

L'ARGUS

de l'assurance

■ ■ ■ Formations

CDA - SÉCURITÉ INFORMATIQUE ET USAGES DIGITAUX : COMMENT AGIR AU QUOTIDIEN

Classe virtuelle

3H30 EN CLASSE VIRTUELLE (3 X 70 MN), 20 MINUTES EN E-LEARNING

CERTIFICAT DIGITAL ASSURANCE (CDA)

CODE : WOBV03

Objectifs de la formation

- Percevoir les principaux risques liés à l'utilisation des outils digitaux dans l'entreprise
- Comprendre les enjeux de la sécurisation des systèmes et des données
- Réaliser ses missions en respectant les procédures de sécurité, règles déontologiques & réglementaires et le règlement de l'entreprise
- Maîtriser la notion de fiabilité, sauvegarde, partage et confidentialité des données

Animée par

- AGHROUM Christian

Retrouvez les modalités pédagogiques et techniques, les moyens d'encadrement et d'accompagnement [ICI](#)

Une formation composée d'une session en classe virtuelle de 3x70min et d'un module e-learning de 20 min

**SÉCURITÉ INFORMATIQUE ET
USAGES DIGITAUX : COMMENT**

Public concernés

- Tout public

Dates

- Classe virtuelle
02-16/12/2019

Prérequis

- Cette formation entre dans le champ d'application des dispositions relatives à la formation professionnelle continue car considérée comme une action d'adaptation et de développement des compétences des salariés.

Modalités pédagogiques

- Tous nos stages de formations sont limités, dans la mesure du possible, à une douzaine de participants.
- Les formations se déroulent en présentiel ou en classe virtuelle avec un équilibre théorie / pratique. Chaque fois que cela est pertinent des études de cas et des mises en pratique ou en situation sont proposées aux stagiaires.
- Un questionnaire préalable dit 'questionnaire pédagogique' est envoyé aux participants pour recueillir leurs besoins et attentes spécifiques. Il est transmis aux intervenant(e)s avant la formation, leur permettant de s'adapter aux publics.
- Toute formation se clôture par une évaluation à chaud de la satisfaction du stagiaire sur le déroulement, l'organisation et les activités pédagogiques de la formation. Les intervenant(e)s évaluent également la session.
- Une auto-évaluation des acquis pré et post formation est effectuée en ligne afin de permettre à chaque participant de mesurer sa progression à l'issue de la formation.
- Une évaluation à froid systématique sera effectuée à 6 mois et 12 mois pour s'assurer de l'ancrage des acquis et du transfert de compétences en situation professionnelle, soit par téléphone soit par questionnaire en ligne.

Tarifs

AGIR AU QUOTIDIEN (CLASSE VIRTUELLE)

Module 1

Comprendre l'environnement sécurité lié aux usages digitaux

- Tour d'horizon des menaces et adversaires de votre système d'information
- Les principaux vecteurs d'attaque et la vigilance adaptée : quid du « fishing » et des emails suspects

Comment agir au quotidien en toute sécurité

- Votre rôle clé en tant qu'utilisateur dans la chaîne de sécurité de votre système d'information
- Choisir avec soin ses mots de passe : appliquer les procédures et bonnes pratiques

Module 2

Développer votre vigilance numérique

- Mettre à jour des logiciels
- Prendre soin de son identité numérique
- Protéger ses données lors de ses déplacements
- Savoir conserver et sauvegarder des informations ou des données

Module 3

Développer votre vigilance numérique (suite)

- Les règles générales à respecter en termes de confidentialité, sur le poste de travail, sur le réseau interne et sur les réseaux externes

Usages digitaux et équilibre de vie

- Les usages digitaux et la santé au travail
- Le cadre légal et le droit à la déconnexion

Modalités pédagogiques

- Le formateur fait défiler le support en le commentant ou en parlant devant la caméra. Il peut faire des démonstrations d'outils informatiques, faire travailler ses stagiaires dans une application partagée ou aller sur internet via le partage du navigateur. Il peut soumettre aux participants des évaluations, des sondages.
- Les participants écoutent et peuvent : poser ou répondre à des questions sur le « chat » ou de vive voix.

MODULE E-LEARNING: MAÎTRISER LES RISQUES LIÉS A UN ENVIRONNEMENT NUMÉRIQUE

Percevoir les principaux risques liés à l'utilisation des outils digitaux

- Comprendre les risques liés au digital : analyse à partir des usages
- Comment gérer ces risques en fonction de leur source : cybercriminalité, parties prenantes, collaborateurs...

- Quelles outils mettre en place, quelles bonnes pratiques adopter : logiciels, usage professionnel et privé, formation...

- Comment communiquer les bonnes pratiques

Une formation sous forme de vidéos et de quizz

- Modalités pédagogiques et techniques : Durée de 20 minutes pour le module. Consultation de vidéos et réponses à des questions en lien vers le contenu

- Accès au module de E-learning via la plateforme 360Learning. Module accessible pendant 1 mois à partir de la réception de l'invitation de connexion