le cnam
Nouvelle-Aquitaine

Fiche récapitulative

SEC104 | Analyse de risques des données, réseaux et systèmes

51
Total d'heures d'enseignement

6
Crédits ECTS

Date non définie
Début des cours prévu

Programme

Introduction Présentation de la boucle d'analyse et AC de la sécurité informatique d'un SI (AR et CA)

Travail personnel : recherche bibliographique sur les analyses de risque

Temps 1 : Analyse de risques : enjeux, processus et bien informationnels (AR)

Cours 1 : Analyse de risques (AR)
Cours 2 : Classification
TD 1 : Cartographies
Cours 3 : Classes de menaces
Cours 4 : Audit
TD 2 : Audit d'un composant du SI

Temps 2 : Analyse de risques : SI (AR)

Cours 5 : Méthode EBIOS
Cours 6 : Application spécifique
TD3 : Application spécifique et étude de cas EBIOS

Temps 3 : Analyse de risques : données (AR)

Cours 7 : Méthode PIA
TD4 : Application spécifique et cas d'étude PIA

Temps 4 : AR et CA (CA)

Cours 8 : continuité d'activité - incertain
Cours 9 : CA et services informatiques
Travail personnel : Recherche bibliographique sur une thématique de la continuité d'activité

Temps 5 : AR et tests (CA)

Cours 10 : Réaction aux incidents
Cours 11 : Suivi et revue du processus - Amélioration continue (AC)
Cours 12 : Essai et exercice
TD ou Cyberchallenge

Objectifs : aptitudes et compétences

Objectifs :

Lorsqu'une organisation vise l'amélioration continue de sa sécurité informatique, elle peut, en conformité avec le bouquet de norme

ISO 27., mettre en place un système de management de la sécurité de l'information (SMSI) et un système de management de la continuité d'activité (SMCA) en s'appuyant sur une méthodologie d'analyse des risques.

Au coeur de l'analyse de risque, l'identification des actifs constitue une étape essentielle. Les données sont un cas d'actifs précieux dont les propriétés relèvent également d'une analyse spécifique vis à vis de la vie privée. Cette analyse peut suivre la méthode PIA proposée par la CNIL.

Une fois les actifs identifiés, l'analyse de risque permet d'appréhender les enjeux de l'organisation et d'identifier un ensemble d'exigences qui font appel à des connaissances organisationnelles et techniques en vue d'élaborer un Système de Management de la Sécurité de l'Information (SMSI). Pour ce faire, l'analyse de risque fait appel à une méthodologie qui en première intention contribue à une maitrise des risques connus et visera à appréhender ces risques avec une bonne connaissance de ses enjeux et menaces, en menant une démarche en alignement avec les autres directions de l'organisation et en mettant en place un plan de traitement des risques. Cette première intention ne prend pas toujours en compte les risques dans l'incertain, qui requièrent une amélioration continue de cette première mise en place.

Les enjeux d'un dispositif de continuité d'activité sont de de survivre à un sinistre et de préserver l'activité de l'organisation, la norme ISO 22301 en décrit les contours qui reposent sur un Système de Management de la Continuité d'Activité (SMCA).

L'objectif de ce cours est de fournir aux apprenants de SEC104 les outils et socles de connaissances pour parvenir à réaliser des missions (fiches métiers génériques).

Compétences :

AR

Savoir mener, argumenter et déployer une politique de sécurité informatique (PSSI) dans une entreprise en lien avec une analyse de risque (AR) des infrastructures et des données avec la compréhension des principales normes en matière de sécurité de l'information, données et IT,
Mettre en place une hiérarchisation des risques entre eux afin de cibler les actions à mener, générer et gérer un plan d'action (PA),
Rédiger les documents de gouvernance de la sécurité de l'information (Politique de Sécurité du SI, chartes informatiques, Gouvernance des données),
Conduire une analyse de risque PIA à l'aide de la cartographie des données (DCP) et des traitements,
Savoir mettre en place le reporting et les tableaux de bord pour assurer le suivi auprès de RSSI opérationnels,
Identifier et analyser les risques opérationnels en utilisant les cartographies et audit d'un composant, en interprétant les indicateurs de compromission,
Prendre en charge les analyses qualitatives et quantitatives menées au travers des audits et traiter les risques,
Accompagner la mise en conformité aux référentiels de la sécurité du SI (ISO 2700x, RGPD, LPM, HDS, PCI DSSH, HADS, etc.).Savoir mener, argumenter et déployer un tableau de bord à partir de la PSSI,
Conduire des audits d'évaluation de conformité réglementaire et le suivi des veilles réglementaires d'un SI ou de l'un de ses composants,
Répondre aux recommandations d'audit en acquérant une base solide sur les méthodes d'audit stratégiques et techniques au service de l'analyse de risques,

