CONFISEC

Partner for Security

- CONSTRUIRE ENSEMBLE
- VOTRE CYBERSÉCURITÉ

Catalogue des formations 2022

Nous mettons à votre disposition toute notre expertise et tout notre retour d'expérience pour accompagner votre organisme à relever les défis de la sécurité des systèmes d'information, de la résilience et de la protection des données aussi bien sur le plan managérial, technologique qu'humain.

NOUS SOMMES CONFISEC

Le partenaire de confiance pour votre cybersécurité

Nos valeurs

ECOUTE - SERVICE - PROBITÉ INTELLECTUELLE - ENGAGEMENT

SOMMAIRE

EDITO

La formation en cybersécurité, un incontournable pour édifier votre protection contre les cybermenaces

Le Saviez-vous? Toutes les normes ISO renferment une clause intitulée « *Compétences* » évoquant la nécessité de confier la gestion des systèmes de management à des personnes compétentes sur la base d'une formation initiales ou continue.

Les technologies ne peuvent à elles seules suffire même si elles sont aussi indispensables pour protéger vos données. La sécurité de vos données reposera toujours sur les aptitudes des ingénieurs à gérer efficacement les différentes mesures de sécurité tant sur le plan technique qu'organisationnel. Seule la formation initiale et même continue garantira la mise à niveau ou la mise à jour des connaissances et compétences en matière de sécurité des données.

3,5 millions ! C'est le nombre de postes en cybersécurité non pourvus en 2021. Et ce chiffre ne fera que grimper dans les années à venir. Ceci témoigne des défis colossaux que font face aux différentes organisations pour trouver les profils spécialisés dans ce domaine. Quand on ne peut trouver la perle rare, il est donc possible pour chaque entreprise d'investir dans la formation cybersécurité de ses ressources, ce qui au-delà des besoins internes peut s'avérer motivant pour les collaborateurs dans leur plan de carrière.

Toutes les études sérieuses en matière de gestion des ressources humaines projettent les métiers liés à la cybersécurité parmi les métiers du futur. Ce n'est donc pas étonnant d'observer de plus en plus des reconversions professionnelles vers ces métiers qui deviennent une aubaine pour le développement des carrières.

Ces constats nous montrent qu'il existe aujourd'hui des enjeux majeurs d'adaptation des compétences, auxquels seule la formation professionnelle initiale et/ou continue peut répondre. Adaptation, mais aussi individualisation et qualification… C'est tout l'esprit de notre catalogue de formation.

Nous sommes convaincus que ce catalogue répondra à vos attentes et restons disponibles pour tout besoin spécifique en matière de formation sur la sécurité des données.

La Direction Générale CONFISEC

CITATIONS

Investir dans la formation c'est conjuguer au présent mais aussi au futur le souci des hommes et le souci des résultats. »

Philippe BLOCH

Nous sommes ce que nous faisons de manière répétitive, l'excellence n'est donc pas un acte mais une habitude .

Aristote

TYPOLOGIES DES FORMATIONS

FORMATION INTER-ENTREPRISES

- Formation de collaborateurs de plusieurs organismes
- Formation dans les locaux propre ou désigné par CONFISEC
- Dates fixées par CONFISEC
- Logistique à la charge de CONFISEC
- Tarif de participation forfaitaire, public et fixe par participant

Avantages principaux:
- Partage d'expérience
- Échange de méthodes et bonnes pratiques

FORMATION INTRA-ENTREPRISES

- Réunissant uniquement des collaborateurs de votre organisme, dans vos locaux
- Formation spécifique à votre contexte
- Permet d'aborder des problématiques internes propres à votre organisation
- Formation dans les locaux de CONFISEC si vous ne disposez pas de moyens logistiques adéquats
- Sessions planifiées au choix selon les disponibilités des participants

Avantages principaux :
- Confidentialité
- Flexibilité et adaptabilité

COACHING PERSONNALISÉ

- Formation selon vos besoins (choix de modules)
- Plan d'actions défini avec nos consultants formateurs
- Entretien individuel de suivi après chaque module; permettant ainsi de vérifier s'il y a des difficultés lors de la mise en application du plan d'actions

Avantages principaux :
- Formation sur mesure
- Accompagnement

NOS ENGAGEMENTS QUALITE

Nous nous engageons à

- Faire intervenir des formateurs certifiés dans le domaine de la formation dispensée et ayant une expérience terrain
- Fournir des supports de formation de qualité lors des sessions organisées
- Être à l'écoute à travers les évaluations à chaud et à froid des sessions de formations et des formateurs
- Se conformer aux conditions générales de vente
- Traiter dans la mesure du possible aux dysfonctionnements qui peuvent impacter la qualité de la formation
- Limiter le nombre de participants à un maximum de 10 participants par session afin d'allouer un temps conséquent du formateur aux participants

A QUI S'ADRESSE NOS FORMATIONS ?

