**G-echo**
6 Avenue de la Gare - C24
31380 Garidech
+33.6.03.62.14.40
contact@g-echo.fr

# Programme de formation

Elaboration de la Politique de Sécurité de l'Information de votre Entreprise

## But de la formation

Cette formation a pour but de donner la capacité à l'entreprise concernée d'élaborer sa propre Politique de Sécurité de l'Information (PSI).

A l'issue de la formation l'entreprise dispose d'une première version de sa PSI, lui permettant ainsi de mettre en place la gouvernance de la cybersécurité.

## Objectifs pédagogiques

1. Etre en capacité d'élaborer sa Politique de Sécurité de l'Information (PSI).

## Pré-requis

- Connaissances générales en sécurité de l'information
- Connaissance du système d'information de l'entreprise
- Culture de la sécurité de l'information ou de l'intelligence économique

## Type de public

- Toute personne de l'entreprise en responsabilité de la sécurité de l'information (RSI, RSSI).

## Moyens pédagogiques

- Support de cours en français
- Présentation Powerpoint
- Fourniture de l'outil Excel d'autodiagnostic pour l'état des lieux
- Fourniture du modèle Word pour la formalisation de la PSI

## Sanction de la formation

- Document de PSI
- Attestation de suivi de formation
- Cette formation n'est pas certifiante

## Méthodes pédagogiques

- Cours magistral
- Exercices pratiques pilotés par le formateur
- Utilisation d'exemples concrets

## Durée

14 heures (2 jours).

## Programme

### 1ère journée

#### Matinée

Introduction : la gouvernance en cybersécurité

La Politique de Sécurité de l'Information (PSI)

Les fondements de la PSI

Exercice 1 : la classification des informations de l'entreprise

**Après-midi**

L'analyse de risques : la méthode EBIOS 2018 RM

Exercice 2 : Les évènements redoutés de l'entreprise

La structure d'une PSI selon la norme ISO 27002

Exercice 3 : autodiagnostic des mesures existantes selon le canevas ISO 27002

**2ème journée**

**Matinée**

Chapitres 5 & 6 : Politiques et organisation de la sécurité de l'information

Exercice 4 : Définir les responsabilités et l'organisation de la sécurité de l'information de l'entreprise

Chapitre 7 : les ressources humaines

Exercice 5 : Définir les règles relatives aux ressources humaines

Chapitres 8 & 9 : La gestion des actifs et leur accès

Exercice 5 : Définir les règles relatives à la gestion des actifs et leur accès

Chapitre 11 : La sécurité physique et environnementale

Exercice 6 : Définir les règles de sécurité physique

**Après-midi**

Chapitres 10, 12,13, 14 & 17 : Les aspects techniques de la sécurité de l'information

Exercice 6 : Définir les règles relatives aux aspects techniques (cryptographie, exploitation, infrastructure, maintenance, continuité).

Chapitre 15 : Relation avec les fournisseurs

Exercice 7 : Définir les règles régissant les relations avec les tiers

Chapitre 16 : La gestion des incidents

Exercice 8 : Définir l'organisation relative à la gestion des incidents

Chapitre 18 : La conformité

Exercice 9 : Définir les règles relatives à l'obtention de la conformité légale et réglementaire.