CA

Faire l'ébauche de scénario à risque afin de mettre à jour les procédures opérationnelles,
Savoir mener, argumenter et déployer une politique de résilience et de Préparation des TIC pour la Continuité d'Activité (PTCA),
Concevoir et gérer un système de management de la sécurité (SOC) et de la continuité d'activité (SMCA) du système d'informations et de ses composants, mettre en place une cellule de réponse à incident au sein d'un SOC,
Savoir mener, argumenter et gérer une réponse à incident en situation ou après sinistres (PRAS),
Prévenir et anticiper les situations de crise, organiser la gestion des situations d'urgence
Concevoir des exercices efficaces pour maîtriser la continuité de service et la résilience d'un système d'information.

Conduire une réponse à incident de sécurité en assurant la création de rapports et de feedback.

Prérequis

Bac+2 Informatique

Délais d'accès

Le délai d'accès à la formation correspond à la durée entre votre inscription et la date du premier cours de votre formation.

- UE du 1er semestre et UE annuelle : inscription entre mai et octobre
- UE du 2e semestre : inscription de mai jusqu'à mi-mars

Exemple : Je m'inscris le 21 juin à FPG003 (Projet personnel et professionnel : auto-orientation pédagogique). Le premier cours a lieu le 21 octobre. Le délai d'accès est donc de 4 mois.

Planning

Légende:

Cours en présentiel

Cours 100% à distance

Mixte: cours en présentiel et à distance

Centre de formation	Prochaine session*	Modalité	Tarif individuel
100% à distance	2024/2025 : Date non définie		De 0 à 1.020 €

*Selon les UEs, il est possible de s'inscrire après le début des cours. Votre demande sera étudiée pour finaliser votre inscription.

Modalités

Modalités pédagogiques :

Pédagogie qui combine apports académiques, études de cas basées sur des pratiques professionnelles et expérience des élèves. Équipe pédagogique constituée pour partie de professionnels. Un espace numérique de formation (ENF) est utilisé tout au long du cursus.

Modalités de validation :

Dossier cahier des charges d'analyse de risque ou d'une analyse de sécurité ou de vulnérabilité et contrôle continu par la notation des travaux dirigés

Ou examen sur table

Ou les 2

Tarif

Mon employeur finance	1.020 €
Pôle Emploi finance	510 €
Je finance avec le co-financement Région	Salarié : 156 €
Je finance avec le co-financement Région	Demandeur d'emploi : 124,80 €

Plusieurs dispositifs de financement sont possibles en fonction de votre statut et peuvent financer jusqu'à 100% de votre formation.

Salarié : Faites financer votre formation par votre employeur

Demandeur d'emploi : Faites financer votre formation par Pôle emploi

Votre formation est éligible au CPF ? Financez-la avec votre CPF

Si aucun dispositif de financement ne peut être mobilisé, nous proposons à l'élève une prise en charge partielle de la Région Nouvelle-Aquitaine avec un reste à charge. Ce reste à charge correspond au tarif réduit et est à destination des salariés ou demandeurs d'emploi.

Pour plus de renseignements, consultez la page Financer mon projet formationopen_in_new ou contactez nos conseillers pour vous accompagner pas à pas dans vos démarches.

Passerelles : lien entre certifications

- CRN0803A - Titre RNCP Niveau 6 Concepteur intégrateur d'infrastructures informatiques (systèmes et réseaux, applicatives, ou de sécurité) parcours Cybersécurité
- CRN0801A - Titre RNCP Niveau 6 Concepteur intégrateur d'infrastructures informatiques (systèmes et réseaux, applicatives, ou de sécurité) parcours Systèmes et réseaux
- CRN0802A - Titre RNCP Niveau 6 Concepteur intégrateur d'infrastructures informatiques (systèmes et réseaux, applicatives, ou de sécurité) parcours Systèmes d'information

Avis des auditeurs

Les dernières réponses à l'enquête d'appréciation de cet enseignement :

↓ Fiche synthétique au format PDF

Taux de réussite

Les dernières informations concernant le taux de réussite des unités d'enseignement composant les diplômes

↓ Taux de réussite