PUBLIC CIBLE	PLUS-VALUE DES FORMATIONS DISPENSÉES
Dirigeants d'entreprises	• Meilleure connaissance des enjeux sécurité • Aide à l'orientation sur les choix en matière de sécurité de l'information • Meilleure assimilation du cadre règlementaire applicable
RSSI & équipe en charge de la cybersécurité	• Renforcement des compétences • Capacité d'apprendre des pairs • Retour d'expérience terrain des formateurs
DPO & équipe en charge de la protection des données personnelles	• Renforcement des compétences • Approfondissement des connaissances sur la protection des données • Retour d'expérience terrain des formateurs
Informaticiens	• Renforcement de la sensibilisation sur la cybersécurité • Renforcement des aptitudes à protéger le système d'information
Auditeurs & fonctions de contrôle interne	• Renforcement de la capacité à auditer selon des référentiels spécialisés en sécurité • Meilleure assimilation des risques liés à la sécurité de l'information

NOS FORMATEURS

CONFISEC dispose d'une équipe de formateurs hautement qualifiés. La plupart de nos consultants ont acquis une expérience à l'international et sont dotés de certifications internationalement reconnues dans le domaine de la sécurité.

LISTE DES FORMATIONS

DÉSIGNATION DE LA FORMATION	DURÉE	PROFIL DES CANDIDATS	CERTIFICAT
Management de la Sécurité de l'information & Cybersécurité			
Cybersécurité pour les décideurs	01	Dirigeants d'entreprise ou d'activités	✗
ISO 27001 Foundation	02	Managers	✓
ISO 27001 Lead Implementer	05	Managers en sécurité de l'information	✓
ISO 27001 Lead Auditor	05	Auditeurs	✓
ISO 27002 Manager	03	Gestionnaires de mesures de sécurité de l'information & Contrôleurs internes	✓
ISO 27002 Lead Manager	05		✓
ISO 27005 Risk Manager	03	Gestionnaires des risques & Contrôleurs internes	✓
EBIOS Risk Manager	03	Equipe de gestion des risques sécurité SI	✓
MEHARI Risk Manager	03	Equipe de gestion des risques sécurité SI	✓
Etat de l'art	03	Chargés des systèmes d'information	✗
ISO 27032 Lead Cybersecurity Manager	05	Equipe de gestion de la cybersécurité	✓
Continuité d'activité			
ISO 22301 Foundation	02	Managers	✓
ISO 22301 Lead Implementer	05	Managers de la continuité d'activité	✓
ISO 22301 Lead Auditor	05	Auditeurs	✓
Etablir le plan de continuité d'activité de son entreprise	03	Personnes impliquées dans un projet de Plan de continuité d'activité	✗
Protection des données personnelles			
RGPD Foundation	02	Managers	✓
Data Protection Officer	05	Membre d'une équipe de gestion de la conformité	✓

LISTE DES FORMATIONS

DÉSIGNATION DE LA FORMATION	DURÉE	PROFIL DES CANDIDATS	CERTIFICAT
Sécurité des technologies			
Sécurité Windows	**03**	Administrateurs système	✗
Sécurité des réseaux	**03**	Administrateurs réseaux	✗
Lead Pen Test Professionnel	**05**	Membres d'une équipe de gestion de la cybersécurité	✓
Certified Lead Ethical Hacking	**05**	Membres d'une équipe de gestion de la cybersécurité	✓
CURSUS			
Métier RSSI	**13**	RSSI ou Aspirants RSSI	✗
Auditeur sécurité SI	**13**	Auditeurs ou Aspirants auditeurs sécurité SI	✗
Métier consultant sécurité SI	**13**	Aspirants consultant sécurité SI & Consultants en technologies de l'information	✗

PROGRAMME DES FORMATIONS

Management de la sécurité de l'information & cybersécurité

Cybersécurité pour les décideurs

Durée: 1 jour

Objectifs

- Identifier les enjeux de la Cybersécurité
- Lister les atouts business et les responsabilités de la Cybersécurité
- Intégrer la Cybersécurité dans vos processus de management

Audience

- Dirigeants d'entreprises
- Directeurs d'entité
- Managers

Prérequis: Aucun

Contenu de la formation

- Enjeux de la cybersécurité en entreprise (notion d'actifs, menaces, incidents réels, cadre juridique, enjeux business, …)
- Leadership en matière de cybersécurité (niveau d'implication, rôles et responsabilités, politique de sécurité, …)
- Gestion des risques liés à la cybersécurité et contrôles essentiels

ISO 27001 Foundation

Durée: 2 jours

Objectifs

- Comprendre la mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI) conforme à l'ISO 27001.
- Comprendre la relation entre un SMSI (incluant le management des risques et des contrôles) et la conformité aux exigences des déférentes parties prenantes d'une organisation.
- Acquérir les connaissances nécessaires pour contribuer à la mise en œuvre d'un SMSI tel que spécifié dans la norme ISO 27001

Audience

- Managers.
- Professionnel exerçant dans le domaine des technologies de l'information

Prérequis: Aucun

Contenu de la formation

- **Jour 1** - Introduction au concept de Système de Management de la Sécurité de l'Information (SMSI) tel que défini par la norme ISO 27001
- **Jour 2-** Mettre en œuvre des mesures de sécurité de l'information conformes à l'ISO 27002 et examen de certification

ISO 27001 Lead Auditor

Durée: 5 jours

Objectifs

- Comprendre la relation entre le système de management de la sécurité de l'information, le management des risques et les mesures.
- Comprendre les principes, procédures et techniques d'audit de la norme ISO 19011 :2018, et comment les appliquer dans le cadre d'un audit selon la norme ISO 27001.
- Acquérir les compétences nécessaires pour auditer un SMSI conformément aux exigences de l'ISO 27001, et les techniques de gestion d'une équipe d'audit.
- Préparer et compléter un rapport d'audit ISO 27001

