Institut de Droit Pratique
Formation & Mooc

5 -7 rue Villehardouin 75003 Paris Tél : 01.53.26.95.52 Email : info@idp-formation.com Internet : www.idp-formation.com

Les bonnes pratiques de sécurité informatique, du DSI à l'utilisateur final.

Aspects informatiques, organisationnels et juridiques.

Public :

- Tout utilisateur traitant ou accédant à des données personnelles de clients, prospects ou membres du personnel

- Personne ayant en charge l'informatique et les réseaux au sein de son entreprise ou service (dirigeant de TPE, PME, chef de service...).

Objectif :

- Maîtriser les fondamentaux de la sécurité informatique afin d'éviter des intrusions, vols ou pertes de données confidentielles (personnelles ou non).

- Acquérir des réflexes (ou en abolir d'autres) et adopter une véritable hygiène informatique.

- Maitriser les risques juridiques à la lumière du RGPD et les enjeux de responsabilité.

Durée :

1 à 3 jours (une journée = 7 h en présentiel, 6 h en distanciel)

La formation complète, en présentiel ou distanciel, dure trois jours. Mais elle est **modulable** en fonction des besoins de nos clients (par exemple, la partie consacrée aux audits ou les enjeux juridiques peuvent être exclus, ou au contraire, être le thème unique de la formation.

S'agissant des thématiques purement informatiques, certaines entreprises ont déjà sécurisé partiellement leur système (par exemple, les messageries sont sécurisées, les clés USB bloquées, les mails cryptés…), permettant de focaliser sur les points restant à traiter ou améliorer

L'ensemble des collaborateurs d'une entreprise ou d'un établissement peuvent bénéficier d'une formation de sensibilisation aux bonnes pratiques informatiques

Coût :

1 jour : 1890 € net 2 jours : 3490 € 3 jours : 4990 €

Le nombre de participants est limité à 15 par session, sauf pour la formation de sensibilisation d'une durée d'une journée, qui peut être organisée à l'attention de l'ensemble des collaborateurs.

Programme (modulable) :

Qu'est la sécurité informatique ?

Les sessions

L'authentification et les mots de passe

- Pourquoi
- Qu'est-ce qu'un bon mot de passe
- L'authentification forte multifacteurs
- Ce qu'il ne faut surtout pas faire
- Transmettre un mot de passe
- Stocker ses mots de passe

Les clés USB

- Ce qu'il ne faut pas faire : utiliser les clés USB personnelles sur un poste de travail professionnel
- Ce qui est recommandé

Les ordinateurs portables et smartphones

- Les dangers de la connexion automatique
- Sécurisation physique
- Verrouillage de session

Le chiffrement des unités de stockage, des dossiers et documents et des smartphones

- Pourquoi chiffrer ?
- La certification électronique
- Le chiffrement sous Windows
- Le chiffrement sous MacOs
- Les smartphones

Les Mails ou courriels

- Recevoir une pièce jointe
- Envoyer une pièce jointe
- Dangers des mails indépendamment des pièces jointes
  - Les images
  - Les liens suspects
  - Le phishing ou hameçonnage
  - Les hoax et les fake-news

- La signature et le chiffrement par certificat
  - Principe
  - Obtenir un certificat
  - La signature par certificat
  - Le Chiffrement par certificat

Virus, antivirus et firewall (pare-feu)

- Les virus informatiques
  - Les ransomwares
  - Les key loggers
  - Les Ad-wares
  - Les mineurs de crypto monnaies
  - Les chevaux de Troie ou trojan (trojan horses)
  - Les portes dérobées ou backdoors
  - Les rootkits
  - Les vers ou worms
  - Les virus perturbant ou détruisant le matériel
- Les Antivirus
- Les Firewall ou pare-feu

Le WIFI

- Le WIFI en interne : séparer le réseau local de celui accessible aux visiteurs
- Le WIFI à l'extérieur des locaux

Le stockage des données

- Stockage local au poste
- Stockage partagé : Les droits d'accès
- Stockage en cloud avec chiffrement
- Les sauvegardes

L'obsolescence

- Mise à jour du système d'exploitation et des logiciels
- Destruction des machines obsolètes

La cartographie des données

- Une obligation instaurée par le RGPD pour les données à caractère personnel
- L'évaluation de la taille et de la complexité du système d'information (SI)
- La détermination des données à caractère personnel et des traitements à leur appliquer
- Le suivi de l'évolution du système d'information
- L'externalisation du système d'information
- Méthodologies de la cartographie des données à caractère personnel (DCP)
  - L'individu au centre du processus
  - Analyse des processus et de la technique
- Bonnes pratiques de cartographie

Maintenir à jour

Intégrer la cartographie aux biens de l'entreprise ou de l'établissement

Construire une vue graphique

Construire un référentiel des traitements

Être attentif aux données échangées ou reçues

Faire la chasse aux mauvaises pratiques

Conclusion sur la cartographie des données à caractère personnel (DCP)

Les audits

Qu'est un audit ?

Audit de Vulnérabilités

Audit de Conformité

Aspects juridiques de la sécurité informatique

Introduction

Les enjeux de responsabilité

La responsabilité civile et l'indemnisation d'un préjudice

La responsabilité pénale

La spécificité des données à caractère personnel

Le RGPD : une obligation de moyen ou de résultat ?

Le régime des sanctions

Le consentement au traitement des données à caractère personnel et ses limites

Les opérateurs de services essentiels (OSE)

Contact :

Raymond Taube

Institut de Droit Pratique

5 rue Villehardouin 75003 Paris

06.60.46.45.45 raymond.taube@idp-formation.com