Formation SSI : Homologation RGS

PLUS D'INFOS

- Contactez-nous

CONTACT REFERENT

- Commercial@ageris-group.com
- +33 3 87 62 06 00

MODALITES D'ACCES

- Accessible à distance
- Accessible en présentiel

DELAI D'ACCES

- La durée estimée entre la demande du stagiaire et le début de la formation est de 7 jours (peut être raccourci pour le mode distanciel)

ACCESSIBILITE AUX PERSONNES EN SITUATION D'HANDICAP

- Accessible à distance pour les personnes à mobilité réduite
- Pour connaître l'accessibilité aux salles de formation, vous pouvez nous joindre au +33 3 87 62 06 00

REFERENCE

- SSIRGS

TARIF

- Sur devis

DUREE DE LA FORMATION

- 2 jours – 14 heures

DATES DES SESSIONS

- Sur demande en INTRA uniquement

FINANCEMENT

- OPCO

FORMULE INTRA-ENTREPRISE

Formulaire : soumettez votre projet

RESSOURCES PEDAGOGIQUES

- Cours théorique
- Exemples concrets
- Evaluation des compétences par un quizz en cours et en fin de formation
- Support de cours remis au stagiaire en fin de formation
- Outils distanciel : teams

PRESENTATION DE LA FORMATION

Dans le cadre de la mise en œuvre de téléservices, les autorités administratives sont soumises à l'obligation légale de respecter l'ordonnance n° 2005-1516 du 8 décembre 2005 relative à leurs échanges électroniques avec leurs usagers. Cette ordonnance introduit le Référentiel Général de Sécurité (article 9) qui fixe les règles auxquelles les SI mis en place par les autorités administratives doivent se conformer pour assurer la sécurité des informations échangées.
Les règles techniques et fonctionnelles imposées par ce référentiel modifient la gouvernance des SI au sein des autorités administratives notamment lors de la conception des nouveaux projets mais également lors du maintien en condition opérationnelle des systèmes numériques opérationnels.
Cette formation vise à fournir tous les éléments juridiques, fonctionnels et techniques permettant d'intégrer les nouvelles exigences du RGS dans les processus opérationnels (métiers et informatique) et de définir les procédures adaptées au déploiement des mesures de sécurité.

OBJECTIFS DE CETTE FORMATION

A l'issue de cette formation, le stagiaire aura les compétences pour :

- Comprendre comment appliquer les directives de protection des données à caractère personnel (loi sur la protection des données personnelles et RGPD) dans le cadre de la mise en œuvre d'un téléservice
- Savoir mettre en œuvre la démarche permettant d'appliquer la sécurité des SI durant tout le cycle de vie d'un projet informatique (en conformité avec les principes énoncés dans le guide GISSIP de l'ANSSI)
- Connaître et savoir appliquer les directives du RGS en matière d'homologation de la sécurité des systèmes d'information
- Être en mesure d'appliquer les directives techniques (certificat, horodatage, authentification, …) définies dans la dernière version du RGS en vigueur
- Savoir conduire une démarche d'appréciation des risques et d'audit conforme aux directives du RGS
- Être capable de définir les objectifs et la politique de sécurité adaptés aux enjeux de l'autorité administrative

PUBLIC

Responsable de la Sécurité du Système d'Information (RSSI), DPO, chefs de projet, Directeur des Systèmes d'Information, responsables métiers en charge de la mise en œuvre des téléservices.

PREREQUIS

Aucun prérequis n'est nécessaire.

PROGRAMME DETAILLE

En présentiel/à distance

1. Introduction

- Cadre juridique du RGS (ordonnance du 8 décembre 2005 et arrêtés d'application) ;
- Modèle général de gestion des risques
- Périmètre d'éligibilité au RGS (organismes concernés par le RGS, …)
- Historique de la sécurité des systèmes d'information
- Principes généraux relatifs à la protection des données à caractère personnel (Informatique et Libertés)

2. Les principes généraux du Référentiel Général de Sécurité

Formation SSI : Homologation RGS

POUR ALLER PLUS LOIN

- SSI – Auditer et contrôler la sécurité du Système d'Information
- SSI – Devenir Responsable de la Sécurité des Systèmes d'Information (RSSI)

PLUS D'INFOS

- Contactez-nous

- Démarche de mise en œuvre du RGS pour tous les nouveaux téléservices
- Mise en conformité des téléservices opérationnels avant la parution du RGS
- L'homologation de la sécurité des systèmes d'information
- Les prestataires de services de confiance (PSCO)
- Les produits de sécurité labellisés ou certifiés
- Les fonctions techniques de sécurité
- La prise en compte de la sécurité dans les démarches projets

3. La mise en place d'une filière sécurité au sein de l'autorité administrative

- Les instances de décisions
- L'autorité d'homologation
- Les acteurs de la filière SSI (RSSI, CIL/DPO, Référents SSI …)
- Les rôles et responsabilités collectives et individuelles de tous les personnels de l'autorité administrative
- Exemple de modèle organisationnel
- Exemple de document décrivant les rôles et les responsabilités

4. L'homologation de la sécurité

- Le rôle du chef de projet dans le processus d'homologation
- La création du dossier de sécurité d'un nouveau projet informatique
- La présentation du dossier de sécurité à l'autorité d'homologation

5. L'appréciation des risques et la définition des objectifs de sécurité

- Présentation du guide méthodologique de la CNIL
- Présentation de la méthode EBIOS de l'ANSSI
- Appréciation des risques dans le cadre d'un téléservice
- Analyse de la maturité du SI – présentation du guide de maturité de l'ANSSI
- Étude de cas basée sur l'utilisation du logiciel SCORE Priv@cy

6. L'audit de la sécurité des systèmes d'information

- Les catégories d'audit
- Les exigences relatives aux choix d'un prestataire d'audit
- Les métriques d'audit et la présentation des résultats
- Présentation du guide de l'auditeur de l'ANSSI

7. La formalisation de la PSSI

- Les objectifs de la PSSI, son périmètre
- Les sujets à aborder dans le cadre de la politique de sécurité
- La structure document d'une politique de sécurité
- Les chartes à destination des personnels internes ou externes
- Exemple de directives de sécurité, de PSSI et de chartes

8. La sensibilisation des personnels

- La démarche de sensibilisation

- Construire son plan de sensibilisation
- Exemple de support et d'outils de sensibilisation
- Le suivi de la sensibilisation

9. La prise en compte de la SSI dans les nouveaux projets

- Présentation du guide GISSIP de l'ANSSI
- Les livrables de sécurité attendus à chaque étape d'un nouveau projet
- La formalisation d'un dossier de sécurité
- Exemple de création d'un dossier de sécurité en utilisant le logiciel SCORE Priv@cy

10. Les fonctions techniques de sécurité informatique

- Les règles relatives à la cryptographie
- Les règles relatives à la protection des échanges électroniques
- Les règles relatives aux accusés d'enregistrement et aux accusés de réception

11. Le plan de traitement des incidents et de reprise d'activité

- Principes généraux relatifs à la gestion des incidents
- Introduction à la mise en œuvre d'un PCA / PRA (basé sur la norme ISO 22301)
- Procédures d'alertes et de gestion d'une cyber-crise

12. La maintenance et le suivi de la sécurité des systèmes d'information

- La mise en place d'une démarche d'amélioration continue basée sur la norme ISO 27001
- La veille technique et juridique de la sécurité des systèmes d'information

13. Conclusion

MODALITES D'EVALUATION

Validation des connaissances et compétences par un quizz à la fin de chaque chapitre.