Audience

- Auditeur interne
- Equipe de contrôle interne
- Personne désirant diriger des audits de certification ISO 27001 en tant que responsable d'une équipe d'audit
- Consultant désirant préparer et accompagner une organisation lors d'un audit de certification ISO 27001

Prérequis: Une connaissance préalable des normes ISO 27001 et ISO 27002 est recommandée

Contenu de la formation

- **Jour 1-** Introduction à la gestion d'un système de management de la sécurité de l'information selon ISO 27001
- **Jour 2-** Principes d'audit, préparation et déclenchement d'un audit
- **Jour 3-** Activités d'audit sur site
- **Jour 4-** Clôture de l'audit
- **Jour 5-** Examen de certification

ISO 27001 Lead Implementer

Durée: 5 jours

Objectifs

- Comprendre la corrélation entre la norme ISO/CEI 27001 et la norme ISO/CEI 27002, ainsi qu'avec d'autres normes et cadres réglementaires
- Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SMSI
- Savoir interpréter les exigences de la norme ISO/CEI 27001 dans un contexte spécifique de l'organisation
- Savoir accompagner une organisation dans la planification, la mise en œuvre, la gestion, la surveillance, et la tenue à jour du SMSI
- Acquérir l'expertise nécessaire pour conseiller une organisation sur la mise en œuvre des meilleures pratiques relatives au Système de management de la sécurité de l'information

Audience

- Responsables ou consultants impliqués dans le management de la sécurité de l'information
- Conseillers spécialisés désirant maîtriser la mise en œuvre d'un Système de management de la sécurité de l'information
- Toute personne responsable du maintien de la conformité aux exigences du SMSI
- Membres d'une équipe du SMSI

Prérequis: Une connaissance préalable des normes ISO 27001 et ISO 27002 est recommandée

Contenu de la formation

- **Jour 1-** Introduction à ISO/IEC 27001 et initiation d'un SMSI
- **Jour 2-** Planification de la mise en œuvre d'un SMSI
- **Jour 3-** Mise en œuvre d'un SMSI
- **Jour 4-** Surveillance du SMSI, amélioration continue et préparation à l'audit de certification
- **Jour 5-** Examen

ISO 27002 Manager

Durée: 3 jours

Objectifs

- Comprendre la corrélation entre la norme ISO/CEI 27002 et la norme ISO/CEI 27001
- Comprendre la mise en œuvre des mesures de sécurité d'information en conformité avec la norme ISO /CEI 27002
- Développer l'expertise pour soutenir une organisation dans la mise en œuvre, la gestion et le maintien des mesures de sécurité d'information
- Comprendre la formulation et la mise en œuvre des exigences et des objectifs de la sécurité d'information

Audience

- Responsables désirant mettre en œuvre un système de la sécurité d'information (SMSI) conforme aux normes ISO/CEI 27001 et ISO/CEI 27002
- Tout individu responsable de la sécurité d'information dans une organisation
- Membres de l'équipe de sécurité de l'information
- Conseillers spécialisés en technologies de l'information
- Professionnels des TI
- Agents de la protection des données personnelles
- Agents de la sécurité de l'information

Prérequis: Des connaissances fondamentales de la norme ISO/CEI 27002 et des connaissances approfondies sur la sécurité de l'information

Contenu de la formation

- **Jour 1-** Introduction aux mesures de sécurité d'information selon la norme ISO/CEI 27002
- **Jour 2-** Exigences et objectifs de la sécurité de l'information conformes à la norme ISO/CEI 27002
- **Jour 3-** Examen de certification

ISO 27002 Lead Manager

Durée: 5 jours

Objectifs

- Maîtriser la mise en œuvre des mesures de sécurité de l'information en respectant le cadre et les principes de la norme ISO/CEI 27002
- Maîtriser les concepts, les approches, les normes et les techniques nécessaires pour la mise en œuvre et la gestion efficace des mesures de la sécurité d'information
- Comprendre la relation entre les différentes composantes des mesures de sécurité de l'information, y compris la responsabilité, la stratégie, l'acquisition, la performance, la conformité et le comportement humain
- Comprendre l'importance de la sécurité d'information pour la stratégie de l'organisation
- Maîtriser la mise en œuvre des processus de la sécurité d'information
- Maîtriser l'expertise pour soutenir une organisation dans la mise en œuvre, la gestion et le maintien des mesures de la sécurité de l'information
- Maîtriser la formulation et la mise en œuvre des exigences et des objectifs de la sécurité d'information

Audience

- Responsables désirant mettre en œuvre un système de la sécurité d'information (SMSI) conforme aux normes ISO/CEI 27001 et ISO/CEI 27002
- Tout individu responsable de la sécurité d'information dans une organisation
- Membres de l'équipe de sécurité de l'information
- Conseillers spécialisés en technologies de l'information
- Professionnels des TI
- Agents de la protection des données personnelles
- Agents de la sécurité de l'information

Prérequis: Des connaissances fondamentales de la norme ISO/CEI 27002 et des connaissances approfondies sur la sécurité de l'information

Contenu de la formation

- **Jour 1-** Introduction aux mesures de sécurité d'information selon la norme ISO/CEI 27002
- **Jour 2-** Contrôles liés à la gestion des actifs, au contrôle d'accès et à la sécurité des ressources humaines
- **Jour 3-** Contrôles liés à la cryptographie, à la sécurité physique, à la sécurité des communications, sécurité liée à l'exploitation
- **Jour 4-** Contrôles liés à l'acquisition et au développement des systèmes, à la relation avec les fournisseurs, à la gestion des incidents sécurité, à la continuité et à la conformité
- **Jour 5-** Examen de certification

