

Sécurité informatique - Référent en cybersécurité

2 j (14 heures)

Ref : SIRC

Public

Cette formation est adaptée à toute personne souhaitant devenir le référent interne en cybersécurité : dirigeant, cadre, responsable informatique ...

Pré-requis

Avoir suivi le module sécurité informatique - sensibilisation des utilisateurs

Moyens pédagogiques

Formation réalisée en présentiel ou à distance selon la formule retenue
Exposés, cas pratiques, synthèse, assistance post-formation pendant trois mois
Un poste par stagiaire, vidéoprojecteur, support de cours fourni à chaque stagiaire

Modalités de suivi et d'évaluation

Feuille de présence émargée par demi-journée par les stagiaires et le formateur
Exercices de mise en pratique ou quiz de connaissances tout au long de la formation permettant de mesurer la progression des stagiaires
Questionnaire d'évaluation de la satisfaction en fin de stage
Auto-évaluation des acquis de la formation par les stagiaires
Attestation de fin de formation

La cyber délinquance a envahi notre quotidien. Jour après jour les médias nous annoncent des attaques de plus en plus pernicieuses. Nul ne peut se dire à l'écart de ces pratiques malveillantes et chacun peut se trouver confronté à des pertes de données.

Vol, panne de matériel, déni de services, cryptage de données, les risques sont présents pour toutes les entreprises. Il devient essentiel de définir une réelle politique de sécurité du système d'information adaptée à la structure de son entreprise.

Mettre en place des dispositifs techniques, former et sensibiliser ses collaborateurs, mettre en place une charge ou des plans de secours sont des actions qui permettront de limiter les risques et de gagner du temps en cas d'incident.

Cette formation a pour objectif de vous donner les éléments, bonnes pratiques et méthodes permettant de mettre en place une action de Sécurité des Systèmes d'Information dans votre entreprise.

Objectifs

Maîtriser les enjeux de la cybersécurité pour l'entreprise

Identifier et utiliser les outils nécessaires à la protection des informations sensibles

Prendre conscience du rôle que vous avez à jouer

Participer à la mise en œuvre des solutions exposées et veiller à leur application

Savoir traiter les incidents

Connaître les techniques de sécurisation d'un SI, partiellement ou intégralement externalisé

Programme détaillé

QUELS BESOINS DE SECURITE POUR MON ENTREPRISE ?

Principe de défense en profondeur
Identification et évaluation des actifs et des objectifs de sécurité
Analyse de risque

L'HYGIENE INFORMATIQUE POUR LES UTILISATEURS

Connaître le système d'information et ses utilisateurs
Identifier le patrimoine informationnel de son ordinateur (brevets, recettes, codes source, algorithmes...)
Maîtriser le réseau de partage de documents (en interne ou sur internet)
Mettre à niveau les logiciels
Authentifier l'utilisateur

GESTION ET ORGANISATION DE LA SECURITE AU SEIN DE L'ENTREPRISE

Présentation des publications/recommandations
Méthodologie pédagogique pour responsabiliser et diffuser les connaissances ainsi que les bonnes pratiques internes (management, sensibilisation, positionnement du référent en cybersécurité, chartes, etc.)
Méthodologie d'évaluation du niveau de sécurité
Actualisation du savoir du référent en cybersécurité
Gérer un incident / Procédures judiciaires
Plan de continuité d'activité (PCA) / Plan de reprise d'activité (PRA)
Aspects juridiques : Cyber-assurances

LA CYBERSECURITE DES PME AYANT EXTERNALISE TOUT OU PARTIE DE LEUR SI

Les différentes formes d'externalisation

- Les contrats de services « classiques »
- Enjeux du cloud computing
- Software as a Service (SaaS)
- Techniques de sécurité lors de l'externalisation (chiffrement des données...)

Comment choisir son prestataire de service ?

Points clés techniques et organisationnels de sécurité à identifier lors du choix d'un prestataire

Aspects juridiques et contrat

- Bases juridiques pour protéger son patrimoine économique lors de l'externalisation d'un SI
- Présentation du référentiel de l'ANSSI Maitriser les risques de l'infogérance
