Gestion de l'office

INFORMATIONS

CODE PRODUIT :
GDL324A

PUBLIC CONCERNÉ :
Notaires, collaborateurs référents sécurité informatique, directeurs juridiques, secrétaires

NIVEAU :
Pratique courante

DURÉE :
1,0 jour (7,0 heures)

PRÉREQUIS :
Aucun pré-requis exigé. Toutefois, une implication pratique sur les questions de sécurité informatique vous permettra de suivre cette formation plus confortablement. Nous vous invitons à remplir le quiz de positionnement pour tester vos connaissances.

MODALITÉS D'EXÉCUTION
Formation en présentiel ou Visioformation

MODALITÉS PÉDAGOGIQUES
Type de formation : inter, intra ou commandé
L'animation pédagogique permet de susciter l'engagement des stagiaires et de favoriser l'interactivité avec le formateur
Animation pédagogique ponctuée de questions/réponses entre les stagiaires et le formateur
Mise en œuvre pédagogique par des exemples pratiques et des mises en situation professionnelles illustrant la théorie
Un support de formation est mis à disposition de chaque stagiaire préalablement à la formation de manière dématérialisée

MODALITÉS TECHNIQUES
En présentiel : salle de formation adaptée avec tableaux et vidéoprojecteur ; respect des règles sanitaires et de sécurité d'accueil du public
En visioformation : plateforme de visioconférence adaptée à l'animation pédagogique (interactions orales ou écrites, partage d'écrans et de documents en direct) ; accompagnement technique possible par assistance téléphonique pour la première connexion et la découverte environnementale de la plateforme

MODALITÉS D'ENCADREMENT
Inafon s'assure préalablement à la formation que le formateur dispose des qualités pédagogiques et des compétences techniques d'expertise nécessaires pour dispenser la formation

MODALITÉS DE SUIVI ET APPRÉCIATION DES RÉSULTATS
Emargement par les stagiaires participants et l'intervenant
Feuille d'émargement signée en présentiel ou électroniquement (régularisée par l'édition du rapport des connexions à la plateforme de visioconférence)
Evaluation à chaud à l'issue de la formation :

- Un quiz en ligne est adressé à chaque stagiaire afin de lui permettre d'évaluer ses connaissances et compétences acquises au cours de la formation. Les résultats de l'évaluation restent confidentiels pour chaque stagiaire ;
- Un questionnaire en ligne de satisfaction de fin de formation est adressé à chaque stagiaire (enquête mesurant la qualité organisationnelle et pédagogique de la formation).

REMISE D'UNE ATTESTATION
Une attestation de présence et un certificat de réalisation de formation sont remis à chaque stagiaire à l'issue de la formation

Cyberrisques et continuité d'activité : anticiper pour protéger l'étude notariale, les nouvelles obligations

OBJECTIFS PÉDAGOGIQUES :

A la fin de la formation le participant sera capable de :

- Maîtriser les clés de la gestion de crise sous les aspects métiers, bancaires et assurantiels.
- Savoir rédiger un plan de continuité d'activité
- Identifier les principaux types de fraudes informatiques et s'en prémunir
- Mettre en place un plan d'action en cas de cyber attaque

CONTENU :

PRÉVENIR ET GÉRER UNE CYBERATTAQUE

- Identifier les principales sources de fraudes et les prévenir
- Présentation des risques assurantiels spécifiques et leur couverture
- Mettre en place un plan d'action en cas d'attaque cyber
- Mise en situation

ASSURER LA CONTINUITÉ D'ACTIVITÉ EN CAS DE SINISTRE

- Introduction
- Plan de continuité et reprise d'activité
- Assurer la continuité d'activité
- Atelier – mon PCA
- Bien connaitre sa couverture assurantielle pour une meilleure gestion des risques
- Communiquer avec son référent Banque des Territoires en cas de sinistre

Association INAFON – 16, Rue Etienne Marcel – 75002 Paris créée le 25 février 1972, n°existence : 11750094675 (cet enregistrement ne vaut pas agrément de l'Etat) – Siret : 30838863600174 – TVA Intracommunautaire : FR 96308388636