Sécurité des actifs et des personnes en Data Center

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Domaine : Cybersécurité - sécurité informatique

Filière : Fondamentaux de la cybersécurité

Rubrique : Fondamentaux

Éligible au CPF : Non

Action collective : Non

PRÉSENTATION

Objectifs & compétences

- Inventorier les types de menace à circonscrire
- Lister les principales sources réglementaires et normatives de référence
- Prendre connaissance des moyens de prévention des intrusions et malveillances
- Prendre connaissance des moyens de prévention et de traitement des incendies
- Prendre en compte la gestion du risque environnemental
- Connaître les mesures de réduction du risque d'accident électrique
- Savoir tenir compte des capacités de charge des éléments constitutifs de la salle
- Identifier les mesures de réduction du risque de blessure en exploitation courante

Public visé

Responsable informatique, Chef de projet IT, Gestionnaire des installations Bâtiment, Responsable des infrastructures IT, Responsable des Moyens généraux, Chef de projet Bâtiment, Responsable Maintenance Bâtiment

Pré-requis

- Notions fondamentales relatives aux missions et fonctions d'une salle informatique
- Connaissances théoriques au sujet du matériel informatique et des activités de production informatique

PROGRAMME

1. **Introduction : Sécurité du Datacenter et Gestion des risques**

- Enjeux et défis spécifiques de sécurité des actifs et des personnes en salle informatique
- Sûreté de fonctionnement IT vs. Sécurité du Bâtiment : complémentarité des approches
- Apports de MoR (Management of Risks) pour la Sécurité des Datacenters
- Principes d'appréciation et de traitement du risque sécuritaire selon EN 50600
- Classes de protection EN 50600
- Amélioration continue d'une stratégie de gestion des risques sécuritaires

2. Préambule : Implantation géographique du Datacenter

- Impératifs opérationnels de l'emplacement
- Panorama des risques exogènes
- Recommandations et paramètres décisionnels

3. Prévention des intrusions et des actes de malveillance

- Risques liés à la présence de personnels non sollicités
- Application des classes de protection EN50600 à la stratégie d'autorisation d'accès
- Modèles théoriques de protection physique
- Surveillance et protection générale du bâtiment
- Gestion des véhicules et des livraisons
- Empêcher, Détecter, Retarder et Neutraliser les intrusions

Code de formation : CYB509

€ Tarifs

Prix public : 1890 €

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
Le dispositif FNE-Formation.
L'OPCO (opérateurs de compétences) de votre entreprise.
France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
CPF -MonCompteFormation
Contactez nous pour plus d'information : contact@aston-institut.com

Lieux & Horaires

Durée : 48 heures

Délai d'accès : Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

Prochaines sessions

Consultez-nous pour les prochaines sessions.

- Gestion technique des accès (GTA)
- Vidéosurveillance (VSS) en salle informatique
- Normes et réglementation applicables aux techniques de contrôle et de surveillance
- Bonnes pratiques d'exploitation courante pour limiter les intrusions, malveillances et négligences

4. Lutte contre le risque incendie

- Equipements portatifs de lutte contre les incendies
- Impacts de la stratégie d'extinction des incendies sur les structures du bâtiment
- Rappels théoriques : le tétraèdre du feu
- Catégorisation des risques et dégâts occasionnés par les incendies
- Normes et réglementation applicables à la gestion du risque incendie
- Application des classes de protection EN50600 à la stratégie de protection incendie
- Plan de sécurité Incendie
- Mesures de prévention du risque incendie : bonnes pratiques de conception et d'exploitation
- Mesures de compartimentage : limiter l'impact des incendies potentiels
- Stratégie et dispositifs de détection des incendies : identifier et alerter au plus tôt
- Stratégie et dispositifs fixes d'extinction des incendies : préserver les actifs disposés en salle et la santé des exploitants

5. Prévention et réduction d'impact du risque d'accident électrique

- Rappels sur la distribution énergétique en salle informatique : topologie et mesures de protection
- Mise à la masse et mise à la terre : principes, objectifs et complémentarité
- Mise à la masse et mise à la terre : techniques de mise en œuvre
- Formation des collaborateurs confrontés à la manipulation du Courant Fort
- Dispositifs d'arrêt d'urgence de l'alimentation électrique
- Normes et réglementation applicables à la protection des personnes contre le risque électrique

6. Lutte contre les risques environnementaux

- Qualification des risques environnementaux
- Application des classes de protection EN50600 à la stratégie de protection contre le risque environnemental
- Gestion du risque électromagnétique
- Notions de gestion du risque de pollution particulaire et moléculaire (afin d'approfondir ce sujet, nous proposons le cours dédié « MQA – Maîtrise de la Qualité de l'Air en salle informatique »)
- Gestion des risques géologiques

7. Signalisation et éclairage de sécurité en salle

- Signalisation d'urgence en salle informatique : bonnes pratiques d'implémentation
- Eclairage normal, de remplacement et de sécurité
- Mise en œuvre de l'éclairage dans les différentes zones du Datacenter
- Normes et réglementation applicables à la signalisation

8. Gestion capacitaire des structures

- Gestion de la charge au sol : spécifications de plancher et de faux-plancher
- Bonnes pratiques de conception et méthodes de renforcement
- Répartition des masses dans les baies, bonnes pratiques d'exploitation
- Gestion de la capacité d'accrochage au plafond
- Adaptation de la salle informatique et du Datacenter au risque sismique
- Normes et réglementation applicables à la conception

9. Conclusions et synthèse

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.
Pédagogie : essentiellement participative et ludique, centrée sur l'expérience,

l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.
Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.
Pendant la formation : mises en situation, autodiagnostics, travail individuel ou en sous-groupe sur des cas réels.

Méthode

Fin de formation : entretien individuel.
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.
Assiduité : certificat de réalisation.
Validations des acquis : grille d'evalution des acquis établie par le formateur en fin de formation.