# SECURITE DES ACTIFS ET DES PERSONNES EN SALLE INFORMATIQUE (SEC)

Fiche descriptive de la formation

**Durée** : 2 jours (14 heures). **Contact** : contact@cellaconsilium.fr

**Objectifs** : Cette formation expose les catégories de moyens préventifs et curatifs de traitement des menaces et risques induits par l'existence de la salle informatique et du Datacenter, tant pour préserver la santé des collaborateurs que pour garantir la continuité du service technique.

- 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.

**Prérequis** :

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

**Modalités d'accès :** Aucune certification, aucun diplôme préalable n'est exigé pour bénéficier de cette formation. Afin de nous assurer conjointement qu'elle répondra pleinement à vos attentes, un conseiller pédagogique Cella Consilium prendra au préalable contact avec vous par téléphone ou par e-mail ; un questionnaire d'évaluation de vos besoins vous sera également proposé.

**Public concerné** : Toute personne impliquée directement ou indirectement dans un projet de conception, construction ou réhabilitation de salle informatique et/ou de Datacenter ; tout personnel en charge de la planification ou de l'optimisation de la gestion-exploitation d'une salle informatique in-house ou hébergée ; tout collaborateur responsable ou mainteneur des dispositifs de protection des matériels et de l'intégrité physique des exploitants et/ou des intervenants extérieurs en zone technique.

Ex : 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.

**Nombre de participants** : 8 participants maximum, afin de favoriser la compréhension et la participation de chacun.

**Méthodes pédagogiques** :

- Formation présentielle ;
- Support de cours fourni au format numérique à chaque participant ;
- Prêt d'une tablette pour suivre la formation en addition de la projection par le formateur ;
- Rappel des répartitions des responsabilités entre les départements Bâtiment et IT ;
- Présentation des procédés adaptés aux différents types de menace ;
- La formation propose des retours d'expérience issus de la pratique Métier du formateur ;
- Prise en compte des différentes normes en vigueur, émanant des organisations internationales de référence (ISO/IEC, TIA, CENELEC…) ;
- 6 à 8 participants maximum pour favoriser la participation et la compréhension de chacun ;
- Mise à jour gratuite du support de cours durant les 6 mois suivant la formation.

**Évaluation des acquis pédagogiques :**

- Formation ponctuée de questionnaires interactifs, participatifs et ludiques ;
- Exercices de sélection/positionnement des dispositifs de sécurité ;
- QCM soumis au participant à la fin du dernier jour de la formation (seuil de réussite : 70 % de bonnes réponses). Ce QCM permet par ailleurs la validation du module dans le cadre du cursus certifiant « **Conception-urbanisation de salles informatiques – Data Center** ».

**Accessibilité aux personnes handicapées :**

Pour nos formations inter-entreprises, nous sélectionnons des lieux et des salles de formation accessibles aux personnes à mobilité réduite et disposant de locaux sanitaires adaptés. Si vous êtes travailleur ou demandeur d'emploi en situation de handicap, n'hésitez pas à nous le mentionner afin que nous nous assurions spécifiquement que tout sera mis en œuvre pour votre autonomie, votre confort et votre sécurité.

**Délais d'accès et tarification** : veuillez s'il-vous-plaît vous référer à notre site Internet www.cellaconsilium.fr

# CONTENU DE LA FORMATION

## *Première journée*

### *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

### *Préambule : Implantation géographique du Datacenter*

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

### *Chapitre 1 – 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
- 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

### *Chapitre 2 – Lutte contre le risque incendie*

- 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
- Equipements portatifs de lutte contre les incendies
- Impacts de la stratégie d'extinction des incendies sur les structures du bâtiment

## *Chapitre 3 – 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

## *Chapitre 4 – 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

## *Chapitre 5 – Signalisation et Eclairage 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

## *Chapitre 6 – 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

## *Conclusions et synthèse*