CYBERSÉCURITÉ

Sensibilisation à la cybersécurité

OBJECTIF : **être vigilant face aux risques de cyberattaque.**

Compétences développées

- Connaitre les enjeux de sécurité des SI ;
- Comprendre la logique de risque en cybersécurité ;
- Connaître les méthodes employées par les acteurs malveillants et les cyberattaquants (informatique, actions physiques, manipulation des membres) ;
- Appliquer les règles d'hygiène informatique ;
- Réagir en cas d'urgence.

Références

Guide d'hygiène informatique de l'ANSSI – édition 2017 ; Référentiel pédagogique du Service de l'Information, Stratégique et de la Sécurité Economique (SISSE).

Contenu

Heure 1 - Enjeux de cybersécurité du monde naval :

- Systèmes d'information maritimes et industriels ;
- Evaluation des impacts sur la sécurité et la sûreté maritime ;
- Scénarios type ;
- Environnement juridique ;
- Normes applicables en général et dans le milieu naval.

Heure 2 - Panorama des menaces :

- La cybercriminalité : moyens et objectifs, vulnérabilités, menace, attaque, typologie des tactiques malveillantes ;
- Ingénierie sociale – environnement international ;
- Vulnérabilités du navire : aujourd'hui et demain ;
- Évaluation de la probabilité.

Heure 3 - Hygiène informatique :

- Maîtriser les systèmes intégrés et périphériques ;
- Mettre à jour les configurations en sécurité ;
- Surveiller la sous-traitance et la maintenance ;
- Fiabiliser les contrôles d'accès ;
- Réagir en cas d'urgence.

Taux de satisfaction : 4,3/5 sur la période 2021-2022

Formation en ligne et en présentiel

DURÉE : 3 heures

LANGUE : français

LIEU : dans nos locaux de Brest, Toulon et dans toute ville ou pays. Ou sur la plateforme 360 E-Learning pour la formation en ligne.

MÉTHODES PÉDAGOGIQUES : magistral 80 % - pratique 20 %

ÉVALUATION : quizz en fin de chaque module

PRÉREQUIS : aucun

HANDICAP : signaler lors de l'inscription

ATTESTATION : individuelle en français

PRIX : 150 € en inter-entreprise
450 € en intra-entreprise

Management de la cybersécurité pour TPE/PME

OBJECTIF : **organiser et piloter la cybersécurité dans son organisation.**

Compétences développées

- Maîtriser les enjeux de cybersécurité pour l'entreprise ;
- Conduire une analyse de risques ;
- Identifier et utiliser les modes de protection des informations sensibles sur les différents réseaux ;
- Rédiger la politique SSI et la charte informatique ;
- Animer la cybersécurité ;
- Impliquer les collaborateurs ;
- Réagir et résister en cas d'incident.

Formation destinée aux collaborateurs souhaitant devenir référent en cybersécurité dans leur entreprise ou service.

Références

Référentiel pédagogique du Service de l'Information, Stratégique et de la Sécurité Economique (SISSE) - Tronc commun.

Contenu

- Enjeux et définitions en cybersécurité ;
- Typologie de la cybercriminalité ;
- Panorama des menaces et des attaques ;
- Aspects juridiques ;
- Élaboration d'une réponse globale par la définition de la politique de cybersécurité ;
- Analyse des risques ;
- Principes d'hygiène informatique ;
- Réactions en cas d'incidents ;
- Maîtrise de l'image et de la communication ;
- Évaluation de l'organisation interne ;
- Réactions en cas de cyberattaque.

