MCP009 - Gestion de crise cyber : positionnez votre leadership

Présentation

Prérequis

Cette micro-certification ne nécessite pas de prérequis académiques, ni de connaissances techniques.

Objectifs pédagogiques

Adopter les bons réflexes et prendre des décisions éclairées sous pression, afin de limiter les impacts d'une crise sur l'entreprise.

Comprendre les mécanismes de gestion de crise et savoir organiser une réponse efficace en identifiant les rôles clés et les ressources nécessaires.

Renforcer une posture individuelle et collective en situation de crise, grâce à des exercices pratiques et des retours d'expérience entre pairs.

Identifier les acteurs de soutien internes et externes à mobiliser en cas de crise pour ne pas rester seul face aux défis.

Élaborer des stratégies de communication de crise claires et efficaces, pour préserver la confiance des collaborateurs, clients et partenaires.

Utiliser des outils comme le Business Impact Analysis (BIA) pour protéger les intérêts vitaux de l'entreprise.

Différencier les notions de crise, d'incident et de menace, et tirer des enseignements des crises passées pour améliorer les pratiques.

Intégrer les principes de la norme ISO 22361 afin d'aligner la sécurité et la résilience de la gestion de crise sur les standards internationaux.

Développer les compétences nécessaires pour anticiper, gérer et surmonter les crises cyber, en assurant la continuité de l'activité.

Compétences

Diriger et coordonner les équipes interservices pour assurer une réponse collective et efficace à la crise ; mobiliser rapidement les ressources humaines et matérielles nécessaires en situation de crise.

Identifier les actifs critiques et protéger les intérêts vitaux de l'entreprise (infrastructures IT, données clients, processus essentiels) pour garantir la continuité des opérations.

Mis à jour le 01-06-2025

Code : MCP009

Certification de type Experte

Enseignement de type mixte

0 crédits

Responsabilité nationale :
EPN05 - Informatique / Vania CONAN

Contact national :
Cnam Bretagne - PSDR3C
2 rue Camille Guérin
22440 Ploufragan
0972311312

psdr3c@Lecnam.net

Développer une communication stratégique en période de crise pour maintenir la confiance des parties prenantes ; fournir des informations claires et rassurantes afin de limiter la désinformation et les rumeurs.

Analyser les crises passées à partir de retours d'expérience (REX) et tirer des enseignements des incidents pour améliorer les pratiques de gestion de crise.

Mettre en place des mesures correctives et préventives pour renforcer la résilience organisationnelle.

Programme

Contenu

Cette micro-certification s'adresse aux acteurs décisionnaires en entreprise / collectivités, confrontés aux cybermenaces, qui souhaitent réagir en situation de crise et y préparer leur collectif.

Cela s'adresse tous les décisionnaires d'une organisation (exécutif, business. RH, finance, communication...) risquant d'être impliqués dans une cellule de crise.

Dans un contexte où les cyberattaques se multiplient et gagnent en complexité, aucune organisation n'est à l'abri. Les conséquences peuvent être lourdes : paralysie des systèmes, perte de données sensibles, atteinte à l'image de marque. Or, le collectif, le facteur humain, la préparation sont les clés de la survie de l'organisation en cas de crise. Il devient donc essentiel de former les équipes à adopter les bons réflexes, à réagir efficacement sous pression et à assurer la continuité d'activité.

Cette micro-certification répond à cet enjeu en développant des compétences clés en gestion de crise, communication stratégique et protection des intérêts vitaux de l'entreprise. Un atout concret pour renforcer la résilience des organisations face aux menaces numériques.

Modalités de validation

- Examen final

Description des modalités de validation

Réussite du test final

(minimum de 50% des points requis)