

# Manager des risques sûreté et malveillance

RNCP35599 · RNCP · Publiée

## L'essentiel

|                         |                            |
|-------------------------|----------------------------|
| Niveau de qualification | Niveau 7                   |
| Code(s) NSF             | 344                        |
| Formacode(s)            | 42881                      |
| Code(s) ROME            | K2503, K2502               |
| Type d'enregistrement   | Enregistrement sur demande |
| Date d'enregistrement   | 19/05/2021                 |
| Date d'échéance         | 19/05/2023                 |

## Certificateur(s)

CNPP ENTREPRISE · SIRET : 34290125300050

## Résumé de la certification

### OBJECTIFS ET CONTEXTE

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 de 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 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.

## Blocs de compétences

### RNCP35599BC01 — Concevoir et gérer la sûreté d'un site privé ou public

#### LISTE DE COMPÉTENCES

Réaliser une analyse détaillée des environnements (naturels, dessertes, socio-économique et réglementaires) afin d'évaluer les risques associés.

Effectuer une étude des flux (flux humain, produits, finances, utilités ...) afin de cartographier l'organisation et la vie interne de l'entreprise.

Intégrer le contexte géopolitique, économique, le positionnement sur le marché de l'entreprise afin d'évaluer les menaces susceptibles d'impacter l'entreprise.

Réaliser une analyse de la typologie de l'agresseur afin d'adapter le dispositif sûreté.

Analyser les retours d'expériences des dernières années afin de considérer l'évolution de la menace et se prémunir d'actions violentes et du risque terroriste dans l'entreprise.

Intégrer le cadre législatif et réglementaire de la lutte contre la malveillance afin de l'adapter à son propre site.

#### MODALITÉS D'ÉVALUATION

Étude de cas et de questionnaire - Présentation orale de l'analyse et des solutions

### RNCP35599BC02 — Mettre en oeuvre les dispositifs techniques et organisationnels de la sûreté

#### LISTE DE COMPÉTENCES

Evaluer les solutions techniques et organisationnelles en intégrant les avantages et les inconvénients de chacune d'elles afin de répondre à la problématique sûreté.

Identifier les menaces qui pèsent sur l'entreprise en termes de protection des données et des risques cyber afin de déployer un dispositif de protection de son site.

Accompagner l'entreprise dans la protection de ces risques en communiquant sur les "bonnes pratiques" et en développant une culture "sûreté".

Identifier le besoin de l'entreprise, les contraintes techniques avérées, les modalités de réalisation, de mise en place et de formation en vue d'établir un cahier des charges exhaustif et fonctionnel selon la norme NF EN 16271.

Réaliser un audit sûreté en respectant la méthodologie suivante :

- o identifier les menaces,
- o appréhender de manière globale le fonctionnement de l'entreprise,
- o appréhender les différents environnements, les flux de l'entreprise,
- o identifier la typologie des auteurs, en déduire des scénarios plausibles...
- o intégrer l'organisation sûreté existante.

Construire un plan d'action en apportant des solutions organisationnelles, techniques et humaines cohérentes et homogènes sur l'ensemble de la chaîne sûreté afin d'en garantir l'effort d'investissement.

#### MODALITÉS D'ÉVALUATION

Étude de cas et de questionnaire – Mise en situation pratique reconstituée - Présentation orale de l'analyse et des solutions

## **RNCP35599BC03 — Réaliser l'analyse systémique sûreté d'un établissement**

### **LISTE DE COMPÉTENCES**

Réaliser un diagnostic financier de l'entreprise (santé financière capacité d'emprunt, capacité d'autofinancement, niveau d'indépendance) afin d'identifier les possibilités de financement du plan de traitement.

Analyser le fonctionnement, l'histoire, la culture, les fonction clés, le marché, les clients, l'environnement, le niveau de conformité réglementaire, l'évolution et les projets (sur la base de la matrice SWOT) de l'entreprise pour établir une vision exhaustive de la stratégie de l'entreprise.

Identifier les flux de l'entreprise (flux humains (flux humains, produits, biens et marchandises, utilités, énergies, chiffre d'affaire.) afin d'établir une cartographie détaillée de l'organisation et de la vie de l'entreprise.