ISO 27005 Risk Manager

Durée: 3 jours

Objectifs

- Acquérir l'expertise nécessaire pour gérer de façon responsable un processus de gestion des risques liés à la sécurité de l'information
- Acquérir une connaissance approfondie des spécificités de la gestion des risques de sécurité de l'information dans le cadre d'un programme de gestion globale des risques d'entreprise
- Obtenir les compétences nécessaires pour accompagner la mise en œuvre efficace d'un processus de gestion des risques liés à la sécurité de l'information au sein d'une organisation

Audience

- Responsables de la sécurité d'information
- Membres d'une équipe de sécurité de l'information
- Tout individu responsable de la sécurité d'information, de la conformité et du risque dans une organisation
- Tout individu mettant en œuvre ISO/IEC 27001, désirant se conformer à la norme ISO/IEC 27001 ou impliqué dans un programme de gestion des risques
- Consultants des TI
- Professionnels des TI
- Agents de la protection des données personnelles
- Auditeurs TI désirant rehausser ses connaissances dans le domaine de la gestion des risques de sécurité de l'information

Prérequis: Des connaissances fondamentales dans la gestion des risques en entreprise

Contenu de la formation

- **Jour 1-** Introduction au programme de gestion des risques conforme à ISO/IEC 27005
- **Jour 2-** Mise en œuvre d'un processus de gestion des risques conforme à ISO/IEC 27005
- **Jour 3-** Aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'information et examen de certification

MEHARI Risk Manager

Durée: 3 jours

Objectifs

- Comprendre et découvrir la puissance de la méthode MEHARI
- Cartographier les risques avec la méthode MEHARI
- Maîtriser les éléments de gestion des risques de base pour la sécurité de l'information, en utilisant la méthode MEHARI
- Pratiquer la gestion des risques avec la méthode MEHARI
- Analyser et communiquer les résultats d'une étude MEHARI

Audience

- Personnes souhaitant apprendre les concepts fondamentaux du management des risques
- Personnes participant aux activités d'appréciation des risques sur les SI
- Responsables désirant comprendre les techniques d'appréciation des risques basées sur la méthode MEHARI
- Responsables souhaitant maîtriser les techniques d'analyse et de communication des résultats d'appréciation des risques selon la méthode MEHARI

Prérequis: Des connaissances fondamentales dans la gestion des risques en entreprise

Contenu de la formation

- **Jour 1-** Introduction aux concepts et aux étapes de la méthode d'analyse de risque MEHARI
- **Jour 2-** Conduire une analyse de risque en utilisant la méthode MEHARI
- **Jour 3-** Planification de la sécurité selon la méthode MEHARI et **examen de certification**

EBIOS Risk Manager

Durée: 3 jours

Objectifs

- Comprendre et découvrir la puissance de la méthode EBIOS
- Cartographier les risques avec la méthode EBIOS
- Maîtriser les éléments de gestion des risques de base pour la sécurité de l'information, en utilisant la méthode EBIOS
- Pratiquer la gestion des risques avec la méthode EBIOS
- Analyser et communiquer les résultats d'une étude EBIOS

Audience

- Personnes souhaitant apprendre les concepts fondamentaux du management des risques
- Personnes participant aux activités d'appréciation des risques sur les systèmes d'information
- Responsables désirant comprendre les techniques d'appréciation des risques basées sur la méthode EBIOS

Prérequis: Des connaissances fondamentales dans la gestion des risques en entreprise

Contenu de la formation

Jour 1

- Introduction à la méthode d'analyse de risque EBIOS
- Atelier 1 : « cadrage et socle de sécurité »
- Atelier 2 : « sources de risques »

Jour 2

- Atelier 3 : « Scénarios stratégiques »
- Atelier 4 : « Scénarios opérationnels »
- Atelier 5 : « Traitement des risques »

Jour 3

- Examen de certification

ISO 27032 Lead Cybersecurity Manager

Durée: 5 jours

Objectifs

- Acquérir des connaissances approfondies sur les composantes et les opérations d'un programme de cybersécurité en conformité avec l'ISO/IEC 27032 et le cadre de cybersécurité NIST
- Comprendre la corrélation entre ISO 27032, le cadre de cybersécurité NIST et les autres normes et cadres réglementaires
- Maîtriser les concepts, approches, normes, méthodes et techniques pour établir, mettre en œuvre et gérer efficacement un programme de cybersécurité au sein d'un organisme
- Apprendre à interpréter les exigences d'ISO/IEC 27032 dans le contexte spécifique d'un organisme
- Maîtriser l'expertise nécessaire pour planifier, mettre en œuvre, gérer, contrôler et maintenir un programme de cybersécurité tel que spécifié dans ISO/IEC 27032 et le cadre de cybersécurité NIST
- Acquérir les compétences pour conseiller un organisme sur les bonnes pratiques de management de la cybersécurité

Audience

- Professionnels de la cybersécurité
- Experts en sécurité de l'information
- Professionnels souhaitant gérer un programme de cybersécurité
- Responsables du développement d'un programme de cybersécurité
- Spécialistes des technologies de l'information
- Conseillers spécialisés dans les technologies de l'information
- Professionnels des technologies de l'information souhaitant accroître leurs connaissances et compétences techniques

Prérequis: Des connaissances fondamentales de la norme ISO/CEI 27002 et des connaissances approfondies sur la sécurité de l'information.

