

Formation Cybersécurité, Conformité et évolution des normes

Présentation

Ce programme de formation en cybersécurité couvre les bases de la conformité, les exigences légales et réglementaires, et les stratégies pour atteindre et maintenir la conformité. Il inclut une introduction à l'ISO/IEC 27001, la gestion de la sécurité de l'information, et l'application des normes internationales comme le RGPD et le cadre NIST. Le programme aborde également l'évolution des normes de cybersécurité, l'implémentation de la conformité dans les entreprises, et la gestion des incidents liés à la conformité.

Durée : 21,00 heures (3 jours)

Tarif INTRA : Nous consulter

Objectifs de la formation

- Comprendre les normes et méthodes de cybersécurité et leur évolution dans le contexte global.
- Identifier les exigences de conformité et les réglementations en matière de sécurité informatique.
- Appliquer les meilleures pratiques pour répondre aux exigences légales et aux normes internationales.
- Analyser les défis liés à l'évolution des normes et adapter les pratiques de sécurité aux nouvelles menaces.

Prérequis

- Connaissances de base en cybersécurité, gestion des risques et sécurité des systèmes d'information.
- Expérience en gestion des normes et de la conformité au sein d'une organisation.
- Connaissance des principales régulations et normes internationales (ISO, GDPR, NIST, etc.).

Public



- Responsables de la sécurité informatique et des systèmes d'information.
- Consultants en cybersécurité, auditeurs et analystes de la conformité.
- Professionnels de l'IT impliqués dans la gestion des risques et de la conformité en cybersécurité.
- Cadres dirigeants impliqués dans les stratégies de sécurité et de conformité des entreprises.

Programme de la formation

Introduction aux normes de cybersécurité

- Qu'est-ce qu'une norme en cybersécurité et son rôle dans l'amélioration de la sécurité des organisations
- Panorama des principales normes et méthodes (ISO/IEC 27001, NIST, GDPR, PCI-DSS, etc.)
- Objectifs et applications des normes dans différents secteurs d'activité

La conformité en cybersécurité

- La notion de conformité : Qu'est-ce que cela signifie et pourquoi c'est crucial pour les entreprises
- Exigences légales et réglementaires : Analyse du cadre juridique national et international
- Mise en place de stratégies pour atteindre et maintenir la conformité ISO/IEC 27001 et gestion de la sécurité de l'information
- Introduction à l'ISO/IEC 27001 : exigences et processus de certification
- Élaboration et gestion d'un système de management de la sécurité de l'information (SMSI)
- Rédaction de politiques et de procédures de sécurité selon ISO 27001

Réglementation et normes internationales : GDPR, NIST et autres

- Application du RGPD (Règlement Général sur la Protection des Données) dans les organisations
- Le cadre NIST (National Institute of Standards and Technology) pour la gestion des risques et la cybersécurité
- Autres normes : PCI-DSS, HIPAA, CMMC, et leur impact sur la gestion de la sécurité

Evolution des normes et de la cybersécurité

- Analyse des tendances émergentes dans les normes de cybersécurité
- Comment les normes évoluent face aux nouvelles menaces et aux technologies émergentes (IA, IoT, cloud computing)
- Adaptation continue des pratiques de cybersécurité face aux évolutions législatives et aux nouvelles exigences

Implémentation de la conformité dans les entreprises

- Processus d'audit interne pour garantir la conformité et la sécurité
- Utilisation d'outils et de solutions pour automatiser la gestion de la conformité (GRC - Governance, Risk Management, Compliance)
- Formation des équipes et création d'une culture de sécurité à travers l'organisation

Dépannage et gestion des incidents liés à la conformité

- Identifier les faiblesses dans les systèmes de sécurité et les non-conformités
- Gérer les violations de conformité et répondre aux incidents de sécurité en suivant les normes
- Documentation et reporting des incidents de sécurité et des non-conformités

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.

- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation *(évaluation en ligne dans l'extranet apprenant)*

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

Tout au long de la formation

- Évaluations continues réalisées par le formateur à travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

À l'issue de la formation *(évaluations en ligne dans l'extranet apprenant)*

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.