Auteur : Lionel GUILLET
Expert en Management de la Sécurité de l'Information

Pour inscrire le PCA dans la durée : Piloter la sécurité de l'information de l'entreprise

L'expression de la volonté de la Direction, la pluridisciplinarité des démarches, l'engagement sur la durée, … les recommandations de Robert BERGERON « 10 conseils pour réussir son P.C.A. » soulignent la nécessité de disposer des moyens d'une gestion formelle de la Sécurité de l'Information dans tous les processus et dans toutes les activités de l'entreprise, qu'elle soit publique ou qu'elle soit privée. Ces moyens s'inscrivent dans un cadre normatif et méthodologique qu'il est utile de connaître.

Parce que ça n'arrive pas qu'aux autres …

L'ACCIDENT, L'ERREUR, LA MALVEILLANCE, LA NON-CONFORMITE, … votre entreprise n'est pas épargnée des menaces naturellement associées aux activités économiques et de LEURS CONSEQUENCES NEGATIVES sur la DISPONIBILITE, L'INTEGRITE ET LA CONFIDENTIALITE DE SON SYSTEME D'INFORMATION (*).

Parce que les obligations de protéger l'information de l'entreprise ne manquent pas

Pour souscrire aux objectifs de qualité et d'optimisation des gestions, pour assurer la continuité des activités, pour protéger les données patrimoines de l'entreprise, pour respecter la législation et la réglementation, … les raisons majeures de garantir le meilleur niveau de sécurité possible à votre système d'information sont nombreuses.

Mettre en place un écosystème favorable à l'amélioration continue de la sécurité de l'information

Face à cette conjoncture, la mise en place d'une organisation pour le pilotage et le management de la Sécurité de l'Information a pour objectif de garantir une approche coordonnée, dûment formalisée, et régulièrement évaluée, du niveau de sécurité de l'entreprise et des actions accomplies pour la maintenir et la faire progresser.

La sécurité de l'information, pas seulement les sécurités informatiques

La démarche intéresse toutes les ressources nécessaires à la protection globale des données et des actifs (**) sensibles de l'entreprise, dans tous les domaines concernés, techniques, organisationnels,

ressources humaines, juridiques (Vous trouverez une présentation sommaire du cadre normatif en annexe)

Respecter une approche méthodique d'intégration de la Sécurité de l'Information dans tous les processus de l'entreprise

- Mettre en place un Système de Management de la Sécurité de l'Information (S.M.S.I.)
- Connaître et mettre en œuvre les obligations juridiques générales et spécifiques attachées à la Sécurité de l'Information
- Publier une Politique de Sécurité du Système d'Information (P.S.S.I.) par référence aux objectifs de sécurité et aux enjeux d'activité de l'entreprise
- Réaliser des audits de sécurité et des cartographies de risques
- Disposer d'un Plan de continuité d'activité (P.C.A.)
- Élaborer des plans d'actions et préventives
- Evaluer régulièrement les résultats de ces actions
- Suivre et mesurer le niveau de sécurité de votre système d'information par la mise en place d'indicateurs et de tableaux de bord
- Bâtir un dispositif de communication dédié
- Organiser des séances d'information et de sensibilisation ciblées (dirigeants, encadrement, membres du personnel)
- Sensibiliser à la protection des données à caractère personnel
- Disposer d'un Correspondant Informatique et Libertés (C.I.L.) auprès de la C.N.I.L.

…

la Sécurité de l'Information au service de la qualité pour une approche globale des risques opérationnels

Sans pouvoir les confondre, parce que basées sur des normes et des référentiels différents, Qualité et Sécurité sont étroitement complémentaires pour répondre aux risques et vulnérabilités liés aux activités de l'entreprise.

Plans d'action, évaluation, prévention, correction … qualité et sécurité s'inscrivent dans des démarches similaires de recherche continue d'amélioration.

Par contre, la Sécurité souscrit à des normes et des méthodes spécifiques afin de servir la disponibilité, l'intégrité et la confidentialité dont la qualité a besoin pour garantir délais, fiabilité, accessibilité et conformité de votre production.

La Sécurité de l'Information pour Garantir au plan de continuité d'activité l'environnement favorable à sa mise en place et son maintien en conditions opérationnelles.

Le Système de Management de la Sécurité de l'Information, par sa portée et sa permanence, garantit au Plan de Continuité d'activité le contexte fonctionnel et opérationnel indispensable à la préservation de son intégrité et de son efficacité dans la durée.

C'est ainsi que le P.C.A. trouve justement sa place dans le S.M.S.I., une place essentielle en termes de disponibilité et de continuité de service, enjeu majeur pour l'entreprise.

La sécurité de l'information mérite bien votre intérêt

Nous l'avons fait valoir dès le début de l'article, le périmètre de la Sécurité de l'Information dépasse largement le périmètre informatique, sans, pour autant, ignorer l'importance de celui-ci dans l'ensemble des gestions qui se doivent. Nous avons amorcé une énumération des domaines concernés, les ressources humaines, les sécurités juridiques, la sécurité d'organisation … des domaines qui valent bien de vous proposer régulièrement une information quelque peu approfondie sur un sujet ou sur un autre, au fil du temps et au gré de l'actualité.

(*)**LE SYSTEME D'INFORMATION** désigne l'ensemble des moyens (organisation, site, ressources humaines, réglementation, matériel, réseau, logiciel …) mis en œuvre pour collecter, traiter, stocker, restituer l'information à la base de l'activité de l'entreprise quelle que soit sa nature

(**) **UN ACTIF** désigne une ressource ou un processus dont la valeur est estimée importante pour le fonctionnement du système d'information de l'entreprise.

Le cadre normatif de la Sécurité de l'Information

La confusion est fréquente, pourtant le management de la Sécurité de l'Information ne s'intéresse pas qu'aux seules sécurités informatiques, loin de là, même si celles-ci occupent une place particulière dans le dispositif, compte tenu de la dépendance désormais des systèmes d'information à leur égard.

La norme Iso 27001 précise le périmètre d'application de la sécurité du système d'information et publie une liste des domaines à investir :

1. Une politique interne de sécurité
2. Une gestion organisée de la sécurité
3. Un inventaire et une hiérarchisation des données et des actifs de l'Organisme
4. La sécurité liée aux ressources humaines
5. La sécurité physique et environnementale
6. La sécurité des matériels
7. Les sécurités informatiques, développement, déploiement, exploitation et maintenance des ressources informatiques en réseau
8. Le contrôle des accès au système d'information
9. La gestion des incidents de sécurité
10. La gestion d'un plan de continuité d'activité
11. La conformité aux exigences légales et réglementaires

Cet inventaire met en évidence la nature de la démarche, une démarche pluridisciplinaire qui associe de nombreux acteurs intéressés à la Sécurité de l'Information dans l'entreprise.

De son côté, la norme Iso 27002, encore appelée "code de bonnes pratiques", édicte les règles applicables dans chacun de ces domaines.

Par conséquent, c'est dans ce cadre normatif et par référence au contexte, aux enjeux et aux objectifs métiers de l'entreprise qu'il convient de bâtir le référentiel de pilotage et de gestion de la Sécurité de l'Information.