Contenu de la formation

- **Jour 1-** Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032
- **Jour 2-** Politiques de cybersécurité, management du risque et mécanismes d'attaque
- **Jour 3-** Mesures de contrôle de cybersécurité, partage et coordination de l'information
- **Jour 4-** Gestion des incidents, suivi et amélioration continue
- **Jour 5-** Examen de certification

Etat de l'art de la sécurité informatique

Durée: 3 jours

Objectifs

- Reconnaître les divers domaines de la sécurité et de la gestion des risques liés aux informations
- Intégrer les normes et les principes de chaque domaine de la sécurité des systèmes d'informations
- Avoir en sa possession des données actualisées sur les tendances de menaces ou de solutions en matière de SSI
- Optimiser les échanges d'informations entre la maîtrise d'ouvrage, la maîtrise d'œuvre et la SSI
- Rendre les choix techniques moins problématiques et plus faciles au sein de son organisation

Audience

- Directeurs des SI
- Responsables informatiques
- RSSI
- Chefs de projet sécurité
- Architectes informatiques

Prérequis: Aucun

Contenu de la formation

Jour 1

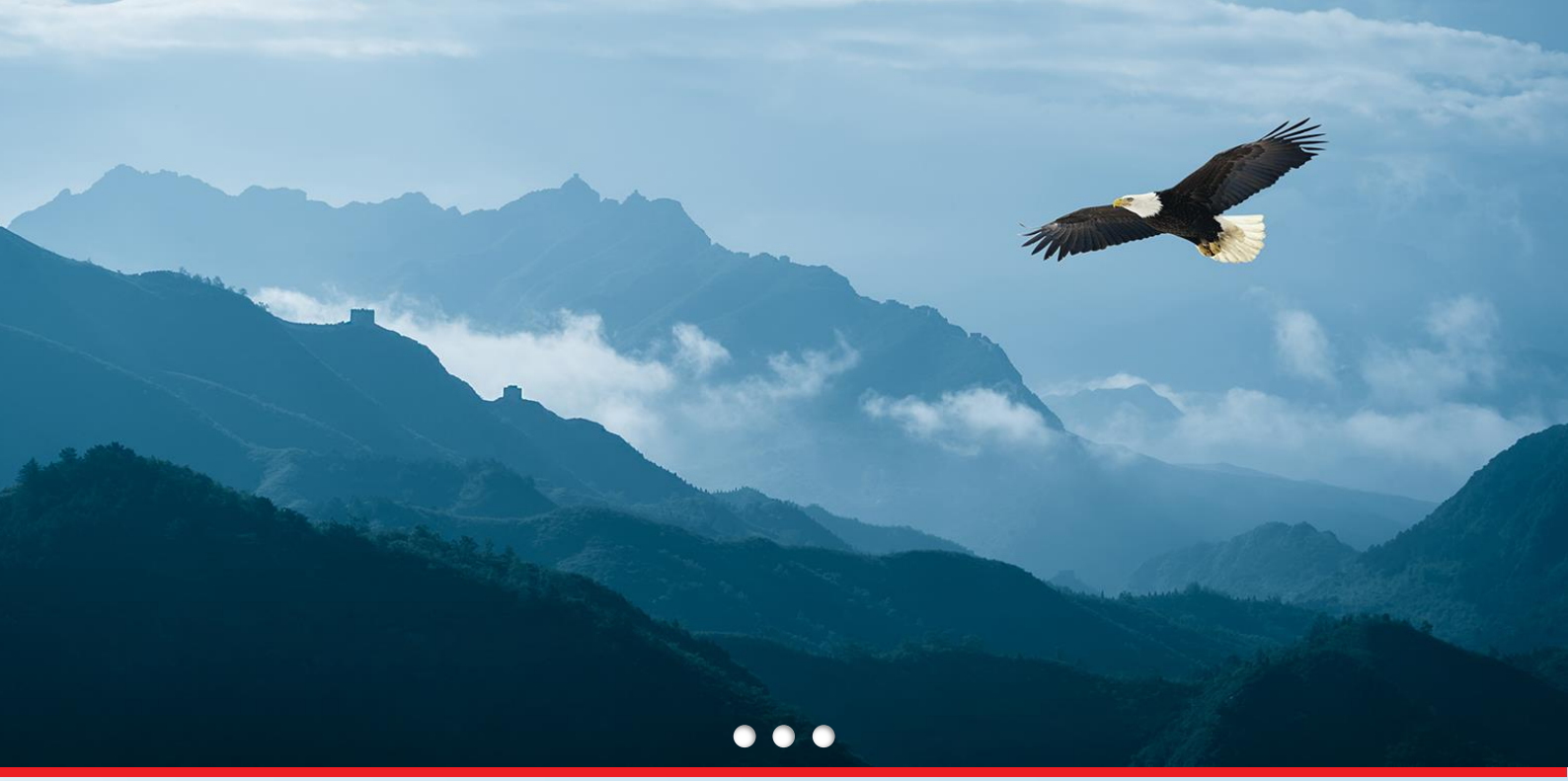
- Introduction, exigences légales et contexte juridique
- Organisation de la sécurité des SI
- Normes et Méthodologies de gestion la sécurité SI

Jour 2

- Panorama des attaques sur les SI
- Etat de l'art des outils de sécurité des SI
- Supervision de la sécurité des SI

