ADS — ACADÉMIE DES SAVOIRS — Centre de formation

Formation cybersécurité pour les Ressources Humaines

PROGRAMME DE FORMATION	DURÉE : 1 jour (7 heures) – en centre de formation ou en entreprise.	Présentiel

Objectif

Contribuer à la cybersécurité de mon entreprise pour les responsables Ressources Humaines (Rôle et responsabilités dans le domaine).

Pré-requis

Compréhension de l'informatique de base.

Participants

Direction des ressources humaines.

Validation

L'évaluation du cours se fera à travers des exercices : des phases de quizz et de questions/réponses.

Modalités

Nos formateurs utilisent les méthodes andragogiques suivantes : la démonstration, l'étude de cas, le projet, le questionnement de groupe et le quizz.

Infos complémentaires

Délai d'accès :
Entre 15 et 45 jours. Formation accessible aux personnes en situation de handicap. Plus d'informations au 0692 22 55 83.

Débouchés :
Cette formation permet une montée en compétences mais ne permet pas de se former à un métier.

Passerelles :
Aucune passerelle disponible.

Programme synthétique

Module 1
Les cyberattaques locales récentes,
Témoignages d'un DRH de victimes de cyberattaques
Un site pour se tenir informé de l'actualité cyber

Module 2
L'environnement numérique des entreprises, et transformation digitale des RH,
Comprendre la révolution numérique, le rôle des géants de la tech, Les usages (WEB, Darkweb, réseaux sociaux..) et les tendances, et les usages locaux (à La Réunion)
Comprendre Les apports concrets des technologies (WEB, Cloud, 5G, Big Data, IA IOT. « smart environment ») pour la fonction « RH », et leur impact.

Module 3
Panorama des menaces
Définir Les sources de risques, les effets recherchés d'une attaque par type (sabotage, espionnage, atteinte à l'image, cybercriminalité, cyberguerre..)
Qualifier brièvement les attaquants, et les menaces qu'ils peuvent faire peser sur les entreprises
Connaître les principales menaces (et les autres) sur les données et les processus RH

Module 4
Les essentiels de la cybersécurité
Connaître les actifs essentiels d'un système d'information
Définir Les critères de sécurité (les exemples pour les ressources humaines
Mettre en œuvre (impérativement) des processus quelle que soit la taille de l'entreprise,
Connaître les activités, les domaines, quelques outils
Différencier cybersécurité et cyber résilience

Module 5
Mise en pratique avec un exemple (actif, critères…)

Module 6
Les RH, acteurs clés de la cybersécurité:
Intégrer la sécurité dans la dématérialisation des processus Rh en particulier dans le recrutement, la gestion de mobilité dont le « onboarding et offboarding », la formation, la paie,
Recruter et gérer des spécialistes cyber,
Intégrer les RH dans la gestion des données, en particulier connaître les obligations de conformité,
Respecter dans le temps les exigences du RGPD (Connaître les principes d'un système de management des données à caractère personnel, quand et comment conduire une analyse d'impact à la protection des données

Module 7
La participation de la fonction à la gestion de crise (exercice)

Module 8
Les bonnes pratiques de cybersécurité au quotidien
Connaître les principaux vecteurs pour les attaquants (le hameçonnage, les supports amovibles, et mots de passe..),
Sécuriser mes informations,
Actions à réaliser en cas de fuite de données RH,
Utiliser internet en sécurité