Les enjeux de la cybersécurité et les exigences de conformité

Date et durée

Code formation : GSI001FR
Durée : 2 jours
Nombre d'heures : 14 heures

Description

Le paysage numérique actuel rend la **cybersécurité** et la **conformité des données** incontournables pour tous les professionnels. La maîtrise de ces deux domaines complémentaires est désormais essentielle pour assurer la **résilience des systèmes d'information** et maintenir la confiance des clients, partenaires et collaborateurs.
Cette formation vise à vous sensibiliser aux enjeux majeurs de la sécurité informatique et à vous transmettre les compétences fondamentales.
Ce programme abordera les fondamentaux de la cybersécurité : **concepts clés, typologie des menaces** (phishing, ransomwares) et identification des acteurs malveillants. Vous étudierez également les exigences réglementaires liées au **RGPD** et à la norme **ISO 27001**, afin de comprendre les obligations légales et d'intégrer la conformité dans vos pratiques professionnelles. Des **travaux pratiques** viendront ponctuer le parcours afin de renforcer votre compréhension et de faciliter la mise en application concrète des notions abordées.
À l'issue de cette **formation de 2 jours**, vous disposerez des compétences opérationnelles essentielles pour assurer la **mise en conformité** de votre organisation et déployer des mesures de sécurité de base. Vous saurez **réagir efficacement aux incidents**, devenant ainsi un acteur clé dans la protection des données.

Objectifs

À l'issue de cette formation de base en cybersécurité, vous atteindrez les objectifs de compétences suivants :

- appréhender les menaces et les risques inhérents à la cybersécurité ;
- identifier les obligations légales et normatives essentielles (notamment le RGPD et la norme ISO 27001) ;
- mettre en œuvre des mesures de sécurité fondamentales au sein de leur environnement professionnel ;
- contribuer activement à la mise en conformité de leur organisation face aux exigences de sécurité des données ;
- réagir efficacement et de manière structurée en cas de survenue d'un incident de sécurité.

Points forts

- **Sensibilisation complète aux enjeux** : cette formation permet aux professionnels de prendre conscience des défis majeurs de la cybersécurité et de comprendre l'importance des exigences de conformité, notamment le RGPD et la norme ISO 27001.
- **Application pratique immédiate** : grâce à une combinaison équilibrée de théorie, de cas concrets et d'ateliers pratiques, les participants sont préparés à mettre en œuvre directement les mesures et les concepts appris dans leur cadre professionnel.
- **Maîtrise des bases de la conformité** : développez les compétences essentielles pour identifier les menaces, appliquer des mesures de sécurité de base, participer activement à la mise en conformité de votre organisation et réagir efficacement en cas d'incident.

Modalités d'évaluation

Travaux Pratiques

Pré-requis

Suivre cette formation nécessite les prérequis suivants :

- **Connaissances générales** : une familiarité avec les concepts de base de l'informatique et l'organisation générale d'une entreprise est recommandée.

Public

Cette formation s'adresse aux publics suivants :

- Les **collaborateurs non techniques** impliqués dans la manipulation de données ou ayant besoin d'une sensibilisation à la sécurité informatique.
- Les **responsables RH, juridiques et administratifs** qui gèrent des données sensibles et doivent comprendre les enjeux de la conformité.
- Les **recruteurs IT** qu souhaitent mieux appréhender les bases de la cybersécurité et les profils associés.
- Toute **personne amenée à manipuler des données personnelles ou sensibles** dans le cadre de ses fonctions professionnelles.

Programme

Module 1 : comprendre les fondamentaux de la cybersécurité

- Les définitions clés (cybersécurité, cybercriminalité et cyberattaque).
- La typologie des menaces (phishing, ransomware, malware et attaques DDoS).
- Les principaux acteurs de la menace (hackers, insiders, hacktivistes et entités étatiques).
- Les impacts potentiels des cyberattaques (conséquences financières, atteintes à la réputation et implications juridiques).

Module 2 : sécuriser son environnement de travail

- Les bonnes pratiques individuelles de sécurité (gestion robuste des mots de passe avec usage de la MFA et des gestionnaires de mots de passe, ainsi que l'identification des courriels frauduleux.
- La sécurité des appareils mobiles et des outils collaboratifs (partage de fichiers, visioconférences, solutions cloud).
- Les mesures de sécurité physique et logique (contrôle des accès aux locaux, verrouillage des postes de travail et stratégies de sauvegarde des données).

Travaux pratiques :

- Analyser un courriel de phishing pour en identifier les caractéristiques.
- Réagir à un incident de sécurité simulé.
- Débriefer collectivement sur les erreurs et les bonnes pratiques observées.

Module 3 : appliquer le RGPD en pratique

- Les principes fondamentaux du RGPD (licéité, loyauté, transparence, minimisation des données et limitation de leur conservation).
- Les droits des personnes concernées par le traitement de leurs données (droit d'accès, de rectification, d'effacement et de portabilité).

- Les obligations clés de l'entreprise (tenue du registre des traitements, notification des violations de données et désignation d'un DPO.
- Les cas concrets d'application du RGPD (recrutement, gestion des ressources humaines et sous-traitance).

Module 4 : s'initier à la norme ISO 27001:2022

- Les objectifs de la norme ISO 27001 (mise en oeuvre d'un d'un Système de Management de la Sécurité de l'Information : SMSI).
- La structure de la norme (politique de sécurité, analyse des risques et plan de traitement des risques).
- Les mesures de sécurité recommandées par l'ISO 27001 (contrôle d'accès, journalisation des activités, chiffrement des données et gestion des incidents).
- Les liens et la complémentarité entre l'ISO 27001 et le RGPD.

Travaux pratiques :

- Identifier les données personnelles au sein d'un processus métier spécifique.
- Évaluer les risques associés à ces données.
- Élaborer un plan d'action pour la mise en conformité.