SEC101 - Cybersécurité : référentiel, objectifs et déploiement

Valide le 20-02-2019

Code : SEC101

6 crédits

Responsabilité nationale :
EPN05 - Informatique / Jean-pierre ARNAUD

Contact national :
EPN05 - Informatique
2 rue Conté
75003 Paris
01 40 27 22 58
Swathi Rajaselvam
swathi.ranganadin@cnam.fr

Présentation

Prérequis

Niveau Bac + 2 en informatique, il est conseillé de suivre ou d'avoir suivi l'unité d'enseignement SEC001.

Objectifs pédagogiques

Savoir mener, argumenter et déployer une politique de sécurité informatique dans une entreprise en lien avec une analyse de risque.

Compétences

- Comprendre les enjeux d'une politique et de sécurité informatique cybersécurité et appliquer des méthodologies efficaces d'aguerrissement
- Comprendre les différentes situations d'incident
- Savoir mettre en place une gouvernance efficace dans le domaine de la cybersécurité
- Savoir auditer, conseiller, accompagner le changement
- Savoir mener et intégrer des solutions de sécurité suite à l'analyse de risque

Programme

Contenu

1- Principaux enjeux de la sécurité pour la société numérique[VL2]
· Présentation de l'écosystème : principales parties prenantes, la sécurité et les métiers (OIV, industrie, santé , finances,...)
· L'identité numérique (vie privée,..)
· L'intelligence économique, géopolitique : principales menaces, bonnes pratiques,...)
· Panorama des obligations normatives, réglementaires et juridiques (RGS, Homologation ANSSI, LPM, ISO, CNIL, CLUSIF, etc.)
2- La continuité d'activité :[VL3]
· Le SI (SSIV,SSI ,...)
· Système de gestion de la sécurité de l'information (ISMS, ISO 2700
· L'incident de sécurité,
· Cycle de vie d'un incident de sécurité : veille (évitement, protection), alertes, détection et réponse (traitement, confinement, acceptation),
· La réponse à incident (procédures, escalade,...)
3- Organisation de la sécurité et de ses métiers dans l'entreprise :
· Acteurs et responsabilités : externes (clients, fournisseurs, assurances,...) , internes (employés, prestataires,...)
· Acteurs internes et RSSI : DSI, RH, DAF, marketing,
· Gouvernance de la sécurité : espaces normatifs (ISO 27001, ISO 22301, ISO 27035)
4- Implémentation de la sécurité
· Volet organisationnel : L'analyse du risque, (panorama des méthodes)
· De l'analyse de risque à la PSSI et schéma de sécurité,
· · Approfondissement d'une méthode d'analyse de risque en vue de l'élaboration d'une fiche FEROS pour l'homologation d'un SI,
· · Déploiement : projets de sécurité, produits et services.
· · Maintien en condition de sécurité, le RSSI et les SECOPS : définition des procédures opérationnelles, ...

Bibliographie

Titre	Auteur(s)

Tableaux de bord de la sécurité réseau », Editeur(s) : Eyrolles, Nbp: 562 , 26/08/2010, 3°ed., EAN13 : 9782212128215	Cédric Llorens, Laurent Levier, Denis Valois, Benjamin Morin
Management de la sécurité de l'information, Implémentation ISO 27001 , Editeur(s)	Alexandre Fernandez-Toro
analyse de la norme ISO27035 , « La gestion des risques Concepts et méthodes 2009	Plusieurs documents du CLUSIF sont disponibles à cette adresse : / https://cl