Mise à jour : 01/03/2026

FORMATION : Cybersécurité Pour les dirigeants

PUBLIC	Cette formation est à destination des dirigeants d'entreprise (TPE, PME, ETI et GE).
PRÉREQUIS	Prérequis : ▪ Connaissances générales en informatique. ▪ Aucune expertise technique approfondie requise. Matériel requis : ▪ Ordinateur portable avec accès Internet, accès administrateur pour les ateliers.
MODALITÉS ET DÉLAIS D'ACCÈS	En présentiel : ⇨ Formation en présentiel : lieu de formation communiqué en amont de la formation. ⇨ Inscription à réaliser 1 mois avant le démarrage de la formation. En distanciel : ⇨ Formation individuelle ou collective à distance sous la forme de visioconférence participative. ⇨ Inscription à réaliser 1 mois avant le démarrage de la formation.
DURÉE	7H pour une période de 1 jour.
DATES	À définir avec l'organisme de formation
HORAIRES	⇨ Les horaires de formation sont : 9H à 12H et de 13H à 17H ⇨ Le monitoring et l'assistance pédagogique sont disponibles du lundi au vendredi de 9H à 18H.
LIEU	En présentiel : ⇨ Sur site ⇨ Au siège de Tricolor Expertise ⇨ Autre adresse En distanciel : ⇨ Formation à distance – visioconférence **Pour les personnes en situation de handicap : Nous adaptons nos formations en fonction de votre handicap et nous mettrons tout en œuvre pour vous accueillir ou pour vous réorienter si besoin.** **Vous pouvez nous contacter au 06 34 31 28 65**
TARIF	1 490€ par personne
NOMBRE DE PARTICIPANTS	En présentiel : Jusqu'à 12 personnes En distanciel : Jusqu'à 5 personnes
OBJECTIF DE LA FORMATION ET COMPÉTENCES VISÉES	À l'issue de la formation, le participant sera capable de mettre en œuvre les compétences suivantes : ▪ Comprendre pourquoi la cybersécurité est un enjeu de direction générale. ▪ Avoir une lecture claire du paysage des menaces sans entrer dans la technique. ▪ Identifier les arbitrages clés relevant du niveau direction. ▪ Mettre en place une organisation adaptée à la taille et aux enjeux de l'entreprise. ▪ Connaître ses obligations et éviter les sanctions. ▪ Savoir comment réagir et diriger en situation de crise cybersécurité. ▪ Repartir avec un plan d'action concret et priorisé.
MODALITÉS D'ÉVALUATION D'ATTEINTE DES OBJECTIFS DE LA FORMATION	⇨ Évaluation individuelle du profil, des attentes et des besoins du participant avant le démarrage de la formation ⇨ Évaluation des connaissances & compétences en début et en fin de formation via un QCM ⇨ Tests de contrôle de connaissances et validation des acquis à chaque étape ⇨ Travaux pratiques et mises en situation ⇨ Echange avec le formateur ou la formatrice par visioconférence (webinar), téléphone et mail ⇨ Questionnaire d'évaluation de la satisfaction en fin de formation

