+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 22/08/2025

S'inscrire

Formation Responsable de la Sécurité des Systèmes d'Information

5 jours (35 heures)

Présentation

Notre formation « Responsable de la Sécurité des Systèmes d'Information » vous permettra de comprendre les enjeux stratégiques, organisationnels et réglementaires liés à la sécurité des services informatiques, et d'en faire un levier de confiance et de performance durable pour votre organisation.

Vous apprendrez à concevoir et à déployer un Système de Management de la Sécurité de l'Information (SMSI) conforme à la norme ISO 27001, à intégrer la cybersécurité dans vos processus métiers, et à mettre en œuvre une gouvernance robuste qui conjugue efficacité opérationnelle et conformité réglementaire (RGPD, NIS2, DORA…).

La formation vous donnera également les techniques de base de la fonction RSSI : élaboration d'une politique de sécurité adaptée, définition et suivi d'indicateurs pertinents, mise en place de dispositifs d'audit et d'amélioration continue. Vous apprendrez à dialoguer avec la direction et les métiers, à prioriser les actions et à piloter les projets de sécurité en conciliant contraintes techniques, exigences réglementaires et enjeux business.

Un volet spécifique sera consacré aux aspects juridiques et réglementaires : obligations légales, responsabilité civile et pénale du RSSI, gestion des clauses contractuelles avec les prestataires, ainsi que la coopération avec les autorités de contrôle (ANSSI, CNIL, ENISA). Vous serez ainsi en mesure d'anticiper les évolutions réglementaires et de positionner la sécurité comme un facteur clé de conformité et de confiance.

En participant à cette formation, vous développerez une posture de leadership en cybersécurité, saurez évaluer la maturité de votre organisation, anticiper les risques techniques, juridiques et réputationnels, et fédérer direction, métiers et collaborateurs autour d'une vision commune de la sécurité numérique.

Objectifs

- Comprendre les enjeux de la sécurité des services informatique dans une organisation
- Connaitre les techniques de base de la fonction RSSI
- Maîtriser la norme ISO 27001 et mettre en œuvre un SMSI dans son organisation
- Connaitre la politique de sécurité et auditer la sécurité et les indicateurs
- Connaitre les règlementations et aspects juridiques de la sécurité des systèmes informatiques

Public visé

- Toute personne amenée à exercer la fonction de responsable de la sécurité des systèmes d'information

Pré-requis

- Avoir une expérience au sein d'une direction informatique
- Avoir des notions de base en sécurité appliquées aux systèmes d'information et une bonne maîtrise des systèmes et des infrastructures

Programme de Notre Formation Responsable de la Sécurité des systèmes d'Information (RSSI)

[Jour 1 - Matin]

Le rôle du RSSI dans l’organisation

- Définir les missions clés du RSSI
- Identifier les parties prenantes internes et externes
- Cartographier le périmètre d’action sécurité
- Positionner la fonction dans la gouvernance de l’entreprise
- Décrypter les attentes de la direction et des métiers
- Atelier pratique : Reconstitution d’un organigramme sécurité d’entreprise.

L’écosystème cybersécurité national et international

- ANSSI : autorité nationale, référentiels & supervision des OIV/OSE
- CERT-FR : centre d’alerte et de réponse aux incidents
- CNIL : protection des données et conformité RGPD
- ENISA : agence européenne, coordination NIS2
- OIV/OSE : opérateurs critiques soumis à obligations renforcées
- Prestataires qualifiés (PASSI, SecNumCloud, PDIS/PRIS) : audits, cloud et réponse aux incidents certifiés.

[Jour 1 - Après-midi]

Fondamentaux de la sécurité des systèmes d’information

- Définir les concepts clés : disponibilité, intégrité, confidentialité, traçabilité
- Comprendre les menaces actuelles (malwares, phishing, ransomware, etc.)
- Identifier les principales vulnérabilités techniques
- Revoir les couches de défense (réseau, système, applicatif)
- Intégrer la notion de sécurité dès la conception
- Atelier pratique : Cartographier les grandes menaces macro : cybercriminalité, cyberdéfense étatique, espionnage, enjeux géopolitiques et économiques.

Panorama des cadres et référentiels

- Politique de sécurité vs. charte informatique
- Articuler gouvernance sécurité et pilotage opérationnel
- Maîtriser les bonnes pratiques du guide d'hygiène numérique
- Initier une feuille de route sécurité réaliste
- Atelier pratique : Diagnostic de maturité SSI simplifié.

[Jour 2 - Matin]

Norme ISO 27001

- Principes et objectifs de l'ISO 27001
- Les domaines de contrôle (Annexe A)
- Processus de certification et cycle PDCA
- Conduire une gap analysis (analyse d'écart)
- Rôles et responsabilités dans la mise en conformité
- Comparatif ISO 27001 vs. NIST Cybersecurity Framework : convergences et différences
- Atelier pratique : Cartographie des exigences ISO 27001 sur un cas d'entreprise.

