Formation Homologation de la sécurité - Référentiel Général de Sécurité (RGS) 2.0

Mettre ses pratiques en conformité avec les obligations légales

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Dans le cadre de la mise en oeuvre 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.

Référence	MGR822
Durée	2 jours (14h)
Tarif	1 990 €HT

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 17 au 18 avril 2025
du 10 au 11 juillet 2025
du 25 au 26 septembre 2025
du 27 au 28 novembre 2025

PARIS

du 10 au 11 juillet 2025
du 25 au 26 septembre 2025
du 27 au 28 novembre 2025

VOIR TOUTES LES DATES

Objectifs

| Appliquer les directives de protection des données à caractère personnel (Loi "Informatique et Libertés") dans le cadre de la mise en oeuvre d'un téléservice
| Mettre en oeuvre 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)
| Appliquer les directives du RGS en matière d'homologation de la sécurité des systèmes d'information
| Appliquer les directives techniques (certificat, horodatage, authentification....) définies dans la dernière version du RGS en vigueur
| Conduire une démarche d'appréciation des risques et d'audit conforme aux directives du RGS
| 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 oeuvre des téléservices

Prérequis

| Aucun

Programme de la formation

1 - Introduction
| Cadre juridique du RGS (ordonnance du 8 décembre 2005 et arrêtés d'application)
| 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
| Démarche de mise en oeuvre 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, 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 basé sur l'utilisation du logiciel SCORE Priv@vy

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 oeuvre d'un PCA / PRA (basé sur la norme ISO 22301)
| Procédures d'alertes et de gestion d'un cyber-crise on

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
| Les tableaux de bord de suivi de la sécurité des systèmes d'information

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.