MIRIADE
PLAY THE CHANGE

HYCU

Atlassian Cloud NIS2 e DORA

La vostra guida per soddisfare i requisiti di continuità operativa e resilienza previsti dalla normativa UE.

CHECK-LIST

01

Prima di iniziare...

Le normative NIS2 e DORA coprono un'ampia gamma di requisiti, dalla risposta agli incidenti alla prevenzione delle minacce. Tuttavia, per quanto riguarda la protezione dei dati, molte organizzazioni non sono preparate a soddisfare i requisiti di continuità operativa e di resilienza. In effetti, molte aziende non sanno ancora di essere responsabili della conformità e la protezione dei dati delle loro applicazioni SaaS!
Per comprendere la vostra responsabilità in Atlassian, leggete il **Modello di responsabilità condivisa di Atlassian Cloud** scansionando il codice QR qui sotto.

Leggi il Modello di responsabilità condivisa di Atlassian

CHECK-LIST

Incontrare NIS2 e DORA BC/DR e i requisiti di resilienza digitale

Continuità operativa, backup e test sono requisiti critici che dovrete soddisfare con NIS2 e DORA.

Come iniziare Valutazione dei rischi

- [ ] Creare un framework per identificare e mappare tutti i servizi ICT (es. Atlassian Cloud, AWS, Salesforce, ecc.).
- [ ] Sfruttare o creare modelli di auditing per valutare ogni TIC in termini di sicurezza, rilevamento, risposta e continuità operativa.
- [ ] Assegnare a specifici stakeholder la responsabilità delle operazioni di protezione dei dati in Atlassian e in altre applicazioni aziendali.
- [ ] Sfruttate gli strumenti per il monitoraggio continuo delle TIC e documentate regolarmente i cambiamenti nel vostro stack tecnologico, in tutti i reparti.
- [ ] Mantenere la documentazione e i registri per dimostrare la conformità ai requisiti NIS2 e DORA, assicurando la preparazione per audit e ispezioni.

Requisiti di backup

- [ ] Pianificare backup giornalieri per ogni istanza e applicazione in Atlassian Cloud.
- [ ] Assicurarsi che le copie di backup siano accessibili in caso di interruzione o minaccia informatica.
- [ ] Definire una frequenza minima per i backup in base all'applicazione.
- [ ] Assicurarsi che il sistema di backup sia in esecuzione all'esterno e distaccato da Atlassian.
- [ ] Archiviare i backup fuori sede, al di fuori di Atlassian, in uno spazio di archiviazione compatibile con S3.
- [ ] Abilitazione dell'immutabilità sulla destinazione di archiviazione di backup in caso di evento informatico.
- [ ] Il sito di archiviazione di backup deve soddisfare i requisiti di residenza (se applicabile).
- [ ] Implementare e mantenere l'autenticazione a più fattori, la crittografia e la segmentazione della rete per salvaguardare l'integrità e la riservatezza dei backup.

Risposta agli incidenti e recupero

- [ ] Assegnare SLA di recupero proporzionati alla natura critica dell'applicazione.
- [ ] Sviluppare e aggiornare regolarmente piani di disaster recovery che includano modelli per diversi scenari di incidente. Assicuratevi che questi piani siano completi e adattati alle esigenze dell'organizzazione.
- [ ] Condurre corsi di formazione e simulazioni periodiche per migliorare la preparazione del personale alla risposta agli incidenti. Concentrarsi su ruoli, responsabilità e azioni per una gestione efficace degli incidenti.

Recupero e reporting dimostrabili

- [ ] Mantenere la documentazione e i registri per dimostrare la conformità ai requisiti NIS2 e DORA, assicurando la preparazione per audit e ispezioni.
- [ ] Sfruttate strumenti avanzati per il monitoraggio continuo e il reporting in tempo reale delle attività di backup e ripristino, migliorando le capacità decisionali e di risposta agli incidenti.

HYCU

Prendete il controllo dei vostri dati.

Per iniziare, scansionate il codice QR qui sotto o contattateci all'indirizzo miriade.it/contatti