### **MODALITÉS D'ÉVALUATION**

Étude de cas et de questionnement – Production d'un rapport de recherche et d'études - Présentation orale de l'analyse et des solutions

## **RNCP35599BC04 — Mener une analyse de risques et vulnérabilités en matière de prévention d'actes de malveillance**

### **LISTE DE COMPÉTENCES**

Identifier les points névralgiques de l'entreprise susceptibles de mettre en péril ses structures et sa survie (image de marque, e-réputation, outils de production, certifications, brevets, recherche et développement, personnels ...) afin d'initier une analyse de risques et de vulnérabilités concrète, exhaustive.

Identifier les scénarios de risques malveillance et les événements dangereux (selon une vraisemblance et une gravité) tels que les logiques d'agressions violentes – attentats-surattentats, les mouvements sociaux, la gestion des formations et des compétences en matière sûreté afin de compléter l'analyse de risques et de vulnérabilités.

Établir une cotation des scénarios de menaces en tenant compte des moyens de maîtrise, en matière de prévention et de protection, et des retours d'expérience du site pour identifier les points majeurs de vulnérabilité malveillance de l'entreprise.

### **MODALITÉS D'ÉVALUATION**

Mise en situation reconstituée – Production d'un rapport d'étude - Présentation orale de l'analyse et des solutions

## **RNCP35599BC05 — Déployer et exécuter un système de management de sûreté et de prévention**

### **LISTE DE COMPÉTENCES**

Identifier les actions de réduction adaptées aux données de sortie de l'analyse de risques et de vulnérabilités, en intégrant des dispositifs techniques, organisationnels et humains, des mesures managériales (dispositifs de gestion des compétences, maintien et évolution dans l'emploi...) afin de construire un plan de traitement des risques malveillants pertinent, cohérent et homogène.

Chiffrer les actions du plan de traitement en intégrant les dépenses d'investissement et de fonctionnement (maintenance préventive, curative et prédictive) et en le planifiant de manière soutenable vis-à-vis de la situation financière de l'entreprise

Justifier les niveaux de risques résiduels en tenant compte des enjeux de stratégie et de tactique de l'entreprise

Élaborer une communication auprès de la direction visant à démontrer la pertinence, l'efficacité et l'efficience des actions de sûreté à traiter.

Définir une culture de la sûreté et des actions de communication en ce domaine pour mener un déploiement efficace du plan de traitement.

Coordonner et accompagner les acteurs du plan de traitement (pilotes et actionnaires) afin de garantir une mise en application efficace et efficiente.

Évaluer et hiérarchiser les opportunités d'intégrer les actions de réduction des risques malveillance afin d'initier une démarche de type processus.

Définir et structurer un programme d'exécution et de déploiement du système de management de la sûreté adapté aux activités et aux besoins opérationnels de l'entreprise (principes directeurs, processus, procédures de prévention de risques sûreté malveillance...)

Contrôler, vérifier, tester et formaliser la bonne installation des systèmes de prévention et de protection.

Évaluer et analyser les résultats des phases de déploiements afin de mesurer l'efficacité des dispositifs de management de la sûreté.

C29 : Concevoir des supports pédagogiques présentant les principes directeurs et les objectifs de la démarche, les processus et les procédures de prévention de risques sûreté malveillance en fonction des publics visés.

C30 : Former le personnel et accompagner les organisations afin de déployer efficacement le système de management.

#### MODALITÉS D'ÉVALUATION

Étude de cas et de questionnaire – Mise en situation pratique reconstituée - Présentation orale de l'analyse et des solutions

### **RNCP35599BC06 — Gérer les situations de crise et préparer un plan de continuité d'activité intégrant la sûreté**

#### LISTE DE COMPÉTENCES

Identifier les scénarios de risques sûreté et les dispositifs de secours et de sûreté correspondants (évacuation/échappement, confinement, sectorisation sanctuarisation).

Constituer une cellule de crise sûreté et entraîner les différents membres acteurs de cette cellule afin d'agir efficacement en cas de survenance d'une crise.

Préparer la communication interne et externe en cas de survenance de la crise pour démontrer la maîtrise des événements (attentats, surattentat, mouvements sociaux, risques atteints à l'image de marque, e-réputation ...).

