Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES

FORMATION À LA CYBERSÉCURITÉ DES TPE ET DES PME

Référentiel pédagogique pour les organismes de formation

DGE DIRECTION GÉNÉRALE DES ENTREPRISES

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION · ANSSI ·

SISSE Service de l'Information Stratégique et de la Sécurité Économiques

Le présent référentiel pédagogique est le résultat d'une réflexion entre des entreprises et des acteurs institutionnels spécialisés dans la protection des acteurs économiques et leur accompagnement en cybersécurité.

Il est destiné à aider les organismes de formation à élaborer des stages en cybersécurité au profit des TPE/PME qui souhaitent former des « **référents cybersécurité** » dans leur structure. Ce référentiel décrit les programmes minimaux à partir desquels les formateurs doivent développer une ingénierie pédagogique permettant de produire des programmes et des contenus adaptés.

Élaboré et édité en 2014 par la Délégation interministérielle à l'intelligence économique (D2IE), il a bénéficié du soutien de l'agence nationale de la sécurité des systèmes d'information (ANSSI).

Aujourd'hui, le Service de l'Information Stratégique et de Sécurité Économiques (SISSE) du ministère de l'Économie et des Finances, reprenant les attributions de la D2IE en la matière, invite avec l'ANSSI tous les organismes en charge de l'accompagnement économique des entreprises, et notamment de leur transition numérique, à s'approprier ce référentiel et à le diffuser aux organismes de formation à même de mettre en œuvre des formations de **référent cybersécurité**.

Ce référentiel est éligible à la labellisation SecNumedu-FC de l'ANSSI.

Cette labellisation permet aux organismes delivrant cette formation d'être référencés sur le site de l'ANSSI et d'utiliser la marque et le logo associés à cette labellisation. Pour plus de précisions, consulter *www.ssi.gouv.fr/entreprise/formations/***, rubrique SecNumedu-FC.**

En France, les très petites entreprises (TPE) et les petites et moyennes entreprises (PME) représentent une source importante d'emplois et d'innovations.

Elles évoluent aujourd'hui dans un environnement de plus en plus numérique, qui favorise incontestablement leur compétitivité et leur croissance. Cependant, on assiste aujourd'hui à une montée en puissance des cyberattaques visant les entreprises et ce quelle que soit leur taille. Ainsi, il est essentiel de prendre conscience que, si elle n'est pas bien organisée et pensée par l'entreprise, la dépendance au « tout numérique » peut s'avérer dramatique en cas d'attaques (vol de données, mise hors service du système informatique, rançongiciel…).

Pour y faire face, les TPE/PME n'ont pas toujours la possibilité de recruter des profils dédiés uniquement à la sécurité informatique. Qui plus est, leur approche de la gestion des infrastructures informatiques varie en fonction de l'utilisation qui en est faite, de leur taille, du secteur économique et du budget qui y est consacré. De fait, à l'exception de certains secteurs très spécifiques, le niveau de perception et de prise en charge du « cyber-risque » dans les TPE/PME est souvent insuffisant.

Afin de les aider à maîtriser ce nouvel environnement, à aborder du mieux possible leur transformation numérique et à préserver leur patrimoine immatériel, il convient de mettre en place, dans une approche de sécurité économique globale, des solutions humaines et techniques de cybersécurité spécialement adaptées.

La formation de **référents en cybersécurité** au sein des TPE/PME permettra de répondre en partie à ce défi.

Objectif de la formation

L'objectif général de la formation est de faire du participant un **référent cybersécurité** interne.

À la fin de la formation, le participant devra être en mesure de maîtriser les enjeux de la cybersécurité pour l'entreprise et d'utiliser les outils nécessaires pour protéger des informations sensibles (personnelles et professionnelles) sur les différents réseaux.

