UpSkilling
Pilot your skills, create your future

Module de formation
Diriger son entreprise en intégrant les enjeux de cybersécurité dans ses processus et ses projets

Version du 01/12/2024

Formation distancielle adaptée aux besoins, intérêts et disponibilités de l'apprenant

Durée de validité de la version : 1 an renouvelable

A QUI S'ADRESSE CETTE FORMATION ?

Profils du stagiaire

- ★ Dirigeant d'entreprise ou cadre dirigeant

Prérequis

- ★ Remplir le questionnaire de positionnement et d'attentes

Information : ce module permet de se préparer au module suivant : "Développer son entreprise en intégrant la cybersécurité comme levier stratégique d'opportunités" adressant notamment : la gestion des incidents et crises cyber, Leadership et communication de crise, Intégration de la cybersécurité dans l'innovation et le business

OBJECTIFS PÉDAGOGIQUES ET COMPÉTENCES VISÉES

Au terme de la formation, le stagiaire sera capable de

- ★ Identifier et évaluer les risques cyber tout en alignant la stratégie de sécurité avec les objectifs de l'entreprise pour assurer la protection des actifs critiques et la continuité opérationnelle.
- ★ Piloter la mise en œuvre des solutions de cybersécurité en collaboration avec les équipes IT et métiers afin de garantir la résilience organisationnelle face aux cybermenaces.
- ★ Engager et responsabiliser l'ensemble des collaborateurs en intégrant la cybersécurité dans la culture d'entreprise pour réduire les risques humains et renforcer la vigilance collective.
- ★ Assurer le respect des cadres législatifs et normatifs en mettant en place une gouvernance de cybersécurité adaptée, afin de prévenir les sanctions et renforcer la confiance des parties prenantes.

Compétence(s) visé(e) :

- ★ Piloter la stratégie globale de cybersécurité de l'entreprise avec une compréhension des menaces actuelles, des enjeux réglementaires (RGPD, lois sectorielles) et des implications économiques, en évaluant les risques stratégiques pour les activités et en alignant les priorités de sécurité sur les objectifs de l'entreprise afin d'assurer la protection des actifs critiques, la résilience organisationnelle et la continuité opérationnelle.

- ★ Superviser et coordonner la mise en œuvre des solutions de cybersécurité en s'appuyant sur une maîtrise des solutions technologiques clés (systèmes de détection d'intrusion, chiffrement, pare-feu) et en assurant une gestion efficace des projets liés à la cybersécurité en collaboration avec les responsables IT et métiers pour minimiser les vulnérabilités et garantir la résilience organisationnelle face aux menaces.
- ★ Instaurer une culture d'entreprise centrée sur la cybersécurité en mettant en avant l'importance de la sensibilisation et de la formation des collaborateurs, en encourageant des comportements sécurisés et en montrant l'exemple à travers des pratiques sécuritaires au niveau exécutif afin de garantir que la sécurité devienne un pilier intégré dans toutes les actions et décisions stratégiques.
- ★ Superviser pour garantir la conformité de l'entreprise aux obligations réglementaires et normatives en matière de cybersécurité (RGPD, ISO 27001, PCI DSS, etc.), en mettant en place des processus internes de suivi et de mise à jour des exigences légales afin d'éviter les sanctions, de préserver la réputation de l'entreprise et de renforcer la confiance des parties prenantes.

CONTENU & PROGRESSION PÉDAGOGIQUE

Jour	Titre de la séquence	Contenu	Méthode pédagogique utilisées
J1 : Date de début	**S1 - Fondamentaux de la cybersécurité stratégique**	• Introduction aux enjeux de la cybersécurité • Pourquoi la cybersécurité est un enjeu stratégique pour l'entreprise ? • Les actifs critiques et leur importance en cybersécurité • Principes fondamentaux de gestion des risques en cybersécurité • Méthodologie pour cartographier les risques de l'entreprise • Les bonnes pratiques pour une approche méthodique de la cybersécurité • L'importance de la communication et de l'écoute dans la cybersécurité	**Apport théorique (0h30)** Assimiler les fondamentaux en cybersécurité, Capsules vidéos courtes et quiz **Atelier pratique (2h30)** Appliquer les notions en identifiant et priorisant ses actifs critiques : Exercice individuel + Matrice de criticité +Débriefing **Live Mentor (1h)** Échanger avec un expert sur l'alignement cybersécurité et stratégie, Discussion interactive + Retours d'expérience **Ressources types :** Template de cartographie des actifs à risque, Exemples concrets d'entreprises ayant subi des cyberattaques (études de cas), Matrice des risques pour aider à prioriser les menaces Checklist "Premières actions cybersécurité pour un dirigeant"
J1+ 1 semaine	**S2 - Évaluation des risques et définition de politiques de sécurité**	• Introduction aux méthodes d'analyse des risques • Présentation des méthodologies d'analyse des risques (EBIOS, ISO 31000, etc.) • Définition des objectifs de sécurité et des politiques de sécurité	**Apport théorique (0h30)** Comprendre l'évaluation des risques et la construction d'une politique de cybersécurité, Capsules vidéos courtes et quiz

