

Sensibilisation des utilisateurs aux risques liés à l'usage des systèmes d'information

Avoir un comportement responsable en toute circonstance

Référence	Niveau	Durée	Pré-requis
AT ME 102	Niveau 1	0,5 jour	Aucun

Avis de l'expert

L'importance du facteur humain dans la sécurité du système d'information n'est plus à démontrer et représente aujourd'hui un enjeu majeur en matière de sécurité informatique.

Compte tenu de l'importance d'impliquer tous les acteurs de l'entreprise dans une démarche de responsabilisation, la formation des utilisateurs des moyens informatiques est devenue indispensable, des organismes de tutelles et de normalisation en ayant d'ailleurs fait une exigence réglementaire.

Cette formation de sensibilisation à la sécurité informatique a pour but d'impliquer et de responsabiliser le personnel d'encadrement, les utilisateurs et/ou des informaticiens en leur faisant assimiler les bases de la sécurité. Il s'agit également d'inculquer les bons réflexes, pour protéger le SI de l'entreprise et éviter les erreurs classiques.

Bénéfices métier

- Fournir ou rappeler les définitions de base en matière de sécurité ;
- Dresser un panorama des risques et des menaces qui pèsent sur l'entreprise
- Décrire les bonnes pratiques pour se protéger et les bons réflexes à acquérir
- Responsabiliser les utilisateurs dans l'usage des moyens informatiques
- Renforcer le changement de comportement des utilisateurs

Itinéraire pédagogique

Partie 1 : Les enjeux et les risques liés à l'usage des systèmes d'information

- Le vocabulaire et les définitions de base (Information (I), Données à caractère personnel, Systèmes d'information (SI), Sécurité des Systèmes d'Information (SSI), Système de Management de la Sécurité de l'Information (SMSI),).
- Quelles sont les obligations légales applicables au contexte professionnel (loi « informatique & libertés », code pénal / code civil, code de santé public, Hadoppi, CLEN, LOPPSI,) ?
- Quels sont les risques liés à l'usage du réseau Internet et à la messagerie ?
- Les rôles et les responsabilités respectives au sein de l'établissement.
- La gouvernance de la sécurité des systèmes d'information.
- Ce qu'impose le régulateur ou notre autorité de tutelle.

Partie 2 : Les mesures de sécurité et les règles à appliquer

- Les mesures de sécurité mises en œuvre par la DSI (contrôle d'accès, lutte contre les virus informatique, filtrage, traçabilité,)
- Les règles de bon usage de la messagerie
- Les règles de bon usage d'Internet (navigation, réseaux sociaux, forum,)
- Les règles de bon usage des applications internes
- Les principes élémentaires pour avoir un comportement responsable
- Les règles à respecter vis-à-vis du personnel extérieur
- Les principes de sécurité de son environnement de travail.
- Comment contribuer à la protection des informations traitées dans nos services ?
- Les processus d'alerte et de remontée d'incident prévus au sein de l'organisme

Comment se déroule le stage ?

Présentation pédagogique des enjeux, des risques et des mesures de sécurité.

Echanges entre les participants sur les bonnes pratiques au quotidien.

Public concerné

Cadres et dirigeants de l'organisme.

Utilisateurs des moyens informatiques.

Equipes informatiques.