Jour 3

- Notions sur le management de la sécurité de l'information
- Notions sur le management de la continuité d'activité
- Notions sur la gestion des données à caractère personnel



Continuité d'activité

ISO 22301 Foundation

Durée: 2 jours

Objectifs

- Reconnaître la corrélation entre la norme ISO 22301 et les autres normes et cadres réglementaires
- Comprendre les composantes et le fonctionnement d'un Système de Management de la Continuité d'Activité (SMCA) basé sur la norme ISO 22301 et ses principaux processus
- Comprendre les concepts, les approches, les méthodes et les techniques utilisés pour la mise en œuvre et la gestion d'un SMCA

Audience

- Les personnes impliquées dans la continuité d'activité
- Les personnes souhaitant acquérir des connaissances sur les principaux processus d'un SMCA
- Les personnes souhaitant poursuivre une carrière dans la continuité d'activité

Prérequis: Aucun

Contenu de la formation

- **Jour 1 -** Introduction au concept de Système de Management de la Continuité d'Activité (SMCA)
- **Jour 2-** Système de management de la continuité d'activité et examen de certification

ISO 22301 Lead Auditor

Durée: 5 jours

Objectifs

- Comprendre la relation entre le système de management de la continuité d'activité, le management des risques et les mesures.
- Comprendre les principes, procédures et techniques d'audit de la norme ISO 19011 :2018, et comment les appliquer dans le cadre d'un audit selon la norme ISO 22301.
- Acquérir les compétences nécessaires pour auditer un SMCA conformément aux exigences de la norme ISO 22301, et les techniques de gestion d'une équipe d'audit.
- Préparer et compléter un rapport d'audit ISO 22301

Audience

- Auditeur interne
- Equipe de contrôle interne
- Personne désirant diriger des audits de certification ISO 22301 en tant que responsable d'une équipe d'audit
- Consultant désirant préparer et accompagner une organisation lors d'un audit de certification ISO 22301

Prérequis: Une connaissance préalable de la norme ISO 22301 est recommandée

Contenu de la formation

- **Jour 1-** Introduction à la gestion d'un système de management de la sécurité de l'information selon ISO 22301
- **Jour 2-** Principes d'audit, préparation et déclenchement d'un audit ISO 22301
- **Jour 3-** Activités d'audit sur site
- **Jour 4-** Conclure de l'audit
- **Jour 5-** Examen de certification

ISO 22301 Lead Implementer

Durée: 5 jours

Objectifs

- Acquérir une compréhension globale des concepts, approches, méthodes et techniques utilisés pour la mise en œuvre et la gestion efficace d'un Système de Management de la Continuité d'Activité (SMCA)
- Apprendre à interpréter et à mettre en œuvre les exigences de la norme ISO 22301 dans le contexte spécifique d'un organisme
- Comprendre le fonctionnement d'un SMCA et ses processus basés sur la norme ISO 22301
- Acquérir les connaissances nécessaires pour aider une entreprise à planifier, mettre en œuvre, gérer, contrôler et améliorer en permanence un SMCA

Audience

- Les responsables de projets et les consultants impliqués dans la continuité d'activité
- Les conseillers experts cherchant à maîtriser la mise en œuvre d'un SMCA
- Les personnes chargées de maintenir la conformité aux exigences du SMCA au sein d'un organisme
- Les membres d'une équipe du SMCA

Prérequis: une bonne connaissance de la norme ISO 22301 et des connaissances approfondies des principes de sa mise en œuvre

Contenu de la formation

- **Jour 1-** Introduction à la norme ISO 22301 et déclanchement d'un SMCA
- **Jour 2-** Plan de mise en œuvre d'un SMCA (objectifs de continuité, analyse d'impact, politique, …)
- **Jour 3-** Mise en œuvre d'un SMCA (évaluation des risques, stratégies de continuité, plans de continuité, …)
- **Jour 4-** Suivi du SMCA, amélioration continue et préparation à l'audit de certification
- **Jour 5-** Examen de certification

Etablir le Plan de continuité d'activité de son entreprise

Durée: 3 jours

Objectifs

- Évaluer les risques et enjeux de la reprise après sinistre et de la continuité de service
- Élaborer les plans répondant aux besoins de l'entreprise
- Connaître les méthodes et outils pour choisir le type de site de reprise et réussir les projets
- Sélectionner les technologies, architectures et solutions les plus pertinentes
- Connaître les meilleures pratiques et bâtir un budget réaliste

Audience

- Les responsables de projets et les consultants impliqués dans la continuité d'activité
- Toute personne amenée à exercer la fonction de responsable du plan de continuité d'activité

Prérequis: Aucun

Contenu de la formation

- **Jour 1-** Introduction à la gestion de crise, à la continuité d'activité et aux normes de continuité
- **Jour 2-** Définition des besoins de continuité et des risques liés aux processus
- **Jour 3-** Dispositif de gestion de crise et plans de continuité d'activité

Protection des données personnelles

RGPD Foundation

Durée: 2 jours

Objectifs

- Comprendre les exigences du Règlement Général sur la Protection des Données (RGPD) et les concepts fondamentaux de protection de la vie privée
- Comprendre les obligations, les rôles et les responsabilités du Délégué à la Protection des Données (DPO : Data Protection Officer)
- Comprendre les concepts, les approches, les méthodes et les techniques pour aligner efficacement un cadre de conformité en ce qui concerne la protection des données personnelles.

