Cybersécurité : Aspects techniques et Stratégiques (ISO 27032)

DESCRIPTION DU COURS

Brève description :

De nos jours, les technologies de l'information évoluent et les menaces de cyberattaques sont de plus en plus nombreuses et nuisibles. L'actualité informatique prouve qu'aucun organisme, ni aucun gouvernement, ne sont à l'abri d'une cyberattaque. Une attaque informatique peut avoir des conséquences désastreuses sur le fonctionnement et la confidentialité d'un organisme. Ainsi, il est primordial de savoir gérer efficacement la cybersécurité dans une entreprise.

La formation ISO 27032 Lead Cybersecurity Manager a pour but de vous apprendre à préserver la confidentialité, l'intégrité et le fonctionnement des informations au sein d'une organisation. Durant cette formation, vous développerez vos compétences et connaissances pour concevoir, mettre en œuvre et entretenir un programme de cybersécurité selon la norme ISO 27032:2012. Vous apprendrez à considérer et à faire face à tous les risques actuels en technologie de l'information.

Ces acquis de formation permettent aux organisations de démontrer qu'elles mettent en œuvre les meilleures pratiques dans les processus de la sécurité de l'information. Elles s'appliquent aux organisations de toutes tailles dans le domaine de la technologie qui souhaitent sécuriser leurs systèmes de management.

Objectifs	A l'issue de la **cette formation**, vous atteindrez les objectifs suivants : • Connaître les méthodes et techniques de la cybersécurité conformes à la norme ISO/IEC 27032:2012 et à la cybersécurité selon le NIST (Institut national américain des normes et technologies) ; • Comprendre la relation entre l'ISO/IEC 27032:2012 et la cybersécurité selon le NIST et d'autres normes ; • Savoir et utiliser les différents concepts, techniques, stratégies et méthodologies pour gérer un programme de cybersécurité efficacement ; • Adapter les exigences de la norme ISO/IEC 27032:2012 au sein d'un organisme ;

	• Devenir expert en management de la cybersécurité et conseiller les organismes et entreprises ; • Réussir l'examen PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager et obtenir votre certification. Toutes les compétences que vous acquérez pourront s'appliquer aux organisations de toute taille et de toute nature afin de leur offrir les avantages suivants : • Une sensibilisation en matière de sécurité de l'information améliorée ; • Une réduction des failles de sécurité ; • Un avantage concurrentiel ; • Une crédibilité et une confiance ; • Une conformité aux lois et aux règlements associés.
Dates	24 au 28 Avril 2023
Durée	05 jours

RESULTATS ATTENDUS

Au terme de la formation, les participants devront avoir les compétences suivantes :

- Connaitre les techniques des cyber-attaquants, les contre-mesures et bonnes pratiques;
- Comprendre la relation entre l'ISO/IEC 27032:2012 et la cybersécurité selon le NIST et d'autres normes ;
- Savoir et utiliser les différents concepts, techniques, stratégies et méthodologies pour gérer un programme de cybersécurité efficacement ;
- Adapter les exigences de la norme ISO/IEC 27032:2012 au sein d'un organisme ;
- Devenir expert en management de la cybersécurité et conseiller les organismes et entreprises ;

PUBLIC FILE

Cette formation s'adresse aux publics suivants :

- Les membres du CODIR amener à prendre des décisions dans le domaine IT
- Les responsables des services techniques et technologiques

- Les personnes amenées à travailler dans le management de la continuité d'activité (gestionnaires de risques, consultants, etc.) ;
- Les personnes responsables de mise en conformité d'un SMSI ;
- Professionnels souhaitant enrichir leurs compétences et techniques en cybersécurité ;
- Professionnels de la sécurité et des technologies de l'information ;
- Conseillers en sécurité et technologies de l'information.

Cette formation s'adresse aux profils suivants

- Auditeur interne / externe
- Chef de Projet
- Consultant en formation
- Contrôleur de gestion
- Directeur des Systèmes d'Information (DSI)
- Responsable des opérations / logistiques
- Responsable informatique
- Responsable réseau ou système
- Responsable Sécurité / RSSI

PRE-REQUIS

- Être impliqué dans la sécurité de système d'information ;
- Connaitre les principes fondamentaux de la sécurité des systèmes d'information

AGENDA ET CONTENU DU COURS

Contenu Pédagogique	**Jour 1 : Introduction et enjeux** • Introduction de la SSI • La Sécurité & la Sureté • Les réseaux d'entreprise (locaux, distantes, Cloud). • Comment une négligence peut-elle créer une catastrophe ? La sociologie des pirates. • Les étapes d'une Cyberattaque • La prise de conscience par les acteurs des conséquences d'une cyberattaque **Jour 2 : Cyber sécurité** • Qu'est-ce que la cyber sécurité ? • Cadre normatif et réglementaire de la norme ISO 27032:2012 ; • Qui sont les acteurs ?

	• Rôles et responsabilités des parties prenantes et Leadership ; • Analyser la structure de votre organisation selon une approche sécuritaire ; • Mise en œuvre d'un programme de cybersécurité. **Jour 3 : Politiques, risques et mécanismes d'attaque :** • Quelle politique de cybersécurité appliquer ? • Gérer les risques et la conformité ; • Cybercriminalité : les différents mécanismes et formes d'attaques. **Jour 4 : Mesurer et contrôler la cybersécurité, coordonner et partager l'information :** • Mesurer et contrôler la cybersécurité ; • Coordonner et partager l'information ; • Former et sensibiliser le personnel. **Jour 5 : Gérer les incidents, assurer la surveillance et l'amélioration continue :** • Gérer la continuité des activités (norme ISO 22301:2019) ; • Gérer les incidents de cybersécurité (norme ISO 27035:2016) ; • Tester le niveau de préparation aux cyberattaques ; • Mesurer la performance ; • Réagir et récupérer pour donner suite à un incident de cybersécurité ; • amélioration continue.

MODE D'ANIMATION PEDAGOGIQUE

La méthodologie du cours sera la suivante :

- Chaque session sera étudiée et discutée sur une durée appropriée ;
- Les supports de cours seront mis à disposition au début de la formation ;
- Echange, l'interactivité et la pratique
- Exposés, ateliers pratiques, exemples, retour d'expérience,

SUPPORTS PEDAGOGIQUE

- Des supports de cours (document en PowerPoint en PDF)
- Documents supplémentaires.
- Logiciels de simulation