POMIAGER
Società Tecnologica del Gruppo IQC

Webinar
“Cybersecurity come certificazione, accreditamento e normazione tecnica possono contrastare i rischi”

6 Aprile 2023
Giuseppe Adduce

IQC - ITALIAN QUALITY COMPANY

Integrated Business Service

Servizi ad alto contenuto professionale e tecnologico per la valorizzazione digitale delle perfomance di sistemi di gestione, processi, prodotti e delle competenze delle persone

ic-box competencies

*for digital certification of **people skills and knowledge** In organisations*

geis gestione ispezioni

*for digital treaceability of the **evaluation** of internal and outsourced processes*

ipdt performance digital traceability

*for digital certification of **organizations, processes, services and products performance***

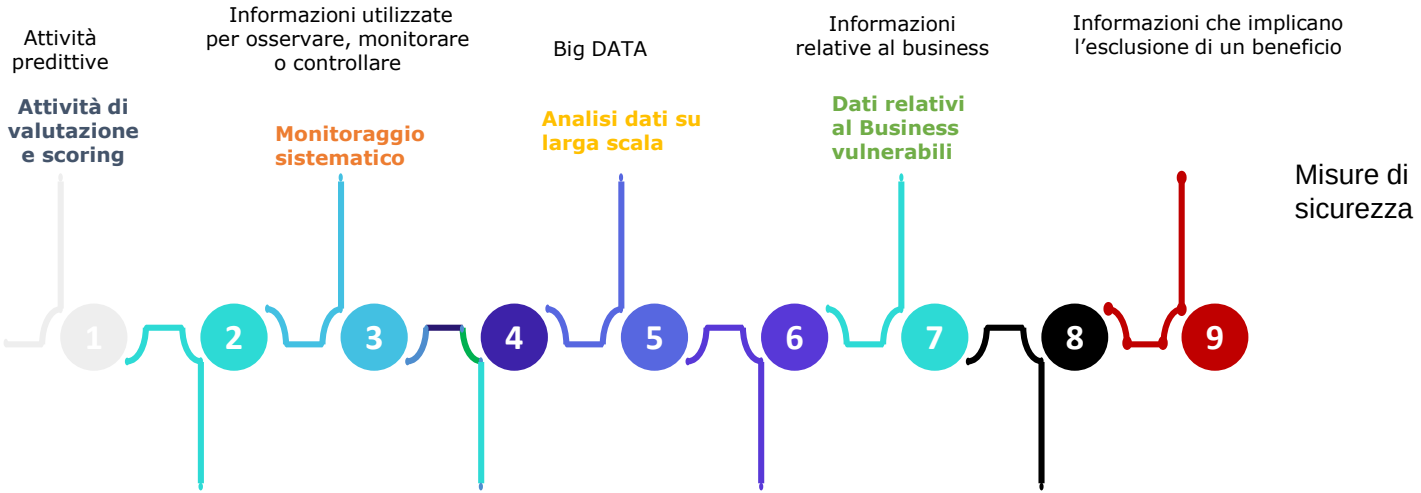
POMIAGER
Società Tecnologica del Gruppo iqc

POMIQC
BLOCKCHAIN

iqc

Valore del Dato Aziendale e della filiera

Analisi dei rischi



Perché Pomiager ha adottato la 27001

Perché parla di controlli che nella sicurezza sono indispensabili:

“Controlli Organizzativi”
“Controlli relativi alle Persone”
“Controlli Fisici”
“Controlli Tecnologici”

La iso/iec 27002:2022

quali controlli ha trattato:

5.1 Politiche per la sicurezza delle informazioni
5.2 Ruoli e responsabilità per la sicurezza delle informazioni
5.3 Separazione dei compiti
5.4 Responsabilità della direzione
5.5 Contatti con le autorità
5.6 Contatti con gruppi di interesse
5.7 Monitoraggio delle minacce
5.8 Sicurezza delle informazioni nella gestione dei progetti
5.9 Inventario delle informazioni e degli altri asset associati
5.10 Uso accettabile delle informazioni e degli altri asset associati
5.11 Restituzione degli asset
5.12 Classificazione delle informazioni
5.13 Etichettatura delle informazioni
5.14 Trasferimento delle informazioni
5.15 Controllo degli accessi
5.16 Gestione delle identità
5.17 Informazioni di autenticazione
5.18 Diritti di accesso
5.19 Sicurezza delle informazioni nelle relazioni con i fornitori
5.20 Sicurezza delle informazioni negli accordi con i fornitori
5.21 Sicurezza delle informazioni nella filiera di fornitura ICT
5.22 Monitoraggio, riesame e gestione dei cambiamenti dei servizi dei fornitori
5.23 Sicurezza delle informazioni per l'uso dei servizi cloud

La iso/iec 27002:2022

quali controlli ha trattato:

5.24 Pianificazione e preparazione per la gestione degli incidenti relativi alla sicurezza delle informazioni
5.25 Valutazione e decisione sugli eventi relativi alla sicurezza delle informazioni
5.26 Risposta agli incidenti relativi alla sicurezza delle informazioni
5.27 Apprendimento dagli incidenti relativi alla sicurezza delle informazioni
5.28 Raccolta di prove
5.29 Sicurezza delle informazioni durante le interruzioni
5.30 Preparazione dell'ICT per la continuità operativa
5.31 Requisiti legali, statutari, regolamentari e contrattuali
5.32 Diritti di proprietà intellettuale
5.33 Protezione delle registrazioni
5.34 Privacy e protezione dei dati personali
5.35 Riesame indipendente della sicurezza delle informazioni
5.36 Conformità con le politiche, le regole e le norme di sicurezza delle informazioni
5.37 Procedure operative documentate
6.1 Screening
6.2 Termini e condizioni di impiego
6.3 Consapevolezza, istruzione, forma- zione e addestramento sulla sicurezza delle informazioni
6.4 Processo disciplinare
6.5 Responsabilità dopo la cessazione o variazione del rapporto di lavoro
6.6 Accordi di riservatezza o di non divulgazione
6.7 Lavoro remoto
6.8 Segnalazione degli eventi di sicurezza delle informazioni

La iso/iec 27002:2022

quali controlli ha trattato:

- 7.1 Perimetri di sicurezza fisica
- 7.2 Accessi fisici
- 7.3 Sicurezza degli uffici, stanze e strutture
- **7.4 Monitoraggio della sicurezza fisica**
- 7.5 Protezione dalle minacce fisiche e ambientali
- 7.6 Lavorare in aree sicure
- 7.7 Scrivania e schermo puliti
- 7.8 Disposizione delle apparecchiature e loro protezione
- 7.9 Sicurezza delle apparecchiature e degli asset all'esterno delle sedi
- 7.10 Supporti di memorizzazione
- 7.11 Infrastrutture di supporto
- 7.12 Sicurezza dei cablaggi
- 7.13 Manutenzione delle apparecchiature
- 7.14 Dismissione sicura o riutilizzo delle apparecchiature

La iso/iec 27002:2022

quali controlli ha trattato:

- 8.1 Dispostivi finali degli utenti
- 8.2 Diritti di accesso privilegiato
- 8.3 Restrizione degli accessi alle informazioni
- 8.4 Controllo degli accessi al codice sorgente dei programmi
- 8.5 Autenticazione sicura
- 8.6 Gestione della capacità
- 8.7 Protezione contro il malware
- 8.8 Gestione delle vulnerabilità tecniche
- **8.9 Gestione delle configurazioni sicure e dell'hardening**
- **8.10 Cancellazione delle informazioni**
- **8.11 Mascheramento e anonimizzazione dei dati**
- **8.12 Prevenzione dalla perdita di dati**
- 8.13 Backup delle informazioni
- 8.14 Ridondanza delle strutture di elaborazione delle informazioni
- 8.15 Logging
- **8.16 Attività di monitoraggio**
- 8.17 Sincronizzazione degli orologi
- 8.18 Uso di programmi di utilità privilegiati
- 8.19 Installazione del software sui sistemi di produzione

La iso/iec 27002:2022

quali controlli ha trattato:

- 8.20 Sicurezza delle reti
- 8.21 Sicurezza dei servizi di rete
- 8.22 Segregazione delle reti
- **8.23 Filtro del web**
- 8.24 Uso della crittografia
- 8.25 Ciclo di vita dello sviluppo sicuro
- 8.26 Requisiti di sicurezza delle applica- zioni
- 8.27 Principi di architettura e ingegnerizzazione dei sistemi sicuri
- **8.28 Codifica sicura**
- 8.29 Test di sicurezza durante lo sviluppo e per l'accettazione
- 8.30 Sviluppo affidato all'esterno
- 8.31 Separazione degli ambienti di sviluppo, test e produzione
- 8.32 Gestione dei cambiamenti
- 8.33 Dati di test
- 8.34 Protezione dei sistemi informativi durante i test di audit

Dalla “sicurezza IT” alla “gestione del cyber risk ”

Sicurezza della rete e dei sistemi informativi

(Direttiva UE/2016/1148 (Cd. direttiva NIS) sulla sicurezza delle reti e dei sistemi informativi attuata con D.Lgs. 18 maggio 2018, n. 65)

“capacità di una rete e dei sistemi informativi di resistere, a un determinato livello di riservatezza, a ogni azione che comprometta la disponibilità, l’autenticità, l’integrità o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tali reti o sistemi informatici”

La componente cyber deve essere gestita attraverso la metodologia propria della compliance aziendale: ricorrendo al cosiddetto **risk based approach**:

- Analisi e valutazione del rischio
- Adozione di procedure e dispositivi per la gestione del rischio
- Individuazione delle responsabilità
- Formazione del personale dipendente
- Continuo miglioramento dei processi

Valore della formazione degli utenti in ambito Cyber

In un’azienda esistono due tipi di asset, tangibili (es. beni materiali) ed intangibili (es. brand, reputazione etc.). La formazione in questo senso è il processo tramite il quale si costruisce il capitale umano, uno degli asset intangibili di un’azienda. Il livello di esposizione al rischio cyber di un asset intangibile e soprattutto l’impatto economico derivante dalla sua perdita o danneggiamento.

Giuseppe Adduce
CEO Pomiager

+39 3488278623

Giuseppe.adduce@pomiager.com

http://blog.pomiager.com/
www.pomiager.com/