Information Security Foundation based on ISO IEC 27001 (certification comprise)

Référence : **SECISF 27001 Fondation** Durée : **2 jours** Certification : **ISO/IEC**

CONNAISSANCES PREALABLES

• Cette formation ne nécessite pas de pré-requis..

PROFIL DES STAGIAIRES

• Entrepreneurs indépendants qui doivent disposer de connaissances élémentaires en matière de sécurité de l'information. • Nouveaux professionnels de la sécurité de l'information. • Tout membre de l'organisation chargé du traitement de l'information.

OBJECTIFS

• Information et sécurité : les concepts, la valeur de l'information et l'importance de la fiabilité. • Menaces et risques : les concepts de menace et de risque, et la relation entre les menaces et la fiabilité. • Approche et organisation : la politique de sécurité et la configuration de la sécurité de l'information incluant les composants de l'organisation de la sécurité et de la gestion des incidents (de sécurité). • Mesures : l'importance des mesures de sécurité, notamment physiques, techniques et organisationnelles. • Lois et réglementations : leur importance et leur impact.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Management de la sécurité

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Information et sécurité

• Le concept d'information : Expliquer la différence entre une donnée et une information ; Décrire le support de stockage qui fait partie de l'infrastructure de base
• Valeur de l'information : Décrire la valeur des données/de l'information pour les organisations ; Décrire comment la valeur des données/de l'information peut influencer les organisations ; Expliquer comment les concepts de sécurité de l'information appliqués protègent la valeur des données/de l'information.
• Critères de fiabilité : Nommer les critères de fiabilité de l'information ; Décrire les critères de fiabilité de l'information

Menaces et risques

• Menaces et risques : Expliquer les concepts de menace, de risque et d'analyse des risques ; Expliquer la relation entre une menace et un risque ; Décrire divers types de menaces ; Décrire divers types de préjudices ; Décrire diverses stratégies de gestion des risques
• Relations entre les menaces, les risques et la fiabilité de l'information : Reconnaître des exemples de divers

types de menaces ; Décrire les effets des divers types de menaces sur l'information et le traitement de l'information

Approche et organisation

- Politique de sécurité et organisation de la sécurité: Donner un aperçu des objectifs et du contenu d'une politique de sécurité ; Donner un aperçu des objectifs et du contenu d'une organisation de la sécurité
- Composantes : Expliquer l'importance d'un code de conduite ; Expliquer l'importance de la propriété ; Nommer les rôles les plus importants dans l'organisation de la sécurité de l'information
- Gestion des incidents : Résumer la manière dont les incidents de sécurité sont signalés et indiquer les informations requises ; Donner des exemples d'incidents de sécurité ; Donner des exemples d'incidents de sécurité ; Expliquer ce qu'implique le processus d'escalade des incidents (au niveau fonctionnel et hiérarchique) ; Décrire les effets du processus d'escalade des incidents au sein de l'organ

Mesures

- Importance des mesures : Décrire diverses façons de structurer ou d'organiser des mesures de sécurité ; Donner des exemples pour chaque type de mesure de sécurité ; Expliquer la relation entre les risques et les mesures de sécurité ; Expliquer l'objectif de la classification des informations ; Décrire l'effet de la classification
- Mesures de sécurité physiques : Donner des exemples de mesures de sécurité physiques ; Décrire les risques impliqués par des mesures de sécurité physiques insuffisantes
- Mesures techniques : Donner des exemples de mesures de sécurité techniques ; Décrire les risques impliqués par des mesures de sécurité techniques insuffisantes ; Comprendre les concepts de cryptographie, de signature numérique et de certificat ; Nommer les trois étapes des opérations bancaires en ligne (PC, site Internet, paiement) ; Nommer divers types de logiciels malveillants ; Décrire les mesu

Lois et réglementations

- Lois et réglementations : Expliquer pourquoi les lois et réglementations sont importantes pour la fiabilité de l'information ; Donner des exemples de lois relatives à la sécurité de l'information ; Donner des exemples de réglementations relatives à la sécurité de l'information ; Indiquer d'éventuelles mesures susceptibles d'être prises pour satisfaire les exigences des lois et réglementations