[Jour 2 - Après-midi]

Mise en œuvre d'un SMSI (Système de Management de la Sécurité de l'Information)

- Définition et périmètre d'un SMSI
- Gouvernance et intégration dans l'organisation
- Politique de sécurité et gestion documentaire
- Gestion des risques dans un SMSI
- Indicateurs de performance et amélioration continue
- Gestion documentaire (PSSI, procédures, preuves d'audit) et les outils de pilotage
- Atelier pratique : Élaboration d'un mini-plan SMSI pour une organisation fictive.

Sécurité de l'utilisateur et posture défensive

- Sensibilisation à la cybersécurité : leviers de communication
- Ingénierie sociale : tactiques et contremesures

- MFA, mots de passe, SSO : arbitrer entre sécurité et ergonomie
- Détection et remontée d'incidents par les utilisateurs
- Rôles des RH, managers et collaborateurs dans l'hygiène numérique

[Jour 3 - Matin]

Élaborer une politique de sécurité adaptée

- Objectifs d'une politique SSI
- Intégrer la SSI dans les processus métiers
- Rédiger une politique claire, communicable et opérationnelle
- Définir des niveaux de criticité et d'exposition aux risques
- Mettre en place des indicateurs de suivi : KPI/KRI de sécurité et leur valorisation auprès de la direction
- Atelier pratique : Rédaction collective d'un extrait de politique SSI.

[Jour 3 - Après-midi]

Mettre en œuvre une gouvernance SSI efficace

- Structure de gouvernance : comité, reporting, délégation
- Budget, ressources et priorisation des actions
- Gérer l'externalisation (infogérance, cloud, prestataires)
- Assurer la conformité RGPD côté sécurité
- Gouvernance internationale : SOX, PCI-DSS, DORA (finance), HIPAA (santé)
- Instaurer une culture sécurité partagée

Planifier et piloter les actions de sécurité

- Établir une feuille de route SSI annuelle
- Suivre les projets SSI : outils, jalons, revues
- Arbitrer entre urgence et long terme (projets, incidents)
- Mettre en place des revues de sécurité périodiques
- Dialoguer avec les métiers et la direction

[Jour 4 - Matin]

Appliquer une démarche de gestion des risques

- Identifier les actifs critiques à protéger
- Cartographier les menaces et les vulnérabilités
- Évaluer la vraisemblance et l'impact des scénarios
- Choisir des mesures de traitement pertinentes
- Suivre les risques et communiquer aux décideurs
- Introduction à la méthode EBIOS Risk Manager (EBIOS-RM)

- Atelier pratique : Cartographie des risques sur cas simulé.

[Jour 4 - Après-midi]

Juridique : Répondre aux exigences réglementaires

- Obligations légales et réglementaires (RGPD, LPM, NIS2, DORA)
- Revue des clauses contractuelles sécurité (clients/fournisseurs)
- Traçabilité, preuves et responsabilités
- Coopération avec le DPO, RSSI groupe, prestataires
- Responsabilité pénale et civile du RSSI et délégation de responsabilités
- Conventions internationales (Convention de Budapest, extraterritorialité, conformité hors UE)
- Préparer un audit ou une inspection sécurité

Évaluer et auditer la sécurité du SI

- Typologie des audits (interne, tiers, technique, organisationnel)
- Méthodes d'audit et outils associés
- Recueillir, analyser et valoriser les écarts
- Suivi des plans d'actions correctifs
- Préparer une restitution pédagogique au management

[Jour 5 - Matin]

Organiser la réponse aux incidents de sécurité

- Typologie des incidents (intrusion, fraude, compromission...)
- Processus de détection, qualification, escalade
- Constitution et rôle d'une cellule de crise
- Contenir, éradiquer, rétablir
- Communication de crise interne et externe : management, presse, autorités (ANSSI, CNIL)
- Post-mortem et retour d'expérience
- Atelier pratique : Simulation d'un incident cyber.

[Jour 5 - Après-midi]

Construire un plan de continuité et de reprise (PCA/PRA)

- Différences PCA / PRA : enjeux, contenus, méthodes
- Identifier les processus critiques et les ressources associées
- Définir les RTO/RPO et scénarios de reprise
- Tester et maintenir son PCA/PRA
- Impliquer les métiers et la direction dans la résilience

Valoriser et faire vivre la fonction de RSSI

- Établir une communication adaptée (tableaux de bord, indicateurs, rapports)
- Valoriser les actions du RSSI auprès de la direction
- Développer les soft skills du RSSI : leadership, pédagogie, gestion de conflits, influence stratégique
- Maintenir la posture d'alerte sans générer la peur
- Former, co-responsabiliser, fédérer les acteurs
- S'inscrire dans une dynamique d'amélioration continue
- Atelier pratique : Présenter un bilan SSI fictif au COMEX.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.