NUMQ47

FONDAMENTAUX DE LA CYBER SÉCURITÉ

VENUS CONSULTING

OBJECTIFS :

- Sécuriser son environnement grâce à la bonne pratique numérique de ses collaborateurs
- Renforcer l'hygiène numérique de son entreprise afin d'éviter les conduites à risque
- Développer des compétences internes sur la gestion du risque et sa communication

PUBLIC :
Cette formation est à destination des non-spécialistes pour apprendre les fondamentaux de la cyber sécurité. Elle est destiné aux managers et dirigeants, issus de tout type de fonction (Juristes, RH, Financiers, Marketing...).

PRÉREQUIS :
Aucun

FORMATEURS :
Cette formation est animée par un formateur expert de Venus Consulting

PROGRAMME

1 - INTRODUCTION

- Transformation numérique.
- Environnement cyber.

2 - ENVIRONNEMENT JURIDIQUE

- Les principaux enjeux juridiques de la propriété intellectuelle (droit d'auteur, logiciels libres, propriété des développements, etc.).
- L'arrivée réglementaire du secret des affaires (directive européenne).
- Les principaux enjeux du droit de la protection des données personnelles :
- Les grands principes de la loi Informatique & Libertés, les obligations légales.
- Le règlement européen sur les données à caractère personnel (RGPD).
- Les principaux enjeux du droit de la sécurité des systèmes d'information : les lois françaises (Godfrain, LCEN ...), la Directive NIS.

3 - INTÉGRER RISQUE CYBER DANS SSI

- Présentation de l'ensemble des risques (menaces, vulnérabilités, etc.) liés à l'information de l'entreprise et réalisation d'une première évaluation qualitative.
- Les techniques d'évaluation des risques (par exemple via la norme ISO 27005).
- Evaluation des risques bruts intrinsèques, et estimation des conséquences des risques avérés (financières, juridiques, humaines, métier, etc.).
- Différences entre le risque Cyber et le risque réel.

4 - RÉALISER UN AUDIT DE SÉCURITÉ

- Présentation des différents types d'audit : Audit de conformité, organisationnel, de - vulnérabilités, technique, de code et tests d'intrusion.
- Bonnes pratiques.
- Plan d'action.
- Démarche "First step".

5 - COMMENT GÉRER UNE CRISE CYBER ?

- Qu'est-ce qu'une crise ?
- Gestion de crise, quels types de difficultés, comment se prépare-t-on ?
- Comment gérer et piloter la crise.
- Communication interne et externe.
- Comment gérer l'après-crise.

6 - ANTICIPER LES RISQUES À VENIR ET CONNAITRE LES ACTEURS

- Processus
- Exemples concrets
- Organisations.

PERSONNALISATION DE LA FORMATION :

Un questionnaire préparatoire sera remis en amont de la formation au participant lui permettant de faire remonter auprès du formateur ses attentes et besoins spécifiques.

VALIDATION DES ACQUIS :

Évaluation des acquis de la formation par des cas pratiques, exercices, QCM... - Questionnaire d'évaluation à chaud proposé à la fin de formation - Une attestation sera remise au stagiaire à la fin de la formation.