Formations
CYBERSÉCURITÉ
Parcours qualifiant 100% SUR-MESURE

24

Sensibilisation à la cybersécurité ☐
Cybersécurité des tâches administratives ☐
DPO - Délégué à la Protection des Données ☐

Je définis mon besoin de montée en compétences et mon projet de formation en cinq questions :

01 - Quelles compétences sont cruciales pour mon poste actuel ou futur ?
J'identifie les compétences spécifiques nécessaires pour exceller dans mon poste actuel ou atteindre mes objectifs de carrière futurs. J'inclut à la fois les compétences techniques et les compétences non techniques (soft skills).

02 - Quelles sont mes lacunes actuelles en compétences ?
J'évalue honnêtement mon niveau actuel de compétence dans les domaines clés de mon poste. J'identifie les domaines où j'ai évalué (ou reçu des retours indiquant) un besoin d'amélioration.

03 - Quels sont les objectifs de cette montée en compétences ?
Je définis clairement pourquoi j'ai besoin de développer ces compétences. Pour améliorer votre performance actuelle, préparer une promotion, adapter mes compétences aux nouvelles technologies ou processus, ou répondre à des attentes spécifiques de mon service, de mon entreprise ?

04 - Quelle est la méthode de formation la plus adaptée à mon style d'apprentissage et à mes contraintes ?
Je réfléchis à la manière dont j'apprends le mieux (présentiel, en ligne, mixte). Je considère également mes contraintes de temps et de disponibilité pour suivre une formation.

05 - Quels sont les bénéfices attendus de cette formation pour moi et pour l'entreprise ?
J'anticipe les avantages concrets quemoi et mon entreprise pouvons tirer de cette montée en compétences. J'inclus une meilleure performance, une plus grande efficacité, une plus grande satisfaction au travail, ou des opportunités de carrière accrues.

En renseignant ces questions, je serai en mesure de définir de manière précise et ciblée projet de formation, ce qui vous aidera à valider le programme de formation le plus adapté pour moi.

AVAMA
Training for Actions

AVAMA

CYBERSÉCURITÉ SENSIBILISATION

TRAINING FOR ACTIONS

Réf : 00000 - 00

Catégorie : Cybersécurité

MODALITÉS PRATIQUES

Dates
Sur demande
Sous réserve d'un nombre suffisant de participants

Lieu
À distance depuis votre poste informatique ou en présentiel

Durée et rythme
14 heures - 2 jours
9h00 - 12h30
13h30 - 17h00

Tarif
selon devis - Nous consulter

Accès à la formation
2 jours au plus tard avant le début de la formation, sous réserve de réception du dossier d'inscription complet

Accessibilité
Accès des publics en situation de handicap en présence d'un référent handicap par campus

Type de formation
Collectif

Individualisation
Oui

Langue d'enseignement
Français

PUBLIC CIBLE
Toute personne utilisant un outil informatique connecté.

OBJECTIFS DE LA FORMATION
Identifier les menaces pesant sur votre SI. Comprendre les enjeux de la sécurité informatique. La formation cybersécurité sensibilisation présente une approche globale pour maîtriser la sécurité du système d'information vis-à-vis des risques de cyberattaques.

PRÉREQUIS & NIVEAU D'ENTRÉE
Cette formation ne nécessite pas de prérequis.

LES POINTS FORTS DE LA FORMATION
Identifier et analyser les risques de cyberattaque dans l'entreprise.

CETTE FORMATION
Est animée par un formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et testées et approuvées par l'éditeur et par AVAMA. La formation bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

MODALITÉS D'ÉVALUATION
Cette formation fait l'objet d'une évaluation formative.

MATÉRIEL NÉCESSAIRE
En cas de formation sur site externe à AVAMA, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation.

AVAMA

CYBERSÉCURITÉ SENSIBILISATION

100 %
des clients recommandent les formations AVAMA en 2023 !

CERTIFICAT

QUALIANOR Organisme certifié QUALIOPI Référentiel National Qualité (RNQ)

ILS NOUS FONT CONFIANCE

Epsyl-Alcen, TotalEnergies, Conseil Elysées Finances, Breveco, Cohérence RH...

POUR COMMENCER

Votre contact :

Serge MAILLET
smaillet@avama.org
06.07.04.25.97

PROGRAMME

1 - Autodiagnostic

- Identifier les postes de travail et leurs usages (du mot de passe au stockage de données)
- Différencier Vulnérabilité/Menaces/Attaques
- Identifier et analyser les risques existants

2 - Périmètre de la cybersécurité

- Définitions, caractéristiques, enjeux
- Les 4 risques : sabotage, espionnage, mise en danger de l'image, cybercriminalité
- Normes ISO/IEC 27000

3 - Menaces et vulnérabilités

- Liste des menaces et vulnérabilité (fishing, fraude au président…)
- Réflexion sur les moyens de les réduire

4 - Management de la sécurité

- PRA/PCA
- Gestion des risques

5 - Mise en situation

- Familiarisation avec les réflexes sécurité

CYBERSÉCURITÉ DES TÂCHES ADMINISTRATIVES

AVAMA

TRAINING FOR ACTIONS

Réf : 00000 - 00

Catégorie : Cybersécurité

MODALITÉS PRATIQUES

Dates
Sur demande
Sous réserve d'un nombre suffisant de participants

Lieu
À distance depuis votre poste informatique ou en présentiel

Durée et rythme
14 heures - 2 jours
9h00 - 12h30
13h30 - 17h00

Tarif
selon devis - Nous consulter

Accès à la formation
2 jours au plus tard avant le début de la formation, sous réserve de réception du dossier d'inscription complet

Accessibilité
Accès des publics en situation de handicap en présence d'un référent handicap par campus

Type de formation
Collectif

Individualisation
Oui

Langue d'enseignement
Français

PUBLIC CIBLE
Tout collaborateur d'entreprise utilisant des moyens informatiques connectés.