Formation en présentiel

DURÉE : 1 jour - 8 heures

LANGUE : français

LIEU : dans nos locaux de Brest, Toulon et dans toute ville ou pays

MÉTHODES PÉDAGOGIQUES : magistral 70 % - pratique 30%

ÉVALUATION : Quizz en fin de session

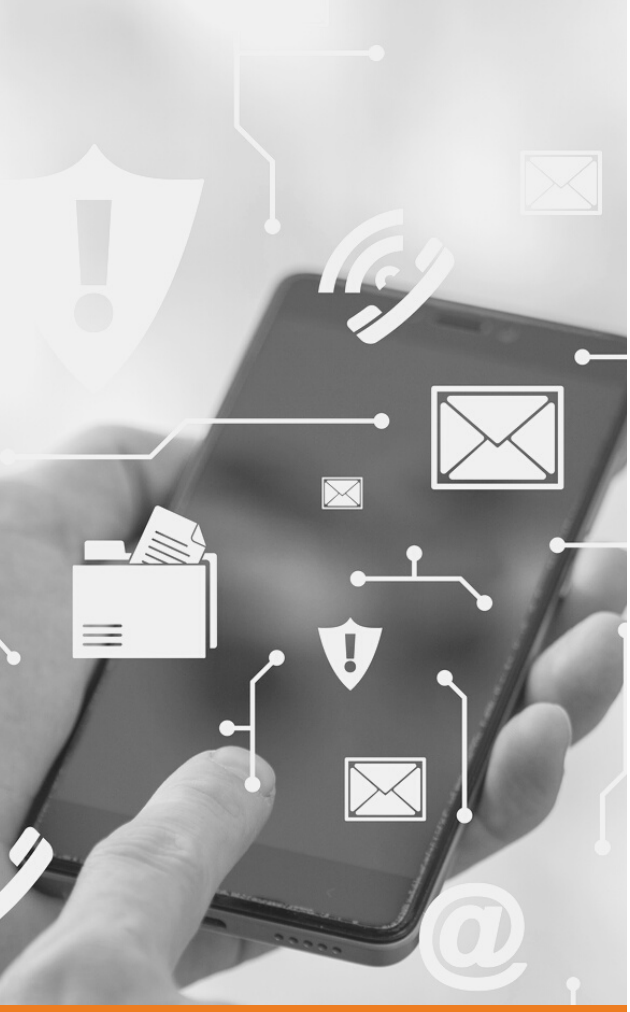
PRÉREQUIS : aucun

HANDICAP : signaler lors de l'inscription

ATTESTATION : individuelle en français

PRIX : 700 € par stagiaire en inter-entreprise
1 600 € par groupe en intra-entreprise

Taux de satisfaction : 4/5 sur la période 2021/2022



Le RGPD dans les TPE/PME

OBJECTIF : **piloter la conformité avec le Réglement Général pour la Protection des Données (RGPD) au sein d'une TPE/PME.**

Compétences développées

- Comprendre les obligations liées au Règlement Général pour la Protection des Données Personnelles (RGPD) ;
- Déployer et entretenir la conformité de son organisation avec le RGPD ;
- Élaborer, mettre en œuvre et entretenir les mesures de cybersécurité dans le cadre de la protection des données personnelles.

Formation destinée aux personnes désignées comme déléguées à la protection des données dans le cadre de la mise en œuvre du RGPD.

Références

Guide d'hygiène informatique de l'ANSSI, règlement européen pour la protection des données personnelles.

Contenu

- Principes généraux de la protection des données personnelles ;
- Présentation du règlement et de la législation française ;
- Respect des droits des personnes ;
- Évaluation des risques pour les données ;
- Processus de mise en conformité ;
- Typologie des menaces sur les données ;
- Politique de protection des données ;
- Hygiène informatique ;
- Réaction en cas d'incident.

Formation en présentiel

DURÉE : 2 jours

LANGUE : français

LIEU : dans nos locaux de Brest, Toulon et dans toute ville

MÉTHODES PÉDAGOGIQUES : magistral 70 % - pratique 30 %

ÉVALUATION : quizz en fin de chaque module

PRÉREQUIS : aucun

HANDICAP : signaler lors de l'inscription

ATTESTATION : individuelle en français

PRIX : 700 € en inter-entreprise
Intra-entreprise sur devis

Taux de satisfaction : 4,4/5 sur la période 2021-2022

LE RGPD DANS LE DOMAINE SCOLAIRE

OBJECTIF : **piloter la conformité avec le Règlement Général pour la Protection des Données (RGPD) au sein d'un établissement scolaire.**

Compétences développées

- Comprendre les obligations liées d'un établissement scolaire avec le Règlement Général pour la Protection des Données Personnelles (RGPD) ;
- Cartographier les traitements de données de l'établissement scolaire ;
- Gérer les spécificités liées à l'établissement : mineurs, enseignants, situation médicale des enfants, logiciels métiers ;
- Informer les parents et répondre aux demandes d'exercice de droits ;
- Élaborer, mettre en œuvre et entretenir les mesures de cybersécurité de l'établissement dans le cadre de la protection des données personnelles.

Références

Règlement UE 2016/679 du 27 avril 2016, Guide d'hygiène informatique de l'ANSSI, Bulletin Officiel n°24 du 16 juin 2005 de l'Education Nationale.

Contenu

- Information des parents, enseignants et salariés ;
- Gestions des prestataires ;
- Analyse d'impact sur la vie privée (PIA) ;
- Expression des droits – incidents ;
- Enjeux et menaces de cybersécurité ;
- Hygiène informatique ;
- Retour d'expérience.

Formation en présentiel

DURÉE : 2 jours

LANGUE : français

LIEU : Brest

MÉTHODES PÉDAGOGIQUES :
magistral 70 % - pratique 30 %

ÉVALUATION : quizz en fin de chaque module

PRÉREQUIS : aucun

HANDICAP : signaler lors de l'inscription

ATTESTATION : individuelle en français

PRIX : (négociés ave OPCA-LIA)
700 € par stagiaire en inter-entreprise
1 600 € par groupe en intra-entreprise

Taux de satisfaction : non calculé en 2022

MENTORING DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES

OBJECTIF : piloter la conformité avec le Règlement Général pour la Protection des Données (RGPD) au sein d'une TPE/PME.