Analyser les retours d'expériences afin d'améliorer le dispositif de crise de manière continue et de maintenir un niveau de sécurité et de sûreté acceptable (mesures compensatoires et conservatoires) en liaison avec le système d'assurance qualité de la sûreté.

Rédiger des rapports de déploiements de systèmes de management de crise sûreté pour instaurer un processus de reporting visant à l'amélioration continue

En fonction des scénarios de crise sûreté identifiés, définir les ressources et les organisations opérationnelles (cotraitance, sous-traitance, location de matériels, relocalisation temporaire, ...) afin d'être capable de réussir une continuité d'activité la plus efficace et rapide possible.

Optimiser le transfert à l'assurance du financement des risques résiduels, directs, indirects, en intégrant les situations de crises identifiées.

#### MODALITÉS D'ÉVALUATION

Rapport de recherches et d'étude à partir d'une étude de cas – Rédaction d'un mémoire et d'une note de synthèse - Présentation orale.

## **Secteur d'activité et type d'emploi**

#### 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.

#### RÈGLEMENTATIONS 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.

## Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

|                                            |                                                                             |
|--------------------------------------------|-----------------------------------------------------------------------------|
| <b>Tension de recrutement (DARES 2024)</b> | Élevée (4/5)                                                                |
| <b>Facteurs principaux</b>                 | Non-attractivité salariale, Intensité d'embauche, Inadéquation géographique |
| <b>Salaire médian (mensuel)</b>            | 1 700 €                                                                     |
| <b>Familles professionnelles (FAP)</b>     | T3X61 — Agents de sécurité et de surveillance · tension 4/5 (Élevée)        |
| <b>Projets de recrutement (BMO 2026)</b>   | 24 576                                                                      |
| <b>Jugés difficiles à recruter</b>         | 48 %                                                                        |
| <b>Emplois saisonniers</b>                 | 23 %                                                                        |
| <b>Familles professionnelles (FAP)</b>     | T3X61 — Agents de sécurité et de surveillance                               |

## Voies d'accès

### MODALITÉS D'ACCÈS

Formation initiale, Formation continue, VAE

### PRÉREQUIS À L'ENTRÉE EN FORMATION

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.

### COMPOSITION DU JURY — FORMATION INITIALE, VAE

Un président (interne)

3 professionnels du domaine de la sûreté (externes)

### COMPOSITION DU JURY — FORMATION CONTINUE

Un président (interne)

3 professionnels du domaine de la sûreté (externes)

## Base légale

|                                            |            |
|--------------------------------------------|------------|
| <b>Date de décision</b>                    | 19/05/2021 |
| <b>Durée de l'enregistrement</b>           | 2 ans      |
| <b>Date d'échéance de l'enregistrement</b> | 19/05/2023 |

## Statistiques

| Année | Certifiés | Dont VAE | Insertion 6 mois | Métier 2 ans |
|-------|-----------|----------|------------------|--------------|
| 2018  | 29        | 0        | 94 %             | 88 %         |
| 2017  | 13        | 0        | 91 %             | 82 %         |
| 2016  | 9         | 0        | 89 %             | 89 %         |

## Liens avec d'autres certifications

ANCIENNES VERSIONS  
RNCP23703

NOUVELLE(S) CERTIFICATION(S)  
RNCP37783

## Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.cnpp.com/Boutique-Formations/Nos-atouts-pour-vous-former/Nos-certifications-professionnelles>

### Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/35599/>

## Entrées et sorties de formation

|                        |                   |
|------------------------|-------------------|
| Entrées en formation   | 19                |
| Parcours menés à terme | 16                |
| Taux d'achèvement      | 84 %              |
| Période                | 02/2022 – 09/2023 |

Entrées et sorties — Caisse des Dépôts (open data), tous organismes confondus.

## Demande CPF — formations engagées

|                          |                   |
|--------------------------|-------------------|
| Dossiers CPF engagés     | 26                |
| Montant total engagé     | 165 507 €         |
| Coût moyen par dossier   | 6 366 €           |
| Durée moyenne            | 95 h              |
| Période                  | 09/2021 – 05/2023 |
| France compétences       | 54 %              |
| Entreprise               | 28 %              |
| Reste à charge titulaire | 13 %              |
| France Travail           | 3 %               |
| OPCO                     | 2 %               |

Formations engagées via le CPF — Caisse des Dépôts (open data), tous organismes confondus.