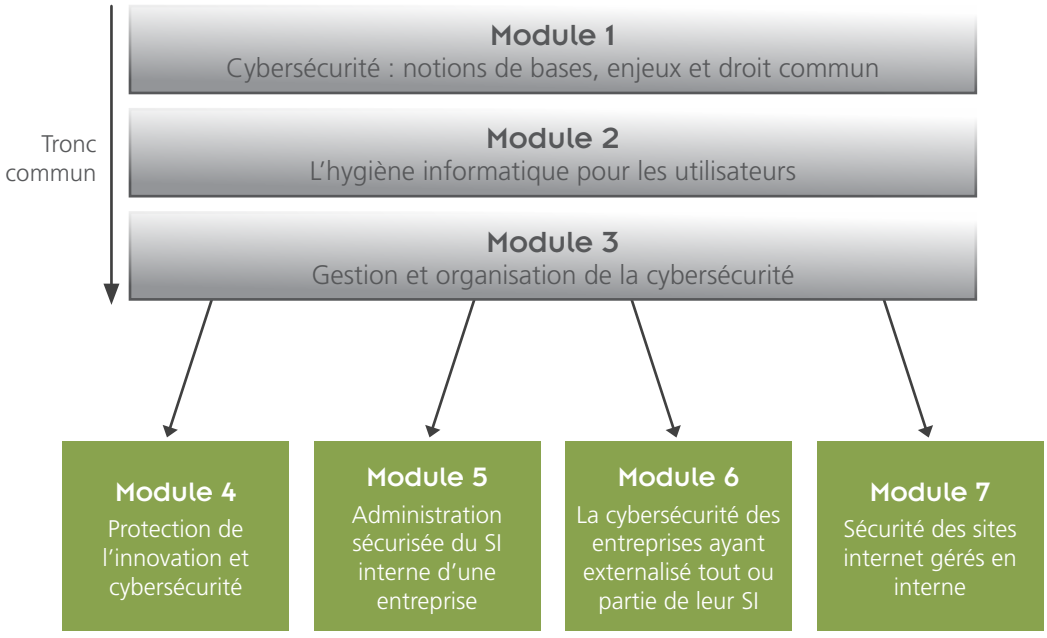
Il sera notamment à même de :

- identifier et analyser des problèmes de cybersécurité dans une perspective d'intelligence et de sécurité économiques ;
- connaître les obligations et responsabilités juridiques de la cybersécurité ;
- identifier et comprendre les menaces liées à l'utilisation de l'informatique et des réseaux internet, réseaux privés d'entreprises ou réseaux publics ;
- mettre en œuvre les démarches de sécurité inhérentes aux besoins fonctionnels ;
- savoir présenter les précautions techniques et juridiques à mettre en place pour faire face aux attaques éventuelles.

Structure pédagogique

Ce programme s'organise autour d'un bloc de trois modules communs à l'ensemble des entreprises, avec des notions d'ordre général, et de quatre modules complémentaires en fonction de l'utilisation du numérique et des profils des entreprises.

Il est préconisé que chaque module se termine par une évaluation, et qu'un ensemble de liens vers des ressources complémentaires (sites web, documents, statistiques, etc.) soit fourni aux participants désireux d'approfondir certains sujets de cybersécurité.



Public

La formation à la cybersécurité peut toucher un public hétérogène parmi les salariés des entreprises, que le référent cybersécurité soit dirigeant, cadre, responsable informatique, etc.

Sommaire

MODULE 1
Cybersécurité : notions de bases, enjeux et droit commun

Service de l'Information Stratégique et de la Sécurité Économiques

Durée* : 3 heures

Objectifs :

- Identifier l'articulation entre cybersécurité, sécurité économique et intelligence économique
- Comprendre les motivations et le besoin de sécurité des systèmes d'information (SI).
- Connaître les définitions et la typologie des menaces.

Contenu détaillé :

Définitions

- Intelligence économique, sécurité économique globale
- Cybersécurité

  Sécurité des SI (prévention) + Cyberdéfense (réaction) + Cybercriminalité (sanction) = Cybersécurité

Les enjeux de la sécurité des SI

- La nouvelle économie de la cybercriminalité

  Les déficiences en matière de cybersécurité peuvent engendrer des pertes financières directes ou indirectes (comme lorsqu'un site marchand est rendu indisponible ou lors d'espionnage économique sur des appels d'offres, par exemple).

