

MANAGER DES RISQUES SÛRETÉ ET MALVEILLANCE



Objectifs et contexte de la certification

Le manager des risques sûreté et malveillance est responsable de la définition, de la mise en place et du suivi d'une politique de prévention et de protection vis-à-vis des actes de malveillance. Il propose, met en œuvre et communique autour des moyens humains, techniques et organisationnels permettant d'éviter ou de limiter les actes de malveillance envers les personnes et les biens.

Le manager des risques sûreté et malveillance, au-delà des actions opérationnelles de prévention des risques, évalue la vulnérabilité de l'entreprise vis-à-vis des menaces de malveillance. Pour cela, il doit avoir une vision globale de l'entreprise (stratégie, fonctionnement, santé financière, modèle économique, ressources humaines...).

Il identifie alors les points névralgiques pouvant être affectés par des scénarios liés aux actes de malveillance envers les personnes (agressions verbales ou physiques, kidnappings, meurtres) et les biens matériels et immatériels (dégradations, vols, destruction). Il propose, sur la base de ce diagnostic de vulnérabilité, un plan d'action complet chiffré, financé et planifié dans le temps.

Il doit enfin défendre et convaincre la Direction de l'entreprise de la pertinence de son analyse et de l'efficacité de ses propositions. Il associe également à ce plan d'action un dispositif de gestion et de communication de crise et conçoit un plan de continuité d'activités.

Activités visées

- Concevoir et gérer la sûreté d'un site privé ou public au regard des problématiques identifiées
- Évaluer et mettre en application les dispositifs techniques et organisationnels de la sûreté
- Réaliser l'analyse systémique d'un établissement
- Réaliser une analyse de risques et de vulnérabilités en matière de sûreté et de prévention d'actes de malveillance
- Déployer et exécuter un système de management de sûreté et de prévention d'actes malveillance
- Gérer les situations de crise et préparer un plan de continuité d'activité intégrant la sûreté

Compétences attestées

- Identifier les environnements, les flux (flux humain, produits, finances, utilités, ...) de l'entreprise ainsi que les menaces susceptibles de l'impacter.
- Analyser le comportement malveillant pour anticiper le passage à l'acte et/ou en réduire les conséquences.
- Prendre en compte des actions violentes et du risque terroriste dans l'entreprise.
- Évaluer et intégrer des exigences légales et des contraintes réglementaires liées aux activités de l'entreprise.
- Évaluer et mettre en application les dispositifs de prévention et des moyens de protections techniques et organisationnels de la sûreté.
- Évaluer les risques en matière de protection des données dans l'entreprise (menace cyber) et construire un cahier des charges fonctionnel pour un achat pertinent au regard de la problématique sûreté.
- Auditer l'organisation et les moyens techniques « sûreté » de l'entreprise, qui lui permettra de construire un plan d'action pertinent en matière de lutte contre la malveillance interne et externe.
- Identifier et établir une cotation des scénarios de risques malveillance pour identifier les points majeurs de vulnérabilité malveillance de l'entreprise.
- Proposer, sur la base de cette analyse de risques et de vulnérabilités, un plan d'action complet chiffré, financé et planifié dans le temps.
- Défendre et de convaincre la Direction de l'entreprise du bien-fondé de son analyse et de ses propositions.
- Concevoir et déployer un système de management de la sûreté malveillance.
- Définir une organisation de gestion de crise performante et adaptée en matière de risques liés à la sûreté ainsi que les principales lignes directrices d'un plan de continuité d'activité avec un éclairage économique, financier et assurantiel.

Secteurs d'activités

Sociétés de sécurité privée (surveillance humaine, surveillance électronique, sûreté aéroportuaire et portuaire, des services internes des entreprises et des donneurs d'ordre privés et publics (collectivités territoriales, bailleurs sociaux, transporteurs, hôpitaux).

Type d'emplois accessibles

Security manager - Manager sécurité - Responsable sécurité de site - Responsable service sécurité - Responsable de sécurité et surveillance - Responsable d'exploitation en sécurité - Directeurs sûreté - Gérants d'entreprise de sûreté - Directeurs techniques - Chefs de service sûreté - Officiers inspecteurs - Chefs de projet sûreté - Experts sûreté.

Références juridiques des réglementations d'activité

L'employeur est tenu à l'égard de ses salariés d'une obligation de sécurité de résultat (article L.4121-1 du code du travail). Il sera tenu responsable pénalement en cas de malveillance infligée (harcèlement, agression, attentat, kidnapping) sauf à être en mesure de justifier que toutes les mesures de prévention avaient été prises et qu'il s'agit d'une faute personnelle de la victime.

Pour répondre à cette obligation légale, l'employeur devra s'appuyer sur des personnes compétentes (article L.4644-1 du code du travail). A ce titre, il devra désigner « un ou plusieurs salariés compétents pour s'occuper des activités de protection et de prévention des risques professionnels de l'entreprise », quel que soit l'effectif de l'entreprise. Le niveau de qualification ou de formation requis, les missions de ces « salariés compétents » ne sont pas précisées réglementairement.

L'article L.271-1 du code de la sécurité intérieure (CSI) prévoit une obligation de surveillance selon laquelle « les propriétaires, exploitants ou affectataires, selon le cas, d'immeubles à usage d'habitation et de locaux administratifs, professionnels ou commerciaux doivent, lorsque l'importance de ces immeubles ou de ces locaux ou leur situation le justifient, assurer le gardiennage ou la surveillance de ceux-ci et prendre les mesures permettant d'éviter les risques manifestes pour la sécurité et la tranquillité des locaux ».

L'instruction Générale Interministérielle sur la protection du secret de la défense nationale n°1300 du 22 novembre 2013, les procédés, objets, documents, données ou fichiers informatisés intéressant la défense nationale peuvent faire l'objet d'une classification en trois degrés de protection.

Voies d'accès

Le cas échéant, prérequis à la validation des compétences :

Être titulaire d'un titre ou diplôme de niveau 6 ou justifier d'une expérience professionnelle dans le domaine de la sûreté de plus de 5 ans.

