HYCU®

Come iniziare con la conformità DORA

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

LISTA DI CONTROLLO

01

Prima di iniziare...

DORA copre un'ampia gamma di requisiti, dalla risposta agli incidenti alla prevenzione delle minacce. Per quanto riguarda la protezione dei dati, molte organizzazioni non sono preparate a soddisfare i requisiti di continuità operativa e resilienza. In realtà, molte aziende non sanno nemmeno di essere responsabili della conformità e della protezione dei dati delle loro applicazioni SaaS!

Per comprendere le vostre responsabilità in materia di dati SaaS e cloud, leggete il **Modello di responsabilità** condivisa scansionando il codice QR qui sotto.

Scopri il modello di responsabilità condivisa ed evita errori critici

Lista di controllo

Soddisfare i requisiti DORA di backup, disaster recovery e resilienza digitale

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

Quante caselle spunta oggi la vostra organizzazione?

Come iniziare Valutazione dei rischi

- [ ] Creare un quadro 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 per tutte le applicazioni SaaS in uso.
- [ ] Sfruttate gli strumenti per il monitoraggio continuo delle TIC e documentate regolarmente le modifiche apportate allo stack tecnologico, in tutti i reparti.

Requisiti di backup

- [ ] Programmare backup giornalieri per ogni istanza e applicazione del vostro ambiente.
- [ ] 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 al di fuori delle applicazioni SaaS primarie.
- [ ] Archiviare i backup fuori sede in uno storage compatibile con S3, indipendente dalle applicazioni SaaS primarie.
- [ ] Abilitare l'immutabilità sul target 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 meccanismi come l'autenticazione a più fattori, la crittografia e la segmentazione della rete, al fine di garantire l'integrità e la riservatezza dei backup

Risposta agli incidenti e recupero

- [ ] Assegnare SLA di ripristino proporzionali alla criticità dell'applicazione.
- [ ] Sviluppare e aggiornare regolarmente piani di disaster recovery che includano modelli per diversi scenari di incidente, garantendo che tali piani siano completi e adattati alle esigenze dell'organizzazione
- [ ] Condurre periodicamente corsi di formazione e simulazioni 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 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

Scoprite le lacune della conformità DORA e attivate la protezione dei dati con questo strumento di rilevamento SaaS gratuito.