Audience

- Personnes impliquées dans la protection des données personnelles et la sécurité de l'information
- Personnes cherchant à acquérir des connaissances sur les principes essentiels de protection de la vie privée
- personnes intéressées à poursuivre une carrière dans le domaine de la protection des données

Prérequis: Aucun

Contenu de la formation

- **Jour 1-** Introduction aux principes de protection des données et du RGPD
- **Jour 2-** Les exigences du RGPD et l'examen de certification

Data Protection Officer

Durée: 5 jours

Objectifs

- Acquérir une compréhension approfondie des concepts fondamentaux et des éléments du Règlement sur la protection des données
- Comprendre l'objectif, le contenu et la corrélation entre le Règlement général sur la protection des données et les autres cadres réglementaires
- Acquérir une compréhension approfondie des concepts, des approches, des méthodes et des techniques permettant une protection efficace des données à caractère personnel
- Savoir interpréter les exigences relatives à la protection des données dans le contexte particulier d'un organisme
- Acquérir l'expertise nécessaire pour aider un organisme à planifier, mettre en œuvre, gérer, surveiller et maintenir un cadre de conformité en ce qui concerne le RGPD

Audience

- Responsables de projets et consultants qui désirent préparer et aider un organisme à mettre en œuvre les nouvelles procédures et à adopter les nouvelles exigences présentées dans le RGPD
- Délégués à la protection des données et membres de la direction générale responsables de la protection des données à caractère personnel d'une entreprise et de la gestion de ses risques
- Membres d'équipes de sécurité de l'information, de gestion des incidents et de continuité des activités
- Conseillers spécialisés en sécurité des données à caractère personnel
- Spécialistes des questions techniques et de conformité qui désirent se préparer à occuper un poste de délégué à la protection des données

Prérequis: Aucun

Contenu de la formation

- **Jour 1-** Introduction au RGPD et mise en œuvre de la conformité au RGPD
- **Jour 2-** Planification de la mise œuvre du RGPD
- **Jour 3-** Déploiement des exigences du RGPD
- **Jour 4-** Surveillance et amélioration continue de la conformité au RGPD
- **Jour 5-** Examen de certification

Formations en sécurité liées aux technologies

Sécurité Windows

Durée: 3 jours

Objectifs

- Comprendre les processus de sécurité mis en place par l'OS
- Déployer une infrastructure en suivant les bonnes pratiques
- Connaître les dangers de configuration Windows
- Mettre en place des GPO efficaces
- Définir une politique de sécurité

Audience

- Auditeurs techniques
- Administrateurs système

Prérequis:

- Notions de sécurité informatique
- Connaissance des protocoles réseaux TCP/IP
- Maîtrise des systèmes Windows (client et serveur) et Active Directory

Contenu de la formation

- **Jour 1-** Présentation de Windows
- **Jour 2-** Durcissement d'un environnement Windows
- **Jour 3-** Protection des services Windows

Sécurité Réseaux

Durée: 3 jours

Objectifs

- Connaître les failles et les menaces des systèmes d'information
- Maîtriser le rôle des divers équipements de sécurité
- Concevoir et réaliser une architecture de sécurité adaptée
- Mettre en œuvre les principaux moyens de sécurisation des réseaux

Audience

- Auditeurs techniques
- Administrateurs réseaux

Prérequis:

- Notions de sécurité informatique
- Connaissance des protocoles réseaux TCP/IP
- Maîtrise des équipements réseaux (fonctionnalités, administration, …)

Contenu de la formation

- **Jour 1-** Risques et menaces sur les réseaux informatiques
- **Jour 2-** Architectures de sécurité
- **Jour 3-** Sécurité des échanges

Lead Cloud Security Manager

Durée: 5 jours

Objectifs

- Acquérir une compréhension complète des concepts, approches, méthodes et techniques utilisés pour la mise en œuvre et la gestion efficace d'un programme de sécurité du cloud.
- Comprendre la corrélation entre ISO/IEC 27017, ISO/IEC 27018 et d'autres normes et cadres réglementaires
- Apprendre à interpréter les lignes directrices des normes ISO/IEC 27017 et ISO/IEC 27018 dans le contexte spécifique d'un organisme
- Développer les connaissances et les compétences nécessaires pour aider un organisme à planifier, mettre en œuvre, gérer, surveiller et maintenir efficacement un programme de sécurité du cloud
- Acquérir les connaissances pratiques pour conseiller un organisme dans la gestion d'un programme de sécurité du cloud en suivant les bonnes pratiques

Audience

- Professionnels de la sécurité du cloud et de la sécurité de l'information cherchant à gérer un programme de sécurité du cloud
- Managers ou consultants cherchant à maîtriser les bonnes pratiques de sécurité du cloud
- Personnes chargées de maintenir et de gérer un programme de sécurité du cloud
- Experts techniques cherchant à améliorer leurs connaissances en matière de sécurité du cloud
- Conseillers experts en sécurité du cloud

Prérequis:

- Connaissance générale des concepts du Cloud computing
- Compréhension fondamentale des normes de sécurité du type ISO 27002

Contenu de la formation

- **Jour 1-** Introduction aux normes ISO/IEC 27017 et ISO/IEC 27018 et à l'initiation d'un programme de sécurité du cloud
- **Jour 2-** Gestion des risques de sécurité du cloud et mesures spécifiques au cloud
- **Jour 3-** Gestion de l'information documentée et sensibilisation et formation à la sécurité du cloud
- **Jour 4-** Gestion des incidents de sécurité du cloud, tests, surveillance et amélioration continue
- **Jour 5-** Examen de certification

