda rispetto ai principali aspetti che riguardano la cybersecurity.

Questo strumento è progettato per offrirti una **panoramica ad alto livello delle aree a rischio** e per guidarti nella comprensione delle misure di sicurezza attualmente in atto.

Una volta individuate le potenziali aree critiche, il nostro team di esperti sarà pronto ad assisterti nel definire e implementare strategie mirate per rafforzare la tua sicurezza informatica.

Non lasciare che le minacce digitali compromettano il tuo business: agisci ora per garantire una protezione solida e affidabile.

Vai al questionario

Glossario

La sicurezza dei dati e la conformità sono valori interconnessi: le normative complesse mirano a prevenire l'accesso non autorizzato alle informazioni sensibili dei clienti e degli utenti, riflettendo l'importanza di garantire la protezione e il rispetto dei dati.

- **Il GDPR (General Data Protection Regulation)** è un regolamento dell'UE che impone rigide normative sulla protezione dei dati personali e della privacy. Richiede alle aziende di implementare misure di sicurezza per proteggere i dati personali da rischi come perdite, accessi non autorizzati o divulgazioni indebite.
- **DORA (DevOps Research and Assessment)** è un framework che fornisce linee guida e metriche per valutare e migliorare le pratiche di DevOps. La cybersecurity può beneficiare dall'integrazione di controlli di sicurezza nelle pipeline di sviluppo e deployment.
- **I SOC (System and Organization Controls)** reports sono documenti che attestano l'efficacia dei controlli interni di un'organizzazione per la gestione dei rischi. Le organizzazioni possono utilizzarli per valutare la sicurezza dei servizi offerti da terze parti.
- **COBIT (Control Objectives for Information and Related Technologies)** è un framework che fornisce linee guida per il governance e il management IT. Include anche un approccio alla gestione dei rischi e alla sicurezza delle informazioni.

- **NIS (National Institute of Standards and Technology)** fornisce una serie di standard e linee guida, come il Cybersecurity Framework, per migliorare la sicurezza delle informazioni e l'infrastruttura IT. È ampiamente utilizzato dalle organizzazioni per creare programmi di sicurezza robusti.
- **ISO (International Organization for Standardization)** fornisce una serie di standard pertinenti alla cybersecurity, come ISO/IEC 27001 per la gestione della sicurezza delle informazioni e ISO/IEC 22301 per la continuità operativa.
- **OWASP (Open Web Application Security Project)** è una comunità globale che fornisce linee guida, strumenti e risorse per migliorare la sicurezza delle applicazioni web. Il suo focus principale è sull'identificazione e la mitigazione delle vulnerabilità delle applicazioni.
- **ISO 22301** è uno standard internazionale per la gestione della continuità operativa, che aiuta le organizzazioni a prepararsi e rispondere efficacemente a situazioni di emergenza e interruzioni del business, inclusi gli eventi di sicurezza informatica.
- **ISO/IEC 27001** è uno standard internazionale per la gestione della sicurezza delle informazioni. Fornisce un quadro per l'implementazione di un sistema di gestione della sicurezza delle informazioni (ISMS) che aiuta le organizzazioni a proteggere i propri dati e ad affrontare le minacce alla sicurezza.

Grazie per l'attenzione.

Quills x NEXiD

Contattaci
per ulteriori informazioni

Siamo specializzati nel fornire soluzioni innovative e all'avanguardia per soddisfare le vostre esigenze aziendali. Siamo una realtà dinamica e flessibile che sa adattarsi alle sfide del mercato attuale ed è in grado di fornire un servizio personalizzato di qualità.

NEXiD

Digital Xperiences

quills.it

Via Fabio Filzi, 27, 20124
Milano (MI)

infoquills@nexid.it