Version 6 – 2026

LC FORMATIONS
CONSEIL & DEVELOPPEMENT

PROGRAMME DE FORMATION

CYBERSÉCURITÉ ET IA : RISQUES ET BONNES PRATIQUES

DOCUMENT REMIS AU STAGIAIRE
AVANT SON INSCRIPTION

CONTACT / RENSEIGNEMENT :

CASTILLON LAURÈNE — 06.69.23.18.16
CONTACT@LC-FORMATIONS.FR

FORMATION CYBERSÉCURITÉ ET IA : RISQUES ET BONNES PRATIQUES

OBJECTIFS PROFESSIONNELS :

A l'issue de la formation, le stagiaire sera capable de :

- Identifier les nouvelles menaces cyber liées à l'intelligence artificielle : phishing augmenté, deepfakes, fraude au président
- Utiliser les outils d'IA en entreprise sans exposer ses données sensibles ni celles de ses clients
- Mettre en place des règles et réflexes de protection efficaces pour son organisation

CATÉGORIE ET BUT

La catégorie prévue à l'article L.6313-1 est : Action de formation

Cette action a pour but (article L.6313-3) : De favoriser l'adaptation des travailleurs à leur poste de travail, à l'évolution des emplois ainsi que leur maintien dans l'emploi et de participer au développement de leurs compétences en lien ou non avec leur poste de travail.

PUBLIC

Le public concerné est : tout public.

PRÉ-REQUIS

Les conditions d'accès sont :
Pré-requis : Aucun
Niveau exigé : Débutant

DURÉE

Cette formation se déroule sur un volume de 7 à 100 heures, soit 1 à 15 jours.
Le volume horaire et le nombre de jours sont définis à l'issue de l'analyse du besoin, en fonction du niveau du stagiaire et des objectifs visés.
Volume horaire exact, dates et horaires : voir convention de formation.

TARIF

Tarif : sur devis.
Le coût est établi en fonction du volume horaire retenu et des modalités de la formation. Il est communiqué dans le devis adressé avant toute contractualisation, puis repris dans la convention de formation.

Organisme de formation net de TVA.

FORMATION CYBERSÉCURITÉ ET IA : RISQUES ET BONNES PRATIQUES

MODALITÉS ET DÉLAIS D’ACCÈS

L’inscription est réputée acquise lorsque : La convention de formation est signée.
Les délais d’accès à l’action sont : 15 jours avant le début de l’action de formation.

FORMATION CYBERSÉCURITÉ ET IA : RISQUES ET BONNES PRATIQUES

MOYENS PÉDAGOGIQUES, TECHNIQUES ET D'ENCADREMENT

MÉTHODES ET OUTILS PÉDAGOGIQUES

L'organisation pédagogique repose sur l'individualisation accompagnée avec présence pédagogique constante du formateur.

OUTILS PÉDAGOGIQUES : L'intervenant alternera apports théoriques illustrés de cas réels d'attaques, démonstrations en direct des menaces et des parades, et ateliers pratiques d'analyse de risques appliqués à l'organisation de chaque stagiaire.
Les exercices permettront de valider les acquis tout au long de la formation. Le stagiaire travaillera sur des cas concrets, notamment la détection de tentatives de phishing générées par IA, l'analyse de deepfakes et la construction d'une charte d'usage de l'IA pour son entreprise.

SUPPORTS PÉDAGOGIQUES : Livret explicatif.

PRISE EN COMPTE DU HANDICAP : Les personnes en situation de handicap peuvent tout à fait rejoindre notre formation. Merci de nous contacter pour toute situation particulière.

ELÉMENTS MATÉRIELS DE LA FORMATION

Équipements divers mis à disposition : un ordinateur avec connexion internet sera mis à disposition du stagiaire.
Documentation : Le formateur s'appuiera sur des supports de cours détaillés, des études de cas d'attaques récentes, les référentiels ANSSI et CNIL et des fiches réflexes remis aux stagiaires.

COMPÉTENCES DES FORMATEURS

Le formateur référent possède les qualités nécessaires à