MISE EN PLACE D'UN AUDIT

800 € HT (tarif inter) | REF : -ENV1053
TARIF SPÉCIAL : particuliers et demandeurs d'emploi

Ce métier de DPO (Data Protection Officer) est apparu suite aux évolutions majeures relatives aux obligations légales et à l'évolution de la réglementation liée à la protection des informations et de la vie privée et de la question de la sécurité des systèmes d'information.
Le métier s'appuie sur le règlement n? 2016/679, dit règlement général sur la protection des données (RGPD / GDPR), qui est un règlement de l'Union européenne. Il introduit de nouveaux droits pour les individus et de nouvelles obligations pour les entreprises.

PROGRAMME

Rappel du contexte réglementaire

- Les enjeux du nouveau règlement européen et les raisons de sa mise en place.
- Les principes fondamentaux (AIPD, Privacy by design, principe d'accountability...).
- Rappel des autres contraintes réglementaires (LPM/NIS, PCI DSS...).
- Les acteurs concernés.
- Le rôle du manager du risque (Risk Manager).

Premiers pas avec la démarche ISO 27005

- Présentation des objectifs et des enjeux d'une démarche ISO 27000.
- Les obligations du responsable des traitements.
- Identification d'une échelle de menaces, vulnérabilités, risques.

Gestion du risque

- Mise en place d'une échelle de risques.
- Classification des risques (opérationnels, physiques, organisationnels etc).
- Les impacts de chaque risque (humain, financier etc).
- Le plan d'action pour anticiper chaque risque .
- La mise en place d'une assurance risque.

Mise en place de la démarche ISO

- Planification.
- La mise en œuvre d'une procédure de management des risques (PDCA).
- Mise en place d'un plan d'actions et d'un plan d'applicabilité (SoA).
- L'analyse du partage des risques avec un tiers (assurance, cloud etc).
- Mise en place par conformité.
- Mise en place par scénarios de risques.

Les autres méthodes

- Les méthodes MEHARI.
- Les méthodes EBIOS.
- Choix d'une méthode globale vs une méthode par projet.
- Les critères pour choisir la méthode la plus adaptée.
- Les avantages et contraintes de la méthode ISO.

2 JOURS
14 HEURES

OBJECTIFS

Identifier les risques liées à la sécurité informatique Connaître différentes démarches d'analyse de risques (EBIOS, RM, MEHARI) Pouvoir choisir la démarche la plus adaptée à son contexte Utiliser ISO 27005 pour analyser les risques

PUBLIC | PRÉREQUIS

PUBLIC

Responsables juridiques, Délégué à la protection des données, Data Protection Officer, correspondant informatique et libertés - CIL, informaticiens en lien avec la sécurité des données ou tout responsable de projet en systèmes d'information.

PRÉREQUIS

Connaissance du RGPD ou avoir suivi le module d'initiation au RGPD dans le cadre du parcours Data Protection Officer. Connaissances de base dans le domaine de la sécurité informatique

INFOS PRATIQUES

HORAIRES DE LA FORMATION
de 9 h 00 à 12 h 30 et de 13 h 30 à 17 h 00
MÉTHODOLOGIE PÉDAGOGIQUE
Théorie | Cas pratiques | Synthèse
MODALITÉS D'ÉVALUATION
Évaluation qualitative des acquis tout au long de la formation et appréciation des résultats

DATES ET LIEUX

Aucune session ouverte