- Panorama des menaces selon une typologie

  Panel assez large des différentes menaces (attaques intrusives - injection SQL, passive – phishing, destructrices – virus, etc.). Détails sur les Advanced Persistent Threat (APT, Attaque persistante avancée) : rôle des entreprises dans ces attaques.

- Les vulnérabilités (exemples, détermination, veille)

  Vulnérabilité : faiblesse d'un bien, que ce soit à la conception, la réalisation, l'installation, la configuration ou l'utilisation.

- Focus sur l'ingénierie sociale

Les propriétés de sécurité

- Présentation du principe de défense en profondeur

  Un logiciel spécialisé dans la cybersécurité n'est pas suffisant. La démarche de cybersécurité s'inscrit dans un processus global de sécurité économique (sécurité bâtimentaire, sécurisation des déplacements, contrôle d'accès, etc.). Cf. La sécurité économique au quotidien en fiches thématiques (SISSE).

- Identification et évaluation des actifs et des objectifs de sécurité

  Arriver à identifier précisément le besoin :
  Un site internet marchand et un site internet « vitrine » n'ont pas les mêmes besoins en termes de sécurité.
  Déterminer les critères (disponibilité, intégrité, confidentialité, preuve / traçabilité) qui permettent d'évaluer le niveau de sécurité des SI.

** Les volumes horaires présentés dans les modules sont donnés à titre indicatif.*

Aspects juridiques et assurantiels

- Responsabilités

  Quelles sont les responsabilités des entreprises qui n'ont pas assez sécurisé leurs SI ?
  Quels recours sont possibles vers les prestataires ?
  Réglementation européenne : analyse de risque obligatoire pour une entreprise dès qu'il y a une déclaration à la Commission nationale de l'informatique et des libertés (CNIL).

- Préservation de la preuve

  Que faire en cas d'attaques informatiques ?
  Comment préserver la preuve tout en restant opérationnel ?
  Qui faut-il contacter ?
  Le rôle de l'huissier.

- L'offre assurantielle

Le paysage institutionnel de la cybersécurité

- La prévention

  Rôle et missions des acteurs étatiques en charge de l'accompagnement des entreprises en matière de cyber.

- Le traitement des cyberattaques et la réponse judiciaire

  L'agence nationale de la sécurité des systèmes informatiques (ANSSI), la Direction générale de la sécurité intérieure (DGSI), la Gendarmerie nationale, etc.

- Rôle et missions des acteurs étatiques chargés du traitement technique et judiciaire des attaques cybers

  L'ANSSI, la Direction centrale de la police judiciaire, sous-direction de la lutte contre la cybercriminalité (SDLC-OCLCTIC), la brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI), la gendarmerie nationale (C3N, NTECH), etc.

Durée* : 3 heures

Objectif :

- Appréhender et adopter les notions d'hygiène de base de la cybersécurité pour les organisations et les individus.

Contenu détaillé :

- Connaître le système d'information et ses utilisateurs

  Faire une cartographie des SI de l'entreprise.

- Identifier le patrimoine informationnel de son ordinateur (brevets, recettes, codes source, algorithmes…)

  Connaître la valeur des informations contenues dans son ordinateur pour appliquer les différentes procédures de sécurité en fonction des documents utilisés.

- Maîtriser le réseau de partage de documents (en interne ou sur internet)

  Identifier précisément les passerelles qui existent entre internet et le réseau interne pour éviter les failles qui permettront ou faciliteront une intrusion non détectée.

- Mettre à niveau les logiciels

  Définir une véritable politique de mise-à-jour des logiciels (qui est en charge ? À quel moment ? etc.).

- Authentifier l'utilisateur

  Présentation des différentes méthodes permettant d'authentifier les utilisateurs et ainsi de leur attribuer la méthode qui correspond le mieux aux documents qu'ils utilisent.

  Evoquer les bonnes pratiques pour les mots/phrases de passe (conception, fréquences d'utilisation, etc.).

