

Dernière mise à jour du document : 23 mars 2022

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

Aspects informatiques, organisationnels et juridiques

Public et prérequis :

- 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...).

Prérequis : aucun. Si la formation se destine exclusivement aux DSI, leur compétence informatique est présumée.

Objectif :

L'objectif de la formation est de doter les stagiaires des aptitudes et compétences suivantes :

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

D'un point de vue opérationnel, le stagiaire doit pouvoir utiliser les acquis de la formation pour réduire significativement les risques et les conséquences de perte de données, qu'elle soit accidentelle ou malveillante.

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

Dates et délais d'accès :

Les formations étant organisées en intra, les dates de réalisation sont déterminées d'un commun accord entre l'IDP et son client. En général, il faut deux à trois semaines pour monter une formation, mais ce délai peut varier en fonction de plusieurs critères, notamment la période de l'année.

Une fois les dates de la formation déterminées, les modalités de participation et les délais d'accès sont déterminés par l'employeur des stagiaires.

Coût net (exo TVA - Art. 261-4-4 du CGI):

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) :

Remarque : compte tenu de la modularité du programme, la séquence ne peut être faite que lorsque son contenu et sa durée auront été déterminés

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 perturbants ou détruisantS 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)

Analyse fine des besoins des stagiaires :

Au plus tard deux semaines avant le début de la formation, les stagiaires ou leur employeur ont la possibilité d'adresser des suggestions ou questions à appreciations@idp-formation.com, afin qu'il y soit répondu collectivement.

En outre, dans ce même délai, le programme ci-dessus peut être modifié, affiné ou aménagé en fonction des besoins particuliers des participants. La formation est conçue pour être accessible sans prérequis, donc par l'utilisateur final de tout ordinateur ou même smartphone accédant à des données professionnelles. Elle peut néanmoins bénéficier aux membres du service informatique soucieux de sensibiliser ou former d'autres personnels en interne, d'améliorer les processus et procédures de sécurité informatique, voire d'en modifier fondamentalement l'organisation. La formation comporte également un volet juridique commun à tous types de participants, pour lequel aucun pré-requis n'est demandé.

Si vous souhaitez qu'une prestation soit destinée uniquement à une catégorie de personnels (utilisateur final sans compétence informatique, service informatique, DSI...), vous pouvez le préciser à l'adresse susmentionnée ou prendre directement contact avec l'IDP (voir ci-dessous). Il en va de même si vous souhaitez une formation « sur mesures ».

Contact et référent pédagogique :

Raymond Taube

IDP

5 rue Villehardouin 75003 Paris

06.60.46.45.45 raymond.taube@idp-formation.com