USCB16 - L'homologation de sécurité

Mis à jour le 21-01-2025

Code : USCB16

Unité spécifique de type mixte

6 crédits

Responsabilité nationale :
EPN05 - Informatique / Nicolas PIOCH

Contact national :

Cnam Centre Régional de Bretagne

Zoopôle Les Croix
2 rue Camille Guérin
22440 Ploufragan
0 972 311 312
Isabelle Guée
bzh_master_cybersecurite@lecnam.

Présentation

Prérequis

SEC103

Objectifs pédagogiques

Description :

La démarche d'homologation d'un système d'information est un préalable à l'instauration de la confiance dans leur exploitation et plus généralement dans leur définition et leur rôle au sein de l'entreprise. Pour un certain nombre de systèmes, cette recommandation est rendue obligatoire par des textes, tels que l'instruction générale interministérielle n° 1300, le référentiel général de sécurité (RGS) et la politique de sécurité des systèmes d'information de l'État (PSSIE).

Objectifs pédagogiques :

Cette formation vise à fournir les éléments juridiques, fonctionnels et techniques permettant d'intégrer les nouvelles exigences du RGS dans les processus opérationnels et de définir les procédures adaptées au déploiement des mesures de sécurité.

Compétences

Compétences acquises :

- Connaître les différents référentiels gouvernementaux de sécurité de l'information et leurs limites
- Mettre en place ou renforcer un processus de management du risque numérique au sein d'une organisation
- Apprécier et traiter les risques relatifs à un projet numérique, notamment dans l'objectif d'une homologation de sécurité
- Définir le niveau de sécurité à atteindre pour un produit ou un service, dans la perspective d'une certification ou d'un agrément

Savoirs :

- Connaître les démarches d'une homologation
- Savoir adapter sa démarche aux enjeux de sécurité du SI (contexte d'emploi, nature des données contenues et utilisateurs)
- Mettre en pratique une analyse de risque

Programme

Contenu

- Introduction
  - Cadre juridique et périmètre du RGS
  - Principes généraux relatifs à la protection des données de la RGPD
- Démarche d'homologation de la sécurité
  - Précision du référentiel réglementaire
  - Délimitation du périmètre
  - Diagnostique des besoins de sécurité et du niveau de maturité SSI de l'organisme
  - Acteurs de l'homologation
- Appréciation des risques
  - Approche et limites de l'analyse des risques
  - Cadre de l'analyse de risques (ISO 27005 :2018)
  - NIST SP 800 30
  - MEHARI
  - ANSSI EBIOS Risk Manager
  - Analyse d'impact relative à la protection des données (Privacy Impact Assessment)
  - Analyse de la maturité du SI

- Focus sur EBIOS Risk Manager
- Périmètre de contrôle et audits
- Décision formelle d’homologation
- Plan de traitement des incidents et de reprise d’activité
    - Principes généraux
    - Introduction à la mise en œuvre d’un PCA / PRA (basé sur la norme ISO 22301)
    - Procédure d’alertes et de gestion de crise
- La maintenance et le suivi de la sécurité des systèmes d’information
    - Mise en place d’une démarche d’amélioration continue basée sur la norme ISO 27001
    - Veille technique et juridique de la sécurité des systèmes d’information

Modalités de validation

- Projet(s)

Description des modalités de validation

Modalités de validation :

Dossier cahier des charges d'analyse de risque ou d'une analyse de sécurité ou de vulnérabilité