- Nomadisme - Problématiques liées au BYOD (Bring your Own Devices)

  Evoquer les risques liés à l'utilisation des terminaux mobiles personnels (PC et/ou Smartphone) dans la chaîne de sécurité de l'entreprise.

* *cf nota p.7*

Durée* : 3 heures

Objectifs :

- Appréhender les multiples facettes de la sécurité au sein d'une organisation.
- Connaître les métiers directement impactés par la cybersécurité.
- Anticiper les difficultés courantes dans la gestion de la sécurité.

Contenu détaillé :

Présentation des publications/recommandations

- Guides de l'ANSSI
- Recommandations de la CNIL
- Recommandations de la police et de la gendarmerie
- Club de la Sécurité de l'information Français, Club des experts de la sécurité de l'information et du numérique (CLUSIF/CESIN), etc.
- Observatoires zonaux de la Sécurité des systèmes d'information (SSI)
- Les CERTs (*Computer Emergency Response Team*)

  Il s'agit ici de sensibiliser les PME à l'importance de la veille sur les différentes documentations disponibles.

Présentation des différents métiers de l'informatique (infogérance, hébergement, développement, juriste, etc.)

Méthodologie pédagogique pour responsabiliser et diffuser les connaissances ainsi que les bonnes pratiques internes (management, sensibilisation, positionnement du référent en cybersécurité, chartes, etc.)

Insister sur les messages que le référent en cybersécurité doit transmettre aux utilisateurs finaux des entreprises. Présenter le principe des chartes informatiques que chaque utilisateur doit connaitre.

Maîtriser le rôle de l'image et de la communication dans la cybersécurité

- Surveillance de l'e-réputation
- Communication externe
- Usage des réseaux sociaux, professionnel et personnel

Méthodologie d'évaluation du niveau de sécurité

Présentation d'un audit de sécurité (réglementation, avantages, coût etc.).

Actualisation du savoir du référent en cybersécurité

Les découvertes en matière de cybersécurité sont nombreuses, rapides et les méthodes d'attaques évoluent en permanence. Il est donc nécessaire que le référent en cybersécurité connaisse les grandes actualités du domaine.

Gérer un incident / Procédures judiciaires

Identifier clairement le point de contact dans l'entreprise ainsi que son rôle (lien avec les services de police, résilience du SI de l'entreprise etc.).

* *cf nota p.7*

Durée* : 3 heures

Objectif :

- Appréhender la protection de l'innovation à travers les outils informatiques

Contenu détaillé :

- Les modalités de protection du patrimoine immatériel de l'entreprise

  L'objectif est de présenter les différentes mesures et éventuelles obligations en la matière, comme le dispositif de zone à régime restrictif (ZRR) concourant à la protection du potentiel scientifique et technique de la Nation (PPST).

- Droit de la propriété intellectuelle lié aux outils informatiques

  Il s'agit ici de donner les moyens nécessaires aux entreprises ayant des données importantes pour connaitre les tenants et les aboutissants des contrats, comme par exemple l'infogérance et le Cloud Computing.

- Cyber-assurances

  Présentation d'un domaine nouveau et émergent. L'objectif est de donner les clés nécessaires à une entreprise dans le cas où elle souhaiterait souscrire à une offre de cyber-assurance.

- Cas pratiques

  Présentation de cas de cyber-attaques avérés.

* *cf nota p.7*

Durée* : 6 à 9 heures

Objectifs :

- Savoir sécuriser le SI interne
- Savoir détecter puis traiter les incidents
- Connaître les responsabilités juridiques liées à la gestion d'un SI

Contenu détaillé :

Analyse de risque (Expression des besoins et identification des objectifs de sécurité -EBIOS / Méthode harmonisée d'analyse des risques - MEHARI)

Définir les besoins auxquels répondre à travers les principes et domaines de la SSI

Principes et domaines de la SSI afin de sécuriser les réseaux internes

Développement de la notion de défense en profondeur évoquée précédemment.

- Politique et stratégie de sécurité
- Gestion des flux, notamment réseaux sans fil / architecture réseaux (cloisonnement du réseau)
- Gestion des comptes, des utilisateurs, des privilèges selon le besoin d'en connaître
- Gestion des mots de passe
- Gestion des mises à jour
- Journalisation et analyse
- Gestion des procédures
- Plan de continuité d'activité (PCA) / Plan de reprise d'activité (PRA)
- Virtualisation / cloisonnement

Détecter un incident

Gestion de crise

- Traitement technique de l'incident
- Procédure organisationnelle et communication
- Reprise d'activité

Méthodologie de résilience de l'entreprise

Traitement et recyclage du matériel informatique en fin de vie (ordinateurs, copieurs, supports amovibles, etc.)

Aspects juridiques

- Responsabilité en l'absence de conformité des infrastructures
- Cyber-assurances

* *cf nota p.7*

Durée* : 3 heures

Objectifs :

- Connaître les techniques de sécurisation d'un SI, partiellement ou intégralement externalisé.

Contenu détaillé :

Les différentes formes d'externalisation

- Les contrats de services « classiques » : *Infrastructure as a Service (IaaS), Platform as a Service (PaaS) et Software as a Service (SaaS)*
- Enjeux du *Cloud Computing*
- Techniques de sécurité lors de l'externalisation (chiffrement des données…)

Comment choisir son prestataire de service ?

Quels sont les points clés, techniques et organisationnels, de sécurité à bien identifier lors du choix d'un prestataire ?
Aborder la notion et le contexte de certification / qualification des produits.

- Présentation du référentiel de l'ANSSI *Maîtriser les risques de l'infogérance*
- Présentation de la qualification *SecNumCloud* applicable aux prestataires de services d'informatique en nuage

Aspects juridiques et contractuels

- Connaître les bases juridiques pour protéger son patrimoine économique lors de l'externalisation d'un SI
  Exemple : qui est propriétaire des données (même après la fin du contrat) ?
- Obligations en matière d'utilisation, de localisation et de transfert de données
  La CNIL
  Règlement général sur la protection des données (RGPD)

** cf nota p.7*

Durée* : 9 à 12 heures

Objectifs :

- Connaître les règles de sécurité pour gérer un site internet

Contenu détaillé :

Menaces propres aux sites internet

Approche systémique de la sécurité (éviter l'approche par patches)

Configuration des serveurs et services

HTTPS et Infrastructure de gestion de clés (IGC)

Services tiers

Avantages et limites de l'utilisation d'un Content Management System (CMS ou Gestion des contenus) et / ou développement web

Sécurité des bases de données

Utilisateurs et sessions

Obligations juridiques réglementaires

- Le e-commerce
- La Loi pour la confiance dans l'économie numérique (LCEN), la CNIL, *Payment Card Industry-Data Security Standard (PCI-DSS)*
- Règlement général sur la protection des données (*RGPD*)

** cf nota p.7*

Pour aller plus loin

La sécurité économique au quotidien en 22 fiches thématiques, à destination des TPE/PME
www.entreprises.gouv.fr/information-strategique-sisse/outils

Guides techniques et bonnes pratiques de l'ANSSI
www.ssi.gouv.fr/entreprise/bonnes-pratiques
www.ssi.gouv.fr/guide-bonnes-pratiques/
http://www.ssi.gouv.fr/surfez-zen-infographie/
https://twitter.com/anssi_fr : #CyberVigilant

Protection du potentiel scientifique et technique de la Nation, site du SGDSN

SISSE Service de l'Information Stratégique et de la Sécurité Économiques

Service de l'information stratégique et de la sécurité économique
Télédoc 726 – 120 rue de Bercy F - 75572 Paris Cedex 12
Tél : (33) 1 53 18 53 01

https://www.entreprises.gouv.fr/information-strategique-sisse

Agence nationale de la Sécurité des Systèmes d'Information
ANSSI - 51, boulevard de la Tour-Maubourg - 75700 PARIS 07 SP
www.ssi.gouv.fr
communication@ssi.gouv.fr
twitter.com/ANSSI_FR

Maquette réalisée par le bureau de la communication (DGE) - décembre 2017

DGE
DIRECTION GÉNÉRALE DES ENTREPRISES

www.entreprises.gouv.fr