DEVELOPPER LES BONNES PRATIQUES EN MATIERE DE CYBERSECURITE

Durée en heures : 7 heures

Date(s) de session(s) : 9 avril - 9 mai - 3 juin. D'autres dates peuvent être envisagées en fonction des demandes

Nombre de participants minimum : 8

Nombre de participants maximum : 16

Lieu(x) de formation : Montpellier - Nîmes

Publics concernés :

Acteurs en capacité à amorcer un projet de transformation de l'entreprise : Personnel de direction salarié, personnel d'encadrement (responsable projet...), représentant du personnel.

Pré-requis :

Personne en charge de la gestion, sécurisation des données en entreprise. Responsable informatique

Tarifs :

800€

Adresse :
Cnam Occitanie
989 rue de la Croix Verte
Parc Euromédecine
34093 Montpellier Cedex 05
04 67 63 63 40
lgr_contact@lecnam.net

www.cnam-occitanie.fr

Objectifs :

- Connaître le rôle et missions d'un pilote SSI (Sécurité du système d'information),
- Gérer les projets et les priorités, négocier un budget,
- Réagir en cas d'incidents, procédures et acteurs à mobiliser,
- Identifier le panorama des menaces principales auxquelles sont exposées les PME,
- Diffuser les bonnes pratiques à mettre en œuvre pour protéger leur organisation,
- Connaître les outils à disposition du pilote SSI,
- Identifier les aides des pouvoirs publics existantes pour faire le point et se faire accompagner, le cas échéant.

Méthodes et supports pédagogiques :

Livrable reprenant les grands concepts abordés en formation

- Démonstration de nouveaux usages.
Accès à la plateforme pédagogique du Cnam pendant 3 mois.

Contenu pédagogiques :

1ère partie :

- Définition de la cybersécurité et présentation des principaux risques encourus dans les entreprises.
- Architecture d'un système d'information dans une organisation et rôle des différentes composants (serveur, réseau, poste de travail, ...)
- Menaces liées à l'utilisation de l'informatique et des différents types de réseaux : privés d'entreprises ou réseaux publics (internet) ;
- Enjeux liés à la cybersécurité pour les entreprises et les personnes; Présentation de cas concrets et discussions : petit tour d'horizon de l'actualité et présentation de "Cas d'école" issus du panorama de la cybersécurité (Clusif).

2 ème partie :

- Aspects juridiques et réactions possibles face aux attaques
- Aspects légaux de la cybersécurité : textes de loi relatifs à la SSI (loi Godfrain) , valeur juridique du courrier électronique, notion de charte de sécurité, droits d'auteur et propriété intellectuelle;
- Principales règles d'hygiène informatique : sécurité physique , authentification des utilisateurs, sécurisation du réseau et des équipements terminaux, surveillance des systèmes, bonnes pratiques, réaction en cas d'incident;
- Principaux freins à la cybersécurité et indications pour réduire ces freins en s'appuyant sur des recommandations faites par des organismes de sécurité des systèmes d'information tels que l'ANSSI ;
- Etude de cas de synthèse : la fin de cette journée se terminera par une réflexion et une discussion collective autour d'un texte ou d'un évènement d'actualité.

3 - Documents remis aux participants : intégralité des supports de cours présentés + Liens utiles sur des sites institutionnels

Maj 31/01/2019