

PROGRAMME DE FORMATION

Sécuriser son organisme de formation : données, accès et fraude

Protégez concrètement l'activité de votre organisme de formation face aux risques de piratage, de fraude et de perte de données. Cette formation vous permet de prioriser vos actifs sensibles, de sécuriser vos accès et de réduire les vulnérabilités les plus fréquentes.

Repartez avec des actions directement applicables : registre des traitements, règles de conservation, procédure de sauvegarde et premiers réflexes en cas d'incident, même sans service informatique dédié.

Dirigeants, responsables administratifs, référents Qualiopi et équipes des organismes de formation.

TAUX DE SATISFACTION

Non disponible

TAUX DE RÉUSSITE

Non disponible

01 OBJECTIFS DE LA FORMATION

- Identifier les données et les comptes critiques de son organisme et les hiérarchiser par niveau de risque
- Mettre en place l'authentification multifacteur et un gestionnaire de mots de passe sur ses accès professionnels
- Reconnaître les tentatives de fraude ciblant spécifiquement les organismes de formation
- Établir le registre des traitements de son organisme et fixer des durées de conservation cohérentes avec ses obligations de preuve
- Formaliser une procédure de sauvegarde et de réaction en cas d'incident

02 INFORMATIONS CONCERNANT LA FORMATION

PUBLIC VISÉ	Dirigeants, responsables administratifs, référents Qualiopi et équipes des organismes de formation.
DURÉE	7,00 h — 1 j
INTERVENANT	Consultant en cybersécurité et protection des données.
ÉQUIPEMENTS NÉCESSAIRES	Ordinateur connecté à Internet, messagerie professionnelle et accès aux outils de l'organisme.
PRÉREQUIS	Être en poste au sein d'un organisme de formation.
MÉTHODES D'ÉVALUATION	Diagnostic initial, quiz interactifs, exercices pratiques et évaluation finale sur cas d'usage, avec 60 % de réussite minimum.

MÉTHODES PÉDAGOGIQUES

MOYENS PÉDAGOGIQUES

Educta - 12 Parc Dromel 13009 Marseille

06 66 16 35 29 | contact@educta.fr | <https://educta.fr>

Société par Actions Simplifiée Unipersonnelle (SASU) au capital de 10.00€ | SIRET : 99915414900010 | APE : 85.59A

- 1 Apports ciblés illustrés par des situations propres aux organismes de formation
 - 2 Diagnostic guidé des données, comptes et outils utilisés par les participants
 - 3 Études de cas de fraude, d'hameçonnage et d'incidents de sécurité
 - 4 Travaux individuels et échanges en petit groupe sur des modèles opérationnels
 - 5 Mises en situation à distance sur la détection d'emails frauduleux
 - 6 Quiz interactifs et restitution collective des plans d'action
- 1 Support de cours PDF téléchargeable
 - 2 Grille de cartographie des données et comptes critiques
 - 3 Modèle de registre des traitements et tableau des durées de conservation
 - 4 Fiche mémo sur les mots de passe, le MFA et les signaux de fraude
 - 5 Modèle de procédure de sauvegarde et de réaction à incident
 - 6 Liste de ressources gratuites et contacts utiles

MODALITÉS ET CONDITIONS D'ACCÈS

Mise en place d'une session de formation pour vos collaborateurs sous 30 jours à compter de la confirmation d'inscription.

03 ACCESSIBILITÉ

Notre référent handicap est disponible pour vous accompagner et adapter le programme selon vos besoins spécifiques. Nous mettons en œuvre tous les moyens nécessaires pour garantir l'accessibilité de nos formations aux personnes en situation de handicap. N'hésitez pas à nous contacter pour étudier ensemble les adaptations possibles.

RÉFÉRENT HANDICAP Imad-Eddine Sellal · contact@educta.fr · 06 66 16 35 29

04 CONDITIONS TARIFAIRES

LIBELLÉ	Tarif catalogue
FORMAT COMMERCIAL	INTER
UNITÉ DE FACTURATION	Par apprenant
MONTANT	499,00 € HT

Organisation d'une session de formation sous 30 jours à compter de la confirmation de votre inscription.

05

CONTENU DE LA FORMATION

Cartographier son patrimoine numérique

- Identifier les données sensibles de l'organisme
- Recenser les comptes, outils et supports utilisés
- Évaluer les impacts d'une perte ou d'un accès indu
- Hiérarchiser les actifs selon leur niveau de risque
- Construire une feuille de route de sécurisation

Verrouiller les accès

- Diagnostiquer les pratiques d'accès existantes
- Organiser des mots de passe uniques et robustes
- Utiliser un gestionnaire de mots de passe
- Mettre en œuvre l'authentification multifacteur
- Gérer les droits, départs et accès partagés

Reconnaître les attaques qui ciblent les organismes de formation

- Examiner les scénarios de fraude propres au secteur
- Repérer les indices d'un email d'hameçonnage
- Vérifier une demande de paiement ou de RIB
- Détecter les faux dossiers, convocations et liens
- Appliquer les réflexes de signalement et d'alerte

Protéger les données des stagiaires

- Identifier les traitements de données personnelles
- Élaborer le registre des traitements de l'organisme
- Organiser les durées de conservation des preuves
- Sécuriser le partage des documents stagiaires
- Encadrer les droits d'accès aux données personnelles

Sauvegarder et réagir

- Appliquer la règle 3-2-1 sans budget informatique
- Organiser des sauvegardes adaptées aux outils utilisés
- Tester une restauration de données et de documents
- Assurer une session si le poste de travail est hors service
- Exécuter les premières actions dans les 24 heures
- Identifier les obligations et ressources mobilisables

06

NOUS CONTACTER

TÉLÉPHONE	06 66 16 35 29
EMAIL	contact@educta.fr
HORAIRESD'OUVERTURE	Lundi au Vendredi de 9h00 à 17h00
ADRESSE	12 Parc Dromel 13009 Marseille
SITE WEB	educta.fr