CYBERSECURITE

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

Tarif et durée
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 2024 !

CERTIFICAT

QUALIANOR
Organisme certifié
QUALIOPI®
Référentiel National Qualité (RNQ)

ILS NOUS FONT CONFIANCE

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

POUR COMMENCER

Serge MAILLET
smaillet@avama.org
06.07.04.25.97

PROGRAMME

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

Périmètre de la cybersécurité

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

Menaces et vulnérabilités

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

Management de la sécurité

- PRA/PCA
- Gestion des risques

Mise en situation

- Familiarisation avec les réflexes sécurité

Pour aller plus loin...
Introduction à la cybersécurité, cybersécurité des tâches administratives

AVAMA

CYBERSÉCURITÉ
INTRODUCTION

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

Tarif et durée
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
INTRODUCTION

100 %
des clients recommandent les formations AVAMA en 2024 !

CERTIFICAT

QUALIANOR
Organisme certifié
QUALIOPI®
Référentiel National Qualité (RNQ)

ILS NOUS FONT CONFIANCE

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

POUR COMMENCER

Serge MAILLET
smaillet@avama.org
06.07.04.25.97

PROGRAMME

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

Périmètre de la cybersécurité

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

Menaces et vulnérabilités

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

Management de la sécurité

- PRA/PCA
- Gestion des risques

Mise en situation

- Familiarisation avec les réflexes sécurité

Pour aller plus loin...
EBIOS, DPO, cybersécurité des tâches administratives

CYBERSÉCURITÉ DES TÂCHES ADMINISTRATIVES

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

Tarif et durée
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 2024 !

CERTIFICAT

QUALIANOR Organisme certifié QUALIOPI® Référentiel National Qualité (RNQ)

ILS NOUS FONT CONFIANCE

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

POUR COMMENCER

Serge MAILLET
smaillet@avama.org
06.07.04.25.97

PROGRAMME

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

Périmètre de la cybersécurité

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

Menaces et vulnérabilités

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

Management de la sécurité

- PRA/PCA
- Gestion des risques

Mise en situation

- Familiarisation avec les réflexes sécurité

Pour aller plus loin...
Introduction à la cybersécurité, EBIOS, DPO

AVAMA

DPO (DÉLÉGUÉ À LA PROTECTION DES DONNÉES)

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

Tarif et durée
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 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
Ouvre à la certification de compétences de DPO selon référentiel CNIL.

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

DPO (DÉLÉGUÉ À LA PROTECTION DES DONNÉES)

100 %
des clients recommandent les formations AVAMA en 2024 !

CERTIFICAT

QUALIANOR
Organisme certifié
QUALIOPI®
Référentiel National Qualité (RNQ)

ILS NOUS FONT CONFIANCE

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

POUR COMMENCER

Serge MAILLET
smaillet@avama.org
06.07.04.25.97

PROGRAMME

Le délégué à la protection des données (DPO)

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

La protection des données à caractère personnel

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

Les grands principes du RGPD

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

Outils de mise en conformité RGPD

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

Risques, impacts et sécurité

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

Pour aller plus loin...
Certification de compétences de DPO selon le référentiel CNIL.

METTRE EN OEUVRE EBIOS

EXPRESSION DES BESOINS ET IDENTIFICATION DES OBJECTIFS DE SECURITÉSENSIBILISATION DU PERSONNEL

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

Tarif et durée
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

Direction (ou décideurs ayant le bon niveau de délégation) ; Responsable de la sécurité des systèmes d'information (RSSI) ou Responsable de la sécurité numérique du périmètre de l'étude ; Directeur des systèmes d'information (DSI) et/ou responsable informatique du périmètre de l'étude, Responsable qualité.

OBJECTIFS DE LA FORMATION

Connaître les concepts, approches, méthodes et techniques associés à un processus de gestion des risques efficace conforme à la norme ISO/CEI 27005
Savoir interpréter les exigences de la norme ISO/CEI 27001 dans le cadre du management du risque de la sécurité de l'information
Maîtriser les étapes de la méthode EBIOS afin de poursuivre l'achèvement des études
Acquérir les compétences nécessaires afin de mener une étude EBIOS et en analyser et restituer les résultats.
Animer des ateliers de sensibilisation auprès d'un public de salariés non IT

PRÉREQUIS & NIVEAU D'ENTRÉE

Connaitre le guide d'hygiène sécurité de l'ANSSI (site de l'ANSSI)

LES POINTS FORTS DE LA FORMATION

Un programme étudié pour permettre aux participants de préparer le passage de la certification dans les meilleures conditions.

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.

METTRE EN OEUVRE EBIOS

EXPRESSION DES BESOINS ET IDENTIFICATION DES OBJECTIFS DE SECURITÉSENSIBILISATION DU PERSONNEL

100 %
des clients recommandent les formations AVAMA en 2024 !

CERTIFICAT

QUALIANOR Organisme certifié QUALIOPI® Référentiel National Qualité (RNQ)

ILS NOUS FONT CONFIANCE

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

POUR COMMENCER

Serge MAILLET
smaillet@avama.org
06.07.04.25.97

PROGRAMME

Jour 1 :

Les bases

- Echanges interactifs
- Fondamentaux de la gestion des risques
- Vraisemblance et gravité du risque
- Evaluation d'un risque
- Fondamentaux de la sécurité numérique
- Méthode EBIOS et son vocabulaire

Approfondissement

- Cadrage et RACI
- Périmètre métier et technique
- Evènements et impact
- Socle de sécurité
- Sources du risque

Atelier articulé sur la réalité du périmètre de chacun

- Scénario stratégique et scénario opérationnel
- Cartographier l'écosystème
- Traitement du risque
- Documenter le risque
- Echanges et cas pratiques

Conception et prévision de déploiement d'atelier de sensibilisation

- Qu'est-ce qu'un atelier game ?
- Comment le concevoir ?
- Quels outils ?
- Animer
- Construire un REX dans une démarche d'amélioration continue

Pour aller plus loin...
AMDEC, motivation des salariés, animation de groupe.