CONTENU	Dans cette formation, le participant aura accès au programme suivant :
MODULE 1	**La cybermenace vue du dirigeant (1h)** 1. Chiffres clés : coût moyen d'une cyberattaque, taux de survie des entreprises après un incident majeur 2. Les attaques qui visent spécifiquement les dirigeants : fraude au président, whaling, compromission de messagerie dirigeant 3. Études de cas : entreprises françaises victimes et conséquences réelles (arrêt de production, perte de clients, liquidation) 4. La responsabilité personnelle du dirigeant : juridique, pénale, vis-à-vis des actionnaires et des assureurs 5. Cybersécurité et continuité d'activité : ce que risque concrètement votre entreprise
MODULE 2	**Comprendre les menaces sans être technicien (1h)** 1. Les 5 menaces prioritaires pour les entreprises : ransomware, phishing, fraude financière, espionnage, attaque via un prestataire 2. Comment fonctionne une attaque en 3 étapes simples : intrusion, propagation, impact 3. Les cibles privilégiées dans une entreprise : messagerie du dirigeant, comptabilité, accès VPN, données clients 4. L'humain comme premier vecteur : pourquoi vos collaborateurs sont la cible numéro 1 5. Ce que les cybercriminels cherchent dans votre entreprise spécifiquement
MODULE 3	**Les décisions stratégiques à prendre (1h)** 1. Définir son appétit au risque : jusqu'où accepte-t-on d'être exposé ? 2. Les 5 décisions fondamentales que seul le dirigeant peut prendre : budget, organisation, prestataires, assurance, communication de crise 3. Comment allouer un budget cybersécurité sans être expert 4. Internaliser ou externaliser : critères de décision pour une PME ou ETI 5. La cybersécurité dans les projets stratégiques : fusion-acquisition, digitalisation, internationalisation 6. Comment challenger son DSI ou son prestataire informatique sur la sécurité
MODULE 4	**Gouvernance et organisation de la cybersécurité (1h)** 1. Qui fait quoi : DSI, RSSI, prestataire, direction — clarifier les rôles et responsabilités 2. Les instances à mettre en place : comité sécurité, reporting régulier, escalade en cas d'incident 3. La politique de sécurité : ce que le dirigeant doit valider et porter 4. Intégration de la cybersécurité dans la culture d'entreprise : l'exemplarité du dirigeant 5. Gestion des prestataires et fournisseurs : les questions à poser, les clauses à exiger 6. Les indicateurs que tout dirigeant devrait suivre : 5 KPI simples et actionnables
MODULE 5	**Obligations légales et réglementaires (1h)** 1. RGPD : ce que risque concrètement le dirigeant en cas de violation de données (sanctions CNIL, recours clients) 2. NIS2 : êtes-vous concerné ? Obligations et calendrier 3. Obligations sectorielles : finance (DORA), santé (HDS), défense, collectivités 4. Obligation de notification en cas d'incident : CNIL sous 72h, ANSSI, clients, partenaires 5. Ce que votre assureur attend de vous : conditions d'éligibilité à la cyber-assurance
MODULE 6	**Gérer une crise cyber (1h)** 1. Les premières heures d'une attaque : ce que doit faire le dirigeant (et ce qu'il ne doit pas faire) 2. La cellule de crise : composition, déclenchement, rôles 3. Communication de crise : vers les clients, les partenaires, les médias, les autorités 4. Décider de payer ou non une rançon : critères, position des autorités françaises, risques juridiques 5. Dépôt de plainte : pourquoi, où, comment (ANSSI, police, parquet) Retour d'expérience : les erreurs de management les plus fréquentes en situation de crise cyber

	MODULE 7	**Construire sa feuille de route et passer à l'action (1h)** 1. Les 10 mesures prioritaires recommandées par l'ANSSI pour tout dirigeant 2. Auto-évaluation 3. Comment choisir un prestataire de confiance : label ExpertCyber, questions à poser 4. L'assurance cyber : ce qu'elle couvre vraiment, comment bien se couvrir Atelier final : chaque participant repart avec ses 3 actions prioritaires à lancer dans les 30 jours
MOYENS PERMETTANT LE SUIVI ET L'APPRÉCIATION DES RÉSULTATS		Suivi de l'exécution : ⇨ Feuilles de présences signées par les participants et le formateur ou la formatrice par demi-journée ⇨ Attestation de fin de formation mentionnant les objectifs, la nature et la durée de l'action et les résultats de l'évaluation des acquis de la formation. Appréciation des résultats : ▪ Recueil individuel des attentes du stagiaire ▪ Questionnaire d'auto-évaluation des acquis en début et en fin de formation ▪ Évaluation continue durant la session ▪ Remise d'une attestation de fin de formation Questionnaire d'évaluation de la satisfaction en fin de formation
MOYENS PÉDAGOGIQUES ET TECHNIQUES D'ENCADREMENT DES FORMATIONS		Modalités pédagogiques : ▪ Évaluation des besoins et du profil du participant ▪ Apport théorique et méthodologique : séquences pédagogiques regroupées en différents modules ▪ Contenus des programmes adaptés en fonction des besoins identifiés pendant la formation ▪ Réflexion et échanges sur cas pratiques ▪ Questionnaires, exercices, ateliers et étude de cas ▪ Tests de contrôle de connaissances et validation des acquis à chaque étape ▪ Retours d'expériences Éléments matériels : ▪ Mise à disposition de tout le matériel pédagogique nécessaire (pour les formations en présentiel) ▪ Support de cours au format numérique projeté sur écran et transmis au participant par mail à la fin de la formation Référent pédagogique et formateur/formatrice : Chaque formation est sous la responsabilité de la directrice pédagogique de l'organisme de formation ; le bon déroulement est assuré par le formateur ou la formatrice désigné(e) par l'organisme de formation.