

CYBER : PROTÉGER SA COLLECTIVITÉ AU QUOTIDIEN

DESCRIPTION

Face à des cybermenaces de plus en plus présentes, les élus ont un rôle clé pour protéger leur collectivité et garantir la continuité du service public. Grâce à des cas concrets et des mises en situation, cette formation vous donnera les clés pour anticiper les risques, prendre les bonnes décisions et agir avec confiance.



1 jour / 7h



Présentiel



Élus

PUBLIC CIBLE

Tout élu souhaitant connaître les clés pour protéger sa collectivité concernant la cybersécurité.

LIEUX et DATES

Lieu : Dijon (21)

Dates : Consultez votre compte élu.

PARTICIPANTS

Mini 5 - maxi 15

OBJECTIFS

À l'issue de la formation, le stagiaire sera capable de :

- Distinguer les principaux types de risques cyber susceptibles d'affecter une collectivité.
- Identifier les impacts potentiels d'une cyberattaque sur les services publics et les usagers.
- Définir le rôle des élus dans la prévention et la gestion des risques numériques.
- Identifier les bonnes pratiques à promouvoir au sein de leur collectivité.
- Déterminer les actions prioritaires à mettre en œuvre lors d'une crise cyber.

PRÉREQUIS

Savoir utiliser à minima les outils de bureautique.

Prérequis matériel : avoir un ordinateur portable ou à défaut en faire part à l'organisme de formation.

LES +

- ▷ Identifiez les principales menaces numériques pour votre collectivité.
- ▷ Adoptez les bons réflexes pour protéger vos données et vos systèmes.
- ▷ Renforcez votre vigilance face aux usages numériques du quotidien.

CONTENU DE LA FORMATION

1. Comprendre les risques cyber pour les collectivités
 - Eléments de contexte.
 - Panorama des risques cyber.
 - Pourquoi les collectivités sont-elles des cibles potentielles ?
2. L'impact d'une cyberattaque
 - Conséquences opérationnelles
 - Conséquences financières
 - Conséquences sur les usagers
 - Conséquences sur les élus et la collectivité
3. Le rôle des élus dans la cybersécurité
 - La cybersécurité : un enjeu de gouvernance
 - Pourquoi le sujet dépasse la seule DSI.
 - Un risque qui peut affecter la continuité du service public.
 - Présentation de NIS2.
 - Les responsabilités des élus
 - Définition des orientations
 - Arbitrages budgétaires
 - Suivi des risques
 - Protection des données
 - Adapter l'approche selon la taille de la collectivité
4. Les bonnes pratiques
 - Les questions à poser régulièrement
 - Les fondamentaux
 - Sensibilisation des agents
 - Gestion des prestataires
 - Protection des données personnelles
5. Réagir face à une attaque – Atelier de mise en situation
 - Les premières heures d'une attaque
 - Organisation de la cellule de crise
 - Communication de crise
 - Les acteurs à mobiliser

INSCRIPTION

Mail : formation@arnia-bfc.fr

Retrouvez les formations programmées :

<https://arnia-bfc.fr/calendrier-des-formations>

Demandez une formation : Inscription via votre compte élu.

<https://www.moncompteformation.gouv.fr/espace-prive/html/#/aide?publicCible=ELU>



CYBERSECURITÉ

Cyber
sécurité

MÉTHODE PÉDAGOGIQUES ET MOYENS TECHNIQUES

Apports théoriques, exercices pratiques, échanges et partages d'expériences, démonstration d'exemples appliqués à des situations réelles, analyses de situations rencontrées par les participants, jeux, exercices de réflexion individuels ou en groupes.

LES INTERVENANTS

Nos intervenants sont des experts dans leurs domaines d'intervention. Leur expérience en conseil et formation auprès des apprenants est le fruit de plusieurs années d'exercice dans leurs domaines. Ils évoluent et adaptent leurs interventions en fonction des besoins des apprenants.

SUIVI ET ÉVALUATION

En amont de la formation : Évaluation individuelle de la candidature - Évaluation des attentes et des besoins des stagiaires - Évaluation du niveau des stagiaires.

En fin de formation : Questionnaire d'évaluation des acquis - Évaluation de la satisfaction des stagiaires - Feuilles de présence signées des participants et du formateur par demi-journée.

Après la formation : Attestation individuelle de fin de formation et Open badge Questionnaire de satisfaction à froid.