		• Exemples de politiques de sécurité réussies et leurs impacts • Bonnes pratiques pour une gestion efficace des risques	**Atelier pratique (2h30)** Construire une matrice des risques et définir une première politique de sécurité Travail guidé + Analyse de cas **Live Mentor (1h)** Échanger sur les stratégies de cybersécurité adaptées à son entreprise Session interactive avec retour sur les matrices des participants **Ressources types :** Template de matrice des risques, Modèles de politiques de cybersécurité (ISO 27001, RGPD, PME vs grands groupes), Étude de cas : Exemples concrets de gestion des risques en entreprise, Checklist "Évaluer et formaliser sa politique de sécurité"
J1+ 2 semaines	**S3 - Conformité, homologation et gouvernance**	• Introduction à la conformité en cybersécurité : enjeux et réglementations • Les fondamentaux du RGPD et ses implications pour les entreprises • Introduction à ISO 27001 : le cadre international de gestion de la cybersécurité • Audit de conformité et gestion des écarts • Gouvernance et mise en place d'une politique de conformité continue	**Apport théorique (0h30)** Assimiler les cadres réglementaires et la gouvernance en cybersécurité, Capsules vidéos courtes et quiz **Atelier pratique (2h30)** Réaliser un audit simplifié et proposer des actions correctives, Étude de cas + Construction d'un tableau de bord **Live Mentor (1h)** Valider les choix stratégiques en matière de conformité et gouvernance, Session interactive avec retours sur audits et plans d'actions **Ressources types** : Checklist d'auto-évaluation RGPD et ISO 27001, Modèle de tableau de bord de suivi de conformité, Exemples de structures de gouvernance cybersécurité (PME, ETI, grands groupes), Guide : Les étapes pour mettre en place un audit de conformité efficace
J1+ 3 semaines	**S4 - Supervision des prestataires et partenaires**	• Pourquoi la gestion des prestataires et la gouvernance sont des piliers de la cybersécurité ? • Méthodes d'évaluation des prestataires en cybersécurité	**Apport théorique (0h30)** Comprendre comment évaluer, contractualiser et suivre les prestataires, Capsules vidéos courtes et quiz

		• Bonnes pratiques de contractualisation avec les prestataires • Introduction aux modèles de gouvernance en cybersécurité • Impliquer les parties prenantes dans la cybersécurité • Mise en place d'un comité de gouvernance cybersécurité • Préparer son entreprise à intégrer la cybersécurité comme levier stratégique d'opportunités	**Atelier pratique (2h30)** Analyser un contrat de prestation, construire une grille d'évaluation des fournisseurs et formaliser une gouvernance cyber **Live Mentor (1h)** Obtenir un retour expert sur les critères de sélection et les pratiques de gestion des prestataires, Session interactive avec feedback sur les exercices **Ressources types** : Modèle de gouvernance cybersécurité (PME, ETI, grands groupes), modèle de grille d'évaluation des prestataires, exemple de clauses contractuelles essentielles pour la cybersécurité, guide pour structurer un comité cybersécurité et piloter la gouvernance, checklist des bonnes pratiques pour l'implication des collaborateurs et partenaires, tableau de bord de suivi des engagements et performances en cybersécurité.

ORGANISATION ET EXPÉRIENCE DE FORMATION

Équipe pédagogique

Upskilling accompagnent et forment les entreprises à tirer partie des nouvelles technologies comme un levier de transformation et d'amélioration. Notre objectif est d'accompagner les professionnels à ancrer les nouvelles compétences digitales durablement.

Nos intervenants(bac +5) et plusieurs années d'expérience de pratique et de formation accompagnent les stagiaires dans leur parcours de formation.

La formation est ainsi animée par des professionnels de la cryothérapie et de l'andragogie, dont les compétences techniques, professionnelles et pédagogiques ont été validées par des certifications et/ou testées et approuvées par les éditeurs et/ou notre équipe pédagogique.

- Le directeur du programme est - Thomas Blanc - t.blanc@upskilling.com

Contact

Administratif - formation@upskilling.com

Moyens pédagogiques

Un intervenant vous guide dans votre progression et converse avec vous tout au long de votre apprentissage.
L'intervenant utilisera les différentes méthodes expositives, démonstratives, interrogatives, actives et expérientielles permettant d'acquérir les éléments théoriques et méthodologiques pour les mettre en pratique en séance et entre les séances.

Le produit Skillpilot est mis à disposition pour accéder aux ressources de mission ainsi que le livret pédagogique.
Skillpilot est une solution logiciel accessible depuis internet, un LMS mis à disposition des stagiaires et intervenants.

