

Formation Les enjeux de la cybersécurité dans son organisation pour les dirigeants

Présentation

Ce module stratégique initie les dirigeants aux enjeux majeurs de la cybersécurité au sein de leur organisation. Il leur permet d'intégrer la sécurité numérique dans la gouvernance d'entreprise, tout en maîtrisant leurs responsabilités légales et leur rôle de leader en situation de crise. À travers des cas concrets et des ateliers, les participants acquièrent les clés pour impulser une véritable culture cyber.

Durée : 10,50 heures (2 jours)

Tarif INTRA : Nous consulter

Objectifs de la formation

À l'issue de la formation, le stagiaire sera capable de s'approprier les enjeux et clés stratégiques de la sécurité numérique dans son organisation.

- Comprendre les enjeux stratégiques de la cybersécurité dans une organisation
- Situer la cybersécurité dans la gouvernance d'entreprise et adapter sa posture
- Connaître le cadre réglementaire et les obligations légales
- Favoriser une culture cyber dans l'entreprise

Prérequis

Cette formation ne nécessite pas de prérequis

Public

Dirigeants d'entreprises, cadre d'entreprise, responsable informatique

Programme de la formation

Jour 1



Module 1. Cybersécurité : un levier stratégique pour l'entreprise

Objectif(s) couvert(s) : Comprendre les enjeux stratégiques de la cybersécurité dans une organisation

- Le paysage actuel des menaces : typologies, motivations, évolutions, nouvelles menaces
- Les impacts économiques, opérationnels, juridiques et réputationnels
- Pourquoi la cybersécurité est un enjeu de performance et de résilience

Cas réel d'entreprise : Analyse des conséquences d'un incident majeur en sous-groupe avec restitution collective

Module 2. Gouvernance et leadership cyber

Objectif(s) couvert(s) : Situer la cybersécurité dans la gouvernance d'entreprise et adapter sa posture

- Intégrer la cybersécurité dans la stratégie globale de l'entreprise
- Les responsabilités des dirigeants : pilotage, exigence de reporting, arbitrages
- Le rôle du COMEX ou des instances dirigeantes : articulation avec la DSI, le RSSI, le juridique
- Anticiper et gérer une situation de crise cyber : posture, communication, décision

Atelier pratique : Réagir à une alerte cyber critique – jeu de rôle du dirigeant en simulant une réunion après une cyberattaque

Module 3. Obligations juridiques et conformité

Objectif(s) couvert(s) : Connaître le cadre réglementaire et les obligations légales

- Les textes de référence : RGPD, NIS2, DORA, directives européennes
- Les responsabilités civiles, pénales, administratives du dirigeant
- Les notifications des incidents, la documentation et la communication externe
- Les risques de non-conformité : sanctions, image, perte de confiance

Étude de cas : À la suite d'une fuite de données, quelles sont les obligations immédiates de l'entreprise ? Liste élaborée collectivement des actions obligatoires à mettre en place dans les délais légaux.

Jour 2 (3,5 heures)**Module 4. Construire une culture cyber au sein de l'organisation**

Objectif(s) couvert(s) :

- Favoriser une culture cyber dans l'entreprise
- Situer la cybersécurité dans la gouvernance d'entreprise et adapter sa posture
 - ? Le rôle du dirigeant dans la diffusion de la culture cyber
 - ? Les actions concrètes :
 - Sensibilisation, formation, processus, politiques internes
 - De la vigilance individuelle à la responsabilité collective
 - S'appuyer sur le management intermédiaire pour relayer les bonnes pratiques

Atelier pratique : Élaborer en sous-groupe une campagne de sensibilisation interne, suivi d'un temps individuel pour compléter sa feuille de route en 5 actions prioritaires pour impulser une culture cyber au sein de son organisation

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

- Apports des connaissances communes.
- Mises en situation sur le thème de la formation et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Équilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux mis à disposition, les apprenants sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

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

En amont de la formation :

- Recueil des besoins des apprenants afin de disposer des informations essentielles au bon déroulé de la formation (profil, niveau, attentes particulières...).
- Auto-positionnement des apprenants afin de mesurer le niveau de départ.

Tout au long de la formation :

- Évaluation continue des acquis avec des questions orales, des exercices, des QCM, des cas pratiques ou mises en situation...

A la fin de la formation :

- Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.
- Evaluation par le formateur des compétences acquises par les apprenants.
- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application au quotidien.

Accessibilité

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