Cybersécurité et Protection des Données en Comptabilité

Gestion - Administration - Comptabilité

10/06/2026

Public et prérequis

Débutants ou professionnels souhaitant renforcer leurs compétences en cybersécurité appliquée à la comptabilité

Les objectifs

Identifier les principes fondamentaux de la cybersécurité
Mettre en œuvre les bonnes pratiques de protection des accès et des postes
Comprendre et appliquer les fondamentaux du RGPD
Sécuriser les échanges et les transactions comptables
Identifier les principales fraudes comptables pour renforcer la sécurisation des processus
Utiliser les outils et bonnes pratiques de surveillance pour prévenir les risques

Les méthodes pédagogiques et d'encadrement

Alternance d'apports théoriques, de cas pratiques, de mises en situation en lien avec son poste de travail

La formation est animée par des formateurs experts, validés par nos équipes pédagogiques et disposant de 5 à 10 années d'expérience dans leur domaine de compétences

Validation et certification

Attestation de formation

Outils pédagogiques

Apports théoriques, exercices pratiques, documents types.
Salle de formation équipée, maintenue et mise à jour régulièrement au niveau du matériel et logiciel à utiliser

Contenu de la formation

Identifier les principes fondamentaux de la cybersécurité

Identifier les enjeux et les menaces liés à la cybersécurité afin de comprendre les risques spécifiques aux systèmes comptables et financiers.
Reconnaître les principales formes de cyberattaques (phishing, ransomware, usurpation d'identité) pour anticiper les atteintes possibles aux données comptables.
Analyser des cas concrets de failles comptables pour mesurer les conséquences économiques, juridiques et organisationnelles d'une cyberattaque.

Mettre en œuvre les bonnes pratiques de protection des accès et des postes

Mettre en œuvre une gestion sécurisée des mots de passe pour protéger les accès aux logiciels et données comptables.
Appliquer les principes d'authentification forte et de gestion des droits d'accès afin de limiter les risques de consultation ou de modification non autorisée des données

RÉFÉRENCE
GEST0014

CENTRES DE FORMATION
Amiens

DURÉE DE LA FORMATION
2 jours / 14 heures

ACCUEIL PSH
Formation ouverte aux personnes en situation de handicap. Moyens de compensation à étudier avec le référent handicap du centre concerné.

Les + Promeo

• 60 ans d'existence
• Une communauté de 3 100 alternautes
• 24 000 stagiaires formés par an
• 3 500 entreprises qui nous font confiance

• Un accompagnement personnalisé et un contact dédié
• L'expertise professionnelle de tous nos formateurs
• La diversité des diplômes sous accréditation par des partenaires de renom
• Une pédagogie active
• Des infrastructures technologiques et un environnement stimulant

financières.
Assurer la mise à jour et la sécurisation des logiciels comptables pour prévenir les vulnérabilités techniques.
Adopter les bons réflexes face aux emails et pièces jointes suspectes dans le cadre des échanges professionnels comptables.

Comprendre et appliquer les fondamentaux du RGPD

Comprendre les principes clés du RGPD (collecte, traitement, conservation, suppression) pour garantir la conformité du traitement des données comptables.
Identifier les données personnelles présentes dans les documents comptables afin de déterminer les obligations légales applicables.
Appliquer les droits des personnes et les obligations du responsable de traitement dans le cadre de la gestion quotidienne des informations financières.

Sécuriser les échanges et les transactions comptables

Utiliser des protocoles sécurisés (SSL/TLS) pour garantir la confidentialité et l'intégrité des échanges d'informations comptables.
Mettre en œuvre la signature électronique et l'horodatage afin d'assurer la traçabilité et l'authenticité des documents financiers.
Organiser la sauvegarde, l'archivage sécurisé et le plan de reprise d'activité (PRA) pour maintenir la continuité comptable en cas d'incident.
Découvrir les outils de chiffrement des données dans le cadre de la protection des transactions et documents comptables.

Identifier les principales fraudes comptables pour renforcer la sécurisation

Identifier les principales formes de fraude et de manipulation comptable afin de reconnaître les menaces pesant sur la fiabilité des états financiers.
Repérer les techniques de fraude numérique (faux documents, altération de fichiers) pour détecter les anomalies dans les enregistrements comptables.
Mettre en place des contrôles internes adaptés dans le but de limiter les risques de fraude et d'erreur volontaire

Utiliser les outils et bonnes pratiques pour prévenir les risques

Utiliser des outils de contrôle et d'audit comptable automatisé pour repérer les anomalies et renforcer la fiabilité des comptes.
Sensibiliser les équipes comptables à la cybersécurité pour développer une culture de vigilance numérique.
Appliquer une procédure d'alerte et une gestion de crise pour réagir efficacement en cas d'incident de sécurité.
Participer à des quiz et mises en situation afin de consolider les réflexes professionnels en matière de cybersécurité.

Modalité d’évaluation

L'évaluation des acquis est réalisée tout au long de la formation au travers des cas pratiques et exercices proposés.