Format : distanciel (asynchrone et synchrone)

Durée

- Une durée totale de formation de 16h30 dont 4h en distanciel synchrone avec un intervenant
- Intensité de formation de 4 heures par semaine sur 4 semaines
- 0h30 de bilan / coaching individuel en fin de formation

Lieu : Classe virtuelle

Dispositif de suivi de l'exécution et de l'évaluation des résultat de la formation

Les stagiaires sont accompagnés et suivis : suivi des présences lors de la journée de formation

Les stagiaires sont préparés par l'intervenant avec des mises en situation tout au long de la formation en pratiquant

- Cas pratiques
- Mise en pratique dans leur contexte

À la fin de la formation, le stagiaire reçoit ses résultats et obtient son attestation de fin de formation si

- le stagiaire a été présent et impliqué sur l'ensemble de la formation
- le stagiaire a présenté ses travaux de mise en pratique lors des rendez-vous synchrones permettant d'évaluer la montée en compétence et la validation des critères
- le stagiaire a acquis 75% de l'ensemble des critères d'évaluation lors du bilan individuel(ci-après)

Barème et critère(s) d'évaluation de la (des)compétence(s) visée(s)

- **Piloter la stratégie globale de cybersécurité**
  Critère d'évaluation : Définir et formaliser une stratégie de cybersécurité alignée sur les objectifs de l'entreprise, intégrant une analyse des menaces, des risques et des enjeux réglementaires : acquis (100%) ou non acquis (0%)
  - La stratégie est formalisée dans un document structuré, Une analyse des menaces et des risques critiques est disponible, Stratégie alignée avec les objectifs stratégiques de l'entreprise
- **Superviser et coordonner la mise en œuvre des solutions de cybersécurité**
  Critère d'évaluation : Mettre en place et suivre des solutions technologiques adaptées (pare-feu, chiffrement, détection d'intrusion), en coordonnant leur déploiement avec les équipes IT et métiers. : acquis (100%) ou non acquis (0%)
  - Les solutions mises en place couvrent des risques identifiés, La collaboration avec les parties prenantes (IT/métiers , partenaire) elle structurée et suivie, Un suivi des performances et des vulnérabilités est-il réalisé régulièrement

- **Instaurer une culture d'entreprise centrée sur la cybersécurité**
  Critère d'évaluation : Déployer un programme de sensibilisation et de formation en cybersécurité, en engageant les collaborateurs à adopter des comportements sécurisés et en intégrant la sécurité dans les pratiques exécutives : acquis (100%) ou non acquis (0%)
    - Un programme de formation et de sensibilisation est mis en place, Les collaborateurs ont été formés et évalués sur leurs pratiques sécuritaires, La cybersécurité est intégrée dans les décisions stratégiques et la communication interne
- **Piloter la stratégie globale de cybersécurité**
  Critère d'évaluation : Réaliser un audit de conformité annuel et mettre en place un plan d'action correctif pour assurer le respect des normes RGPD, ISO 27001 et autres réglementations en vigueur : acquis (100%) ou non acquis (0%)
    - Un audit de conformité a été réalisé et documenté, Les écarts identifiés ont été corrigés via un plan d'action, Un suivi des évolutions réglementaires et une mise à jour des processus sont mis en place

A la fin de la session de formation, le stagiaire recevra un formulaire d'évaluation à chaque fin de session de formation pour mesurer la qualité de la formation

Moyens techniques

Merci de bien vouloir vérifier que vous avez à disposition un environnement informatique :

- Ordinateur connecté à internet
- Webcam et micro

Accessibilité

UPSKILLING répond à la réglementation concernant l'accessibilité aux personnes en situation de handicap. Dans ce contexte, il veille à l'application des conditions d'accueil et d'accès des publics en situation de handicap.

Notre processus suit des étapes précises et concrètes : Identification d'un potentiel handicap, détermination de la typologie du handicap : moteur, auditif, visuel, intellectuel, psychique ou visuel, transmission d'un questionnaire pour mettre en place les compensations possibles et personnalisables en adéquation avec le besoin du stagiaire qu'il aura exprimé.

Dans le cas d'une formation en salle chez le client, celui-ci est sollicité pour garantir le respect de nos processus.

Référent Handicap avec adresse mail : Thomas BLANC t.blanc@upskilling.com

Modalité d'inscription et délais d'accès

Les inscriptions pour effectuer une analyse du besoin avec l'équipe formation auprès de formation@upskilling.com

1. Analyse du besoin
2. Validation du projet de formation
3. Contractualisation

En corrélation avec le délai de rétractation (10 jours L6353-5 du code de travail), le délais d'accès minimum est fixé à 10 jours (délais entre inscription et date de démarrage)

Effectif plafond / Plancher

Plancher : À partir de 5 personnes
Plafond : 10 personnes
Ces éléments respectent nos normes qualité pour garantir la meilleure expérience de formation.

Tarif(s)

Session Inter-entreprise : 940 € ht / stagiaire

Coût salle de formation si souhaité par le client à déterminer (lieux et tarifs proposés par Upskilling)
Hors frais de déplacement (hors de Pau 64000)

Les CGV et de règlement sont disponibles dans la rubrique informations pratiques du : https://upskilling.com