OBJECTIFS DE LA FORMATION
Identifier les menaces pesant sur votre SI. Comprendre les enjeux de la sécurité informatique. La formation cybersécurité sensibilisation présente une approche globale pour maîtriser la sécurité du système d'information vis-à-vis des risques de cyberattaques.

PRÉREQUIS & NIVEAU D'ENTRÉE
Cette formation ne nécessite pas de prérequis.

LES POINTS FORTS DE LA FORMATION
Identifier et analyser les risques de cyberattaque dans l'entreprise.

CETTE FORMATION
Est animée par un formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et testées et approuvées par l'éditeur et par AVAMA. La formation bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

MODALITÉS D'ÉVALUATION
Cette formation fait l'objet d'une évaluation formative.

MATÉRIEL NÉCESSAIRE
En cas de formation sur site externe à AVAMA, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation.

AVAMA

CYBERSÉCURITÉ DES TÂCHES ADMINISTRATIVES

100 %
des clients recommandent les formations AVAMA en 2023 !

CERTIFICAT

QUALIANOR Organisme certifié QUALIOPI Référentiel National Qualité (RNQ)

ILS NOUS FONT CONFIANCE

Epsyl-Alcen, TotalEnergies, Conseil Elysées Finances, Breveco, Cohérence RH...

POUR COMMENCER

Votre contact :

Serge MAILLET
smaillet@avama.org
06.07.04.25.97

PROGRAMME

1 - Autodiagnostic

- Identifier les postes de travail et leurs usages (du mot de passe au stockage de données)
- Différencier Vulnérabilité/Menaces/Attaques
- Identifier et analyser les risques existants

2 - Périmètre de la cybersécurité

- Définitions, caractéristiques, enjeux
- Les 4 risques : sabotage, espionnage, mise en danger de l'image, cybercriminalité
- Protéger les données administratives

3 - Menaces et vulnérabilités

- Liste des menaces et vulnérabilité (fishing, fraude au président…)
- Réflexion sur les moyens de les réduire

4 - Management de la sécurité

- PRA/PCA
- Gestion des risques

5 - Mise en situation

- Familiarisation avec les réflexes sécurité

DPO (DÉLÉGUÉ À LA PROTECTION DES DONNÉES)

AVAMA

TRAINING FOR ACTIONS

Réf : 00000 - 00

Catégorie : Cybersécurité

MODALITÉS PRATIQUES

Dates
Sur demande
Sous réserve d'un nombre suffisant de participants

Lieu
À distance depuis votre poste informatique ou en présentiel

Durée et rythme
35 heures - 5 jours
9h00 - 12h30
13h30 - 17h00

Tarif
selon devis - Nous consulter
(Sans la certification)

Accès à la formation
2 jours au plus tard avant le début de la formation, sous réserve de réception du dossier d'inscription complet

Accessibilité
Accès des publics en situation de handicap en présence d'un référent handicap par campus

Type de formation
Collectif

Individualisation
Oui

Langue d'enseignement
Français

Ouvre à la certification de compétences de DPO selon référentiel CNIL.

PUBLIC CIBLE
Tout membre d'une organisation.

OBJECTIFS DE LA FORMATION
Acquérir les compétences nécessaires à la fonction de DPO.
Comprendre les enjeux du RGPD.
Identifier les impacts et les adaptations nécessaires pour son SI (système d'information).
Se préparer activement à la certification.

PRÉREQUIS & NIVEAU D'ENTRÉE
Cette formation ne nécessite pas de prérequis.

LES POINTS FORTS DE LA FORMATION
S'ouvrir à la certification DPO.

CETTE FORMATION
Est animée par un formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et testées et approuvées par l'éditeur et par AVAMA. La formation bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

MODALITÉS D'ÉVALUATION
Cette formation fait l'objet d'une évaluation formative et en fin de formation, par un questionnaire d'auto-évaluation conforme aux attendus de la certification DPO. Attestation de suivi de formation.

MATÉRIEL NÉCESSAIRE
En cas de formation sur site externe à AVAMA, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation.

AVAMA

DPO (DÉLÉGUÉ À LA PROTECTION DES DONNÉES)

100 %
des clients recommandent les formations AVAMA en 2023 !

CERTIFICAT

QUALIANOR Organisme certifié QUALIOPI Référentiel National Qualité (RNQ)

ILS NOUS FONT CONFIANCE

Epsyl-Alcen, TotalEnergies, Conseil Elysées Finances, Breveco, Cohérence RH...

POUR COMMENCER

Votre contact :

Serge MAILLET
smaillet@avama.org
06.07.04.25.97

PROGRAMME

1 - Le délégué à la protection des données (DPO)

- Pourquoi un DPO ?
- Rôle du DPO
- Certification DPO

2 - La protection des données à caractère personnel

- Minimisation et exactitude
- Licéité, loyauté, finalités
- Protection des données
- Communication des données

3 - Les grands principes du RGPD

- Transparence et information
- Durée de conservation
- Rôle de la CNIL
- Registre

4 - Outils de mise en conformité RGPD

- Transfert hors UE
- Accountability
- Notification de violation
- Gestion des demandes
- Relation aux sous-traitants
- Privacy by design

5 - Risques, impacts et sécurité

- Formation du personnel
- BCR et CCT
- Procédures
- PIA
- Chiffrement