



ORGANISME DE FORMATION AUX TECHNOLOGIES ET METIERS DE L'INFORMATIQUE

Formation ISO 27035 - Lead Incident Manager : Gestion des incidents de sécurité

Mettre en oeuvre, gérer et tenir à jour un plan d'intervention en cas d'incident

N° ACTIVITÉ : 11 92 18558 92

TÉLÉPHONE : 01 85 77 07 07

E-MAIL : inscription@hubformation.com

Objectifs

- | Être capable de maîtriser les concepts, les approches, les méthodes, les outils et les techniques qui permettent une gestion efficace des incidents de sécurité de l'information selon l'ISO/CEI 27035
- | Connaître la corrélation entre la norme ISO/CEI 27035 et les autres normes et cadres réglementaires
- | Acquérir l'expertise nécessaire pour accompagner une organisation durant la mise en oeuvre, la gestion et la tenue à jour d'un plan d'intervention en cas d'incident de la sécurité de l'information
- | Acquérir les compétences pour conseiller de manière efficace les organismes en matière de meilleures pratiques de gestion de sécurité de l'information
- | Identifier l'importance d'adopter des procédures et des politiques bien structurées pour les processus de gestion des incidents
- | Identifier comment développer l'expertise nécessaire pour gérer une équipe efficace de réponse aux incidents

Public

- | Gestionnaires des incidents de sécurité de l'information
- | Responsables des TIC
- | Auditeurs des technologies de l'information
- | Responsables souhaitant mettre en place une équipe de réponse aux incidents
- | Responsables souhaitant apprendre davantage sur le fo

Prérequis

- | Aucun

Programme de la formation

Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'information, tels que définis par l'ISO/CEI 27035

- | Objectifs et structure de la formation
- | Cadres normatifs et réglementaires
- | Gestion des incidents liés à la sécurité de l'information
- | Processus de base de la norme ISO/CEI 27035
- | Principes fondamentaux de la sécurité de l'information
- | Corrélation avec la continuité des activités
- | Questions légales et déontologiques

Conception et préparation d'un plan de gestion des incidents de sécurité de l'information

- | Lancement d'un processus de gestion des incidents de sécurité de l'information
- | Compréhension de l'organisation et clarification des objectifs de la gestion des incidents de sécurité de l'information
- | Planifier et préparer
- | Rôles et fonctions
- | Politiques et procédures

Référence	MGR841
Durée	5 jours (35h)
Tarif	3 840 €HT
Certification	prix inclus

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

- du 27 au 31 mai 2024
- du 8 au 12 juillet 2024
- du 26 au 30 août 2024
- du 21 au 25 octobre 2024
- du 18 au 22 novembre 2024

PARIS

- du 27 au 31 mai 2024
- du 8 au 12 juillet 2024
- du 26 au 30 août 2024
- du 21 au 25 octobre 2024
- du 18 au 22 novembre 2024

[VOIR TOUTES LES DATES](#)

Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information

- | Planification de la communication
- | Premières étapes de la mise en oeuvre
- | Mise en place des éléments de support
- | Détection et rapport
- | Évaluation et décisions
- | Réponses
- | Leçons apprises
- | Transition aux opérations

Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information

- | Analyse supplémentaire
- | Analyse des leçons apprises
- | Mesures correctives
- | Compétence et évaluation des gestionnaires d'incidents

Passage de l'examen de certification PECB Certified ISO/CEI 27035 Lead Incident Manager (en ligne après la formation)

- | Révision des concepts en vue de la certification

Certification

Cette formation prépare au passage de la certification suivante.
N'hésitez pas à nous contacter pour toute information complémentaire.

PECB Certified ISO/CEI 27035 Lead Incident Manager

Un voucher permettant le passage du test de certification est adressé à l'issue de la formation y préparant. Chaque participant doit créer son profil sur l'espace PECB puis, une fois le profil validé, choisir un créneau pour passer l'examen et télécharger l'application PECB Exams.

Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir la certification

- | Durée : 3h00
- | Langue : anglais
- | Score minimum : 70%

En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires

L'examen couvre les domaines de compétences suivants :

- | Domaine 1 : principes et concepts fondamentaux relatifs à la gestion des incidents liés à la sécurité de l'information
- | Domaine 2 : meilleures pratiques de la gestion des incidents liés à la sécurité de l'information selon la norme ISO/CEI 27035
- | Domaine 3 : conception et développement d'un processus de gestion des incidents organisationnels selon l'ISO/CEI 27035
- | Domaine 4 : préparation aux incidents de sécurité de l'information et mise en oeuvre d'un plan de gestion des incidents
- | Domaine 5 : lancement du processus de gestion des incidents et traitement des incidents liés à la sécurité de l'information
- | Domaine 6 : surveillance et mesure de la performance
- | Domaine 7 : améliorer les processus et les activités de gestion des incidents

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

- | Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas

nécessaire suivant l'environnement.

| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.

| Privilégier une connexion filaire plutôt que le Wifi.

| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.

| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).

| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.

| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.

| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.

| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.

Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.