Certified Lead Ethical Hacker

Durée: 5 jours

Objectifs

- Maîtriser les concepts, méthodes et techniques utilisés par les organisations de cybersécurité et les hackers éthiques pour réaliser des tests d'intrusion
- Reconnaître la corrélation entre les méthodologies de tests d'intrusion, les cadres réglementaires et les normes
- Acquérir une connaissance approfondie des composantes et des opérations du piratage éthique

Audience

- Personnes souhaitant acquérir des connaissances sur les principales techniques utilisées pour réaliser des tests d'intrusion
- Professionnels de la sécurité de l'information cherchant à maîtriser les techniques de piratage éthique et de tests d'intrusion
- Responsables de la sécurité des systèmes d'information
- Membres d'une équipe de sécurité de l'information
- Experts techniques souhaitant apprendre comment planifier et réaliser un test d'intrusion

Prérequis:

- connaissance des concepts et principes de sécurité de l'information
- compétences avancées en matière de systèmes d'exploitation
- connaissance des réseaux informatiques et des concepts de programmation

Contenu de la formation

- **Jour 1-** Introduction au piratage éthique
- **Jour 2-** Lancement de la phase de reconnaissance
- **Jour 3-** Lancement de la phase d'exploitation
- **Jour 4-** Post-exploitation et rapports
- **Jour 5-** Examen de certification

Lead Pen Test Professionnel

Durée: 5 jours

Objectifs

- Savoir interpréter et illustrer les principaux concepts et principes relatifs au test d'intrusion
- Comprendre les connaissances techniques de base nécessaires pour organiser et mener à bien un ensemble efficace de tests d'intrusion
- Apprendre comment planifier efficacement un test d'intrusion et identifier un domaine d'application approprié et adapté en fonction du risque
- Acquérir les connaissances et les compétences pratiques sur les outils et les techniques utilisés pour effectuer efficacement un test d'intrusion
- Gérer efficacement le temps et les ressources nécessaires à l'échelle d'un test d'intrusion spécifique

Audience

- Professionnels informatiques souhaitant améliorer leurs connaissances et leurs compétences techniques
- Auditeurs souhaitant comprendre les processus du test d'intrusion
- Responsables des technologies de l'information et de gestion de risques souhaitant acquérir une compréhension plus détaillée de l'utilisation appropriée et bénéfique des tests d'intrusion
- Consultant Pen Testeurs
- Professionnels de la cybersécurité

Prérequis: Des connaissances de bases sur la sécurité de l'information.

Contenu de la formation

- **Jour 1-** Introduction aux tests d'intrusions, à l'éthique, à la planification et au domaine d'application
- **Jour 2-** Connaissances techniques fondamentales et techniques (avec des exercices pratiques dans tous les domaines)
- **Jour 3-** Réalisation d'un test d'intrusion (à l'aide d'outils et de techniques) et revue du domaine du test
- **Jour 4-** Analyse des résultats des tests, rapports et suivi
- **Jour 5-** Examen

Cursus

Métier RSSI

Durée: 13 jours

Objectifs

- Acquérir les compétences nécessaires à la prise de fonction du rôle de RSSI d'une organisation

Audience

- RSSI nouvellement nommés
- Aspirants au métier RSSI

Prérequis: Prérequis des domaines du cursus Métier RSSI

Contenu de la formation

- **Domaine 1 –** Etat de l'art de la sécurité
- **Domaine 2 –** ISO 27001 Lead Implementer
- **Domaine 3 –** Lead Pen Test Professionnel

Métier Auditeur sécurité des SI

Durée: 13 jours

Objectifs

- Acquérir les compétences nécessaires à la prise de fonction du rôle de RSSI d'une organisation

Audience

- Auditeurs SI désirant renforcer leurs capacités d'audit en sécurité de l'information
- Aspirants au métier d'auditeurs en sécurité de l'information

Prérequis: Prérequis des domaines du cursus Métier RSSI

Contenu de la formation

- **Domaine 1 –** Etat de l'art de la sécurité
- **Domaine 2 –** ISO 27001 Lead Implementer
- **Domaine 3 –** Lead Pen Test Professionnel

Métier Consultant sécurité des SI

Durée: 13 jours

Objectifs

- Acquérir les compétences nécessaires pour exercer le métier de consultant en cybersécurité

Audience

- Profils désirant se reconvertir dans le domaine de la sécurité de l'information
- Consultants désirant renforcer leurs compétences en termes de consulting en cybersécurité

Prérequis: Aucun

Contenu de la formation

- **Domaine 1 –** Métier du consultant (formation sur mesure)
- **Domaine 2 –** ISO 27001 Lead Implementer
- **Domaine 3 –** ISO 27001 Lead Auditor

CONTACTEZ-NOUS

contact@confisec.net

Togo : +228 22 25 33 29

Maroc : +212 658 83 96 46 / +212 701 22 49 20

Togo : Bd du 30 Août Route de Kpalimé, Angle Rue Nord du Lycée Adidogomé II, Lomé

Maroc : 26 Avenue Mers Sultan, Apt 3 étage 1 Casablanca

www.confisec.net

@xconfisec

Confisec

@xconfisec

Confisec

Catalogue des formations 2022