

Formation Gouvernance de la sécurité de l'information

Présentation

Ce programme couvre les enjeux de la sécurité des systèmes d'information (SSI), l'évolution des menaces et des risques, et les bonnes pratiques de sécurité. Il aborde également les responsabilités légales et réglementaires, ainsi que la sécurisation des technologies et des infrastructures. Enfin, il propose des méthodologies pour évaluer et traiter les risques, et des solutions pour sécuriser les postes de travail et les échanges distants.

Durée : 7,00 heures (1 jours)

Tarif INTRA : Nous consulter

Objectifs de la formation

- Identifier les domaines clés de la sécurité et de la gestion des risques informatiques.
- Appréhender les normes et les bonnes pratiques en matière de sécurité.
- Comprendre les tendances actuelles des menaces et les solutions existantes.
- Optimiser la communication entre les différents acteurs impliqués dans la SSI.
- Effectuer des choix techniques éclairés en matière de sécurité.

Prérequis

Bonne maîtrise des systèmes d'information.

Public

Directeurs des systèmes d'information, responsables informatiques, RSSI, chefs de projet sécurité, architectes informatiques.

Programme de la formation

Introduction à la sécurité des systèmes d'information

- Contexte général et enjeux de la SSI



Évolutions des menaces et des risques

- Statistiques et tendances actuelles des menaces
- Évaluation des risques : gravité, vraisemblance et solutions de traitement

Modèle d'approche et maturité de l'organisation en SSI

- Responsabilités : acteurs clés, exigences légales et réglementaires, obligations civiles et pénales
- Analyse des besoins DICP et classification des informations et ressources
- Cartographie des risques : identification des menaces et vulnérabilités

Normes et méthodologies de sécurité

- Bonnes pratiques : ANSSI, CNIL, RGS, ISO 27002 et ISO 27001
- Approche des enjeux : les acteurs, les textes de référence et les bonnes pratiques

Modélisation des technologies et choix structurants en SSI

- Maturité des technologies : sécurisation des accès, authentification, gestion des identités
- Sécurité des échanges : algorithmes, protocoles TLS, certificats, et recommandations ANSSI
- Infrastructures de clés publiques : autorités de certification, révocation
- Solutions DLP et leur architecture

Sécurité des postes et infrastructures nomades

- Sécurisation des postes de travail et des appareils mobiles
- VPN : principes, standards et contrôles d'accès à distance
- Sécurité des échanges distants : mise en quarantaine, contrôle des accès

Architecture de cloisonnement et sécurité en profondeur

- Sécurisation des VLAN, DMZ, tunnels, et VPN
- De la sécurité périphérique à la sécurité interne : couches de protection

Sécurisation des endpoints et durcissement des systèmes

- Postes de travail, serveurs et appareils mobiles : durcissement et outils de sécurité
- Sécurisation des applications : bonnes pratiques et standards à suivre

Organisation**Formateur**

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.
- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation**En amont de la formation** (*évaluation en ligne dans l'extranet apprenant*)

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

Tout au long de la formation

- Évaluations continues réalisées par le formateur travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

À l'issue de la formation (*évaluations en ligne dans l'extranet apprenant*)

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.