Compétences développées

- Comprendre et mettre en œuvre les principes généraux du RGPD ;
- Rédiger une fiche de traitement ;
- Rédiger et déployer les mentions légales ;
- Connaître les spécificités de certains traitements ;
- Communiquer avec les sous-traitants ;
- Définir les exigences de sécurité ;
- Évaluer les risques.

Références

Guide d'hygiène informatique de l'ANSSI, règlement européen pour la protection des données personnelles.

Contenu

- Un diagnostic des compétences ;
- Une période d'accompagnement pour la maîtrise des actions de mise en conformité ;
- Un atelier Analyse des Risques.

Formation en présentiel

DURÉE : 2 jours

LANGUE : français

LIEU : dans nos locaux de Brest, Toulon et dans toute ville ou pays

MÉTHODES PÉDAGOGIQUES : Pratique personnalisée 100 %

ÉVALUATION : pratique

PRÉREQUIS : Être désigné comme Délégué à la Protection des Données ou référent dans son organisme. Connaître le fonctionnement de son organisme et de son système d'information.

HANDICAP : signaler lors de l'inscription

ATTESTATION : individuelle en français

PRIX : 700 € en inter-entreprise
1600 € en intra-entreprise

Taux de satisfaction : non calculé en 2022

Management de la cybersécurité en monde maritime

OBJECTIF : **piloter la cybersécurité au sein d'une compagnie maritime.**

Compétences développées

- Maîtriser les enjeux de cybersécurité pour le navire ou les infrastructures portuaires ;
- Conduire l'analyse des risques de cyberattaque ;
- Identifier et mettre en place les procédures de protection adaptée sur les réseaux sensibles ;
- Intégrer de la cybersécurité dans la sûreté maritime
- Responsabiliser les collaborateurs
- Réagir et résister en cas d'incident.

Références

Guides cyber de la DAM, Référentiel Pédagogique du Service de l'Information, Stratégique et de la Sécurité Économique (SISSE).

Contenu

- Impact sur les activités maritimes ;
- Typologie de la cybercriminalité ;
- Panorama des menaces et des attaques ;
- Cartographie des risques cyber ;
- Aspects juridiques ;
- Vulnérabilités spécifiques ;
- Risques sur les systèmes d'informations à intégrer selon l'approche ISPS, dans les plans de sûreté ;
- Élaboration de la politique cyber ;
- Principes d'hygiène informatique appliqués aux navires et aux ports ;
- Ressources documentaires ;
- Diffusion des bonnes pratiques.

Formation en présentiel

DURÉE : 1 jour

LANGUE : français

LIEU : dans nos locaux de Brest, Toulon et dans toute ville ou pays

MÉTHODES PÉDAGOGIQUES : magistral 70 % - pratique 30 %

ÉVALUATION : quizz en fin de parcours

PRÉREQUIS : aucun

HANDICAP : signaler lors de l'inscription

ATTESTATION : individuelle en français

PRIX : 350 € en inter-entreprise
1200 € en intra-entreprise

Taux de satisfaction : changement de format en 2022

Management général de la cybersécurité pour les activités maritimes

OBJECTIF : **organiser et piloter la cybersécurité dans un projet ou une organisation à vocation maritime.**

Compétences développées

- Comprendre, appliquer et animer une politique globale de cybersécurité pour contribuer à la protection et la résilience, en cohérence avec les exigences ISPS et ISM ;
- Des systèmes d'informations vitales d'une compagnie maritime ou d'un navire ;
- Des systèmes mis en œuvre sur les navires et plateformes maritimes.

Références

Circulaire 428 de l'OMI ;
Guide d'hygiène informatique de l'ANSSI – édition 2017 Guide de protection des navires de la DAM et de l'ANSSI – édition septembre 2016 ;
Guide « Renforcer la protection du navire » - DAM/ANSSI – édition janvier 2017

Contenu

- Enjeux de cybersécurité du monde naval ;
- Panorama des menaces ;
- Défense en profondeur ;
- Hygiène informatique ;
- Gestion et organisation de la cybersécurité ;
- Mesures de cyberdéfense.

Formation en présentiel

DURÉE : 1 jour

LANGUE : français

LIEU : dans nos locaux de Brest, Toulon et dans toute ville ou pays

MÉTHODES PÉDAGOGIQUES : magistral 70 % - pratique 30 %

ÉVALUATION : quizz en fin de parcours

PRÉREQUIS : aucun

HANDICAP : signaler lors de l'inscription

ATTESTATION : individuelle en français

PRIX : 350 € en inter-entreprise
1200 € en intra-entreprise

Taux de satisfaction : non calculé en 2022