
G-ECHO cybersécurité

Newsletter n°5 - Mai 2018

## GOUVERNANCE & PROTECTION DES INFORMATIONS

Chefs d'entreprises, responsables et décisionnels, quels modèles organisationnels pour tirer bénéfice de la protection des données ?

**>>> Inscrivez-vous à nos séminaires et formations**

Les chefs d'entreprises, responsables ou décisionnels ont maintenant pris conscience de la nécessité de se protéger contre les cyber-risques. L'actualité nous rappelle fréquemment que les entreprises doivent faire face à des menaces internationales très organisées dont la concrétisation peut provoquer des dommages considérables.
En effet la transition numérique, la mobilité, la gestion des données personnelles, l'infogérance externalisée, ou la connectivité, au même titre que les brevets ou la R&D, constituent des valeurs ajoutées de l'Entreprise qu'il convient de protéger.

Pourtant, la prise en compte des risques qui les concernent est encore trop souvent considérée comme affaire d'expert alors qu'elle est directement liée aux enjeux vitaux de l'entreprise et qu'elle devrait s'intégrer de façon naturelle dans le processus plus général de la gouvernance des risques.

D'autre part l'évolution importante des législations européennes ou françaises telles que le règlement général sur la protection des données (RGPD) ou la loi de programmation militaire nécessite une organisation interne incluant l'ensemble des directions parties prenantes (juridique, RH, métiers, audit, systèmes d'informations, sûreté...).

Dans ces conditions quels modèles organisationnels faut-il adopter pour mettre en place une stratégie et une gouvernance de la sécurité du système d'information ?

>>> En savoir + <<<

## QU'EST-CE QUE LA GOUVERNANCE DE LA CYBERSÉCURITÉ ?

Un projet de mise en place de gouvernance de la cybersécurité ne se limite pas à la conduite d'une série d'analyse de risques. Il doit notamment intégrer les actions ci-dessous avec le pilotage d'un responsable dédié au plus haut niveau de l'Entreprise ayant établi une relation privilégiée et constructive avec le responsable de la sécurité de l'information et les différents responsables de directions.

**Définir la gouvernance de la protection des systèmes d'information**
L'évolution majeure va consister principalement à intégrer harmonieusement les politiques de sécurité propres à chaque système à la politique du Groupe et / ou de ses entités.
Dans ce cadre des redéfinitions des responsabilités sont certainement à envisager.
Si cette organisation existe déjà, ce projet va constituer une évolution majeure qui nécessitera son adaptation pour en élargir la gouvernance.

**Disposer de la cartographie de l'ensemble des systèmes d'information**
Cette cartographie est nécessaire pour définir les priorités en fonction du niveau de sensibilité des systèmes et organiser le déroulement des analyses de risque.
Les analyses de risque doivent être conduites pour tous les systèmes identifiés dans la cartographie selon la planification établie. Le processus de l'analyse de risques doit être formalisé et être établi comme référence unique (préconisation ISO 27001). L'expression du résultat de l'analyse s'effectue selon un canevas unique.

**Valider la sécurité des systèmes d'information**
La validation (ou homologation) consiste à s'assurer du fait que la solution satisfait aux exigences de sécurité dans les conditions d'usage pour lesquelles elle a été prévue.
Une procédure de validation doit être définie dès la phase initiale du projet. Elle précise notamment la composition de l'autorité de validation, les responsabilités afférentes ainsi que le contenu du dossier afférent.

**Mettre en place la protection physique**
La protection des systèmes d'information s'intègre dans une protection physique des sites déjà existante. Les analyses de risques devront s'assurer que la protection physique est d'un niveau cohérent avec la sensibilité des systèmes concernés.

**Gérer les incidents de sécurité des systèmes d'information**
Il est nécessaire de mettre en place une structure de gestion des incidents de sécurité dès la phase initiale et vraisemblablement de la considérer comme un sous-projet pour y aborder tous les aspects (organisationnels, techniques, définition de l'incident de sécurité, exploitation, pertinence d'un SOC...).

**Évaluer le niveau de sécurité**
L'évaluation est un outil de la gouvernance. Elle devra exploiter ou adapter celle déjà existante. Elle devra être créée si ce n'est pas le cas en s'accordant au préalable sur la notion de "niveau de sécurité" et les indicateurs qui permettent de l'exprimer.

G-echo, expert en cybersécurité, vous accompagne dans cette démarche et met à votre service toutes ses compétences en gouvernance et protection des informations pour valoriser votre SI.

En savoir +

## DATES DES SÉMINAIRES ET FORMATIONS

- **le 23 Mai, de 14h00 à 18h00:**
Séminaire Gouvernance et protection des informations, Toulouse
- **du 24 au 25 Mai:**
Formation Gouvernance et protection des informations, Toulouse
- **le 28 Mai, de14h00 à 18h00:**
Séminaire Gouvernance et protection des informations, Paris
- **Du 31 Mai au 01 Juin:**
Formation Gouvernance et protection des informations, Paris
- **le 06 Juin, de 14h00 à 18h00:**
Séminaire Gouvernance et protection des informations, Toulouse
- **du 13 Juin au 14 Juin:**
Formation Gouvernance et protection des informations, Toulouse
- **le 20 Juin, 14h00 à 18h00:**
Séminaire Gouvernance et protection des informations, Paris
- **Du 26 Juin au 27 Juin:**
Formation Gouvernance et protection des informations, Paris

>>> Inscrivez-vous <<<

Pour trouver d'autres formations rendez-vous sur notre site internet www.g-echo.fr

À suivre...

Dans notre prochaine Newsletter nous parlerons de la norme 27001

**wwww.g-echo.fr**