

Cybersécurité - Gouvernance

CYBERGOUV

Cette formation offre une vue d'ensemble des concepts clés et des enjeux contemporains de la cybersécurité. Elle met l'accent sur le rôle crucial de la gouvernance dans ce domaine et explore le développement de politiques de sécurité et de normes.

Présentiel - Synchrone

Public Visé

Dirigeants, DSI, chefs de projet, développeurs, architectes et toute personne souhaitant comprendre la cybersécurité.



Pré Requis

Avoir des connaissances en informatique et en cybersécurité.

Objectifs pédagogiques et d'évaluation

Mettre l'accent sur l'importance de la gouvernance pour garantir la sécurité des informations, les principes fondamentaux de la gouvernance en cybersécurité, y compris les normes, les politiques et les meilleures pratiques

Identifier les risques liés à la cybersécurité dans le contexte de la gouvernance et mettre en oeuvre des stratégies efficaces de gestion des risques

Élaborer et mettre en oeuvre des politiques de conformité dans un cadre de gouvernance

Méthodes pédagogiques

Beaucoup de tests et d'exemples concrets en lien direct avec les besoins des participants

Des techniques directement mobilisables dans le cadre de leurs fonctions

Formation axée sur la mise en pratique

Méthode participative

Alternance de cours et d'exercices dirigés ou en autonomie

Travaux individuels et corrections collectives

Évaluation croisée et partage de bonnes pratiques

Parcours pédagogique

Compréhension approfondie de la cybersécurité

Les participants auront une connaissance approfondie des concepts clés de la cybersécurité, y compris les menaces, les vulnérabilités et les méthodes de protection.

Compétences en gouvernance de la cybersécurité

Les apprenants seront capables d'élaborer des politiques de sécurité et des normes conformes aux meilleures pratiques et aux réglementations en vigueur.

Gestion des risques

Les participants seront en mesure d'identifier, évaluer et gérer les risques liés à la cybersécurité dans un environnement organisationnel.

Conformité réglementaire

Comprendre les exigences réglementaires et normatives en matière de cybersécurité, et la manière de garantir la conformité de l'organisation.

Planification stratégique en cybersécurité

Développer des stratégies à long terme pour renforcer la posture de sécurité de l'organisation.

Sensibilisation des parties prenantes

Acquérir des compétences en communication pour sensibiliser les différentes parties prenantes à l'importance de la cybersécurité.

Gestion des incidents

Être prêt à mettre en oeuvre des protocoles de communication efficaces en cas d'incidents de cybersécurité.

Moyens pédagogiques

1 ordinateur par stagiaire

Salle de formation claire, climatisée et spacieuse

Tableau blanc

Vidéo projecteur

Support de cours

Qualification Intervenant-e-s

Formateur - Consultant expert en cybersécurité

Version : V1 - CYBERGOUV-20260128

STRATEGIE INFORMATIQUE - Numéro de déclaration d'activité (ne vaut pas agrément de l'état) : 95970120697

Stratégie Informatique

Guadeloupe : Immeuble la Coupole, Grand-Camp 97142 ABYMES Tél : 05 90 83 06 18 Fax : 05 90 83 46 71

Martinique : Immeuble Sera n°6, Zone de Manhity 97232 LAMENTIN Tél : 05 96 57 40 20 Fax : 05 96 51 60 53

SARL AU CAPITAL DE 7775€ - SIRET 352 717 193 00044-APE 6202 A



Méthodes et modalités d'évaluation

Evaluation diagnostique en amont : questionnaire d'auto-positionnement et recueil des attentes & besoins – Tour de table -
Evaluation formative en cours de formation : exercices - Evaluation sommative en fin de formation : exercice/QCM - Bilan individuel des compétences acquises – Attestation de fin de formation -
Questionnaire de satisfaction à chaud - Questionnaire de satisfaction à froid envoyé 15 jours après la formation pour assurer le suivi post formation

Modalités d'accessibilité handicap

Nos formations sont accessibles aux personnes en situation de handicap et aux besoins spécifiques. Une étude personnalisée avec notre référente handicap, permettra d'adapter les moyens pédagogiques, techniques ou organisationnels.



Durée

21.00 Heures

3

Jours

Effectif

De 3 à 8 Personnes