Cours de synthèse de 1 jour(s)
Réf : SES

Participants

Tous les utilisateurs ayant accès au Système d'Information via un poste informatique.

Pré-requis

Aucune connaissance particulière.

Prix 2020 : 890€ HT

Dates des sessions

AIX
30 nov. 2020, 12 fév. 2021
09 avr. 2021, 21 mai 2021
27 aoû. 2021

BORDEAUX
23 nov. 2020, 08 jan. 2021
09 avr. 2021, 28 mai 2021
06 aoû. 2021

BRUXELLES
16 nov. 2020, 15 jan. 2021
12 mar. 2021, 18 juin 2021
09 juil. 2021

CLASSE A DISTANCE
16 nov. 2020, 22 jan. 2021
26 fév. 2021, 02&09 avr. 2021
07 mai 2021, 25 juin 2021
09 juil. 2021, 13 aoû. 2021
24 sep. 2021

GENEVE
16 nov. 2020, 05 mar. 2021
07 mai 2021, 03 sep. 2021

GRENOBLE
27 nov. 2020

LILLE
16 nov. 2020, 08 jan. 2021
09 avr. 2021, 25 juin 2021
06 aoû. 2021

LUXEMBOURG
16 nov. 2020, 05 mar. 2021
07 mai 2021, 03 sep. 2021

LYON
20 nov. 2020, 29 jan. 2021
02 avr. 2021, 02 juil. 2021
27 aoû. 2021

MONTPELLIER
20 nov. 2020

NANTES
27 nov. 2020, 08 jan. 2021
09 avr. 2021, 28 mai 2021
27 aoû. 2021

ORLEANS
16 nov. 2020

PARIS
16 nov. 2020, 22 jan. 2021
26 fév. 2021, 02&09 avr. 2021
07 mai 2021, 25 juin 2021
09 juil. 2021, 13 aoû. 2021
24 sep. 2021

RENNES
30 nov. 2020

SOPHIA-ANTIPOLIS
27 nov. 2020, 12 fév. 2021
09 avr. 2021, 21 mai 2021
27 aoû. 2021

Cybersécurité, sensibilisation des utilisateurs

Ce cours vous permettra de connaître les risques et les conséquences d'une action utilisateur portant atteinte à la sécurité du système d'information, d'expliquer et justifier les contraintes imposées par la politique de sécurité, comprendre les principales parades mises en place dans l'entreprise.

OBJECTIFS PEDAGOGIQUES

Comprendre la typologie de risques liés à la sécurité SI et les conséquences possibles
Identifier les mesures de protection de l'information et de sécurisation de son poste de travail
Favoriser la conduite de la politique de sécurité SI de l'entreprise

1) La sécurité informatique : comprendre les menaces et les risques

- Introduction : cadre général, qu'entend-on par sécurité informatique (menaces, risques, protection) ?
- Comment une négligence peut-elle créer une catastrophe ? Quelques exemples. La responsabilité.
- Les composantes d'un SI et leurs vulnérabilités. Systèmes d'exploitation client et serveur.
- Réseaux d'entreprise (locaux, site à site, accès par Internet).
- Réseaux sans fil et mobilité. Les applications à risques : Web, messagerie...
- Base de données et système de fichiers. Menaces et risques.
- Sociologie des pirates. Réseaux souterrains. Motivations.
- Typologie des risques. La cybercriminalité en France. Vocabulaire (sniffing, spoofing, smurfing, hijacking...).

2) La protection de l'information et la sécurité du poste de travail

- Vocabulaire. Confidentialité, signature et intégrité. Comprendre les contraintes liées au chiffrement.
- Schéma général des éléments cryptographiques. Windows, Linux ou MAC OS : quel est le plus sûr ?
- Gestion des données sensibles. La problématique des ordinateurs portables.
- Quelle menace sur le poste client ? Comprendre ce qu'est un code malveillant.
- Comment gérer les failles de sécurité ? Le port USB. Le rôle du firewall client.

3) L'authentification de l'utilisateur et les accès depuis l'extérieur

- Contrôles d'accès : authentification et autorisation.
- Pourquoi l'authentification est-elle primordiale ?
- Le mot de passe traditionnel.
- Authentification par certificats et token.
- Accès distant via Internet. Comprendre les VPN.
- De l'intérêt de l'authentification renforcée.

4) Comment s'impliquer dans la sécurité du SI ?

- Analyse des risques, des vulnérabilités et des menaces.
- Les contraintes réglementaires et juridiques.
- Pourquoi mon organisme doit respecter ces exigences de sécurité ?
- Les hommes clés de la sécurité : comprendre le rôle du RSSI et du Risk manager.
- Agir pour une meilleure sécurité : les aspects sociaux et juridiques. La CNIL, la législation.
- La cybersurveillance et la protection de la vie privée.
- La charte d'utilisation des ressources informatiques.
- La sécurité au quotidien. Les bons réflexes. Conclusion.

STRASBOURG

30 nov. 2020, 08 jan. 2021
09 avr. 2021, 25 juin 2021
06 aoû. 2021

TOULOUSE

23 nov. 2020, 26 fév. 2021
12 mar. 2021, 25 juin 2021
27 aoû. 2021

TOURS

23 nov. 2020

Modalités d'évaluation

L'objectif de cette formation étant essentiellement de fournir une synthèse des méthodes et technologies existantes, il n'est pas nécessaire d'avoir recours à une évaluation des acquis.

Compétences du formateur

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

Moyens pédagogiques et techniques

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.

• A l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.

• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.