ADMINISTRATRICES ET ADMINISTRATEURS ENGAGÉS

Programmes courts

Les fondamentaux de la cybersécurité

V01 du 20/11/2024 durée de la validité de la version : 1 an renouvelable

À Paris **Durée :** 1 jour **Tarifs :** public 1150 € net /adhérent 900 € net (frais de restauration inclus)

Depuis plusieurs années, plus une journée ou presque ne se passe sans qu'une entreprise « fasse la une » en raison d'une faille dans la sécurité de ses systèmes d'information. Les enjeux réglementaires liés à ce thème sont par ailleurs en constante évolution (RGPD, NIS 2, DORA...) et exposent les entreprises à des amendes potentiellement très importantes. Dans ce contexte, cette formation vous permettra de maîtriser le vocabulaire de base de la cybersécurité, de mieux appréhender les risques « cybers » (principales attaques/failles) et de maîtriser les principales techniques de prévention, de détection et de remédiation des attaques. Vous serez ainsi en mesure de progresser dans votre rôle de supervision de ce risque devenu majeur.

Public concerné

- Tout type d'administrateur(trice) souhaitant évaluer la gestion des risques de cybersécurité des entreprises supervisées

Format et durée

- En présentiel sur 1 jour (7h)

Prérequis et condition d'accès à la formation

- Une fiche de vocabulaire doit être lue avant la session

Objectifs opérationnels / Compétences visées

Le participant sera capable de :

- Maitriser l'essentiel du vocabulaire (complexe) de la cybersécurité
- D'identifier et d'évaluer les principaux risques « cyber » d'une organisation ainsi que leurs conséquences (opérationnelles, financières, juridiques…).
- D'évaluer la qualité et la quantité des moyens mis en œuvre par l'entreprise pour sa défense (au regard de ses risques)

Objectifs pédagogiques

- Reconnaitre les principaux risques « cyber » d'une organisation (sur la base de son activité, de son organisation, des réglementations applicables…)
- Mesurer la pertinence des outils et méthodes mis en place par l'entreprise pour se défendre

Jour	Séquence	Contenu	Modes pédagogiques
Matinée	- Introduction - Les conséquences de la matérialisation des risques « cyber » - Identifier et évaluer les risques « cyber »	- Quelques chiffres importants en matière de cybersécurité ; - Quelques « mots clés » de la cybersécurité : o Sécurité de l'information vs sécurité de l'informatique o Présentation du concept de « surface d'attaque » Les conséquences du « risque cyber » - Conséquences opérationnelles - Conséquences financières - Conséquences juridique (dans le cadre du RGPD, de NIS2…) - introduction au cadre juridique de la cybersécurité et de la protection des données personnelles - Conséquences réputationnelles - Conséquences humaines A/ Identifier simplement les risques « cyber » de son organisation B/ Présentation des principales « failles » de sécurité de l'information - 1) Les erreurs humaines o Les pertes de matériels o Les usages mixtes o L'utilisation de l'IA o Les connexions non sécurisées o L'élicitation o Le "shadow IT" et "shadow data" - 2) Les attaques o Les attaques par phishing o Les ransomwares o Les attaques des mots de passe o Les attaques par déni de service o Les attaques web (manipulation d'URL, injection SQL, cross-site scripting…). o L'iinterception des communications o La fraude au Président…	Support pédagogique
Après-midi	- La gestion de la cybersécurité : les principaux livrables d'un programme de cybersécurité et le rôle de l'administrateur (**pour chaque livrable, une checklist de vérification vous sera communiquée)**	- La Gouvernance de la sécurité de l'information - Le budget cybersécurité - L'analyse des risques « cyber » - La veille technique et réglementaire - La PSSI et la charte informatique - La gestion des accès - La gestion des mots de passe (et plus largement de l'authentification) - L'analyse des vulnérabilités et la gestion des mises à jour - Le chiffrement - La formation des collaborateurs - La gestion des incidents (y compris en cas de violation de données personnelles) - Autres éléments de gestion de risques « cyber »	Support pédagogique

Toutes ces séquences sont aménageables en fonction des personnes en situation de handicap (PSH).

Accessibilité & prise en compte du handicap

- Pour toutes nos formations, nous réalisons des études préalables à la formation pour adapter les locaux, les modalités pédagogiques et l'animation de la formation en fonction de la situation de handicap annoncée. **Le DUERP (document unique d'évaluation des risques professionnels) du client s'applique à la formation**.
- En fonction des demandes, nous mettrons tout en œuvre pour nous tourner vers les partenaires spécialisés.
- Notre Référent Handicap : Laurence Beauquier– laurence.beauquier@ifa-asso.com

Délais d'accès

- 11 jours ouvrés

Moyen d'encadrement

- Praticiens de la gouvernance ayant une expérience professionnelle confirmée de plusieurs années au sein de conseils d'administration et d'organes de gouvernance

Moyen pédagogiques et techniques

Pour chacun des participants :

- Supports pédagogiques
- Un Vade-mecum de la gouvernance actualisé
- Les dernières publications de l'Institut Français des Administrateurs

Les salles de cours sont climatisées, équipées de WIFI

Evaluation et suivi

- Questionnaire de pré-positionnement sur le niveau de connaissance à l'entrée du programme
- Questionnaire post-formation sur les acquis de la formation
- Evaluation à chaud de la formation
- Feuille d'émargement par demi-journée
- Attestation de présence nominative

Effectif

Minimum : 5 personnes

Maximum : 14 personnes

Référents

- ### Pédagogique

  Alexandra Courel
  alexandra.courel@ifa-asso.com

- ### Handicap

  Laurence Beauquier
  laurence.beauquier@ifa-asso.com

Tarifs et modalités de règlement :

- Public : 1150€ net (frais de restauration inclus)
- Adhérent : 900€ net (frais de restauration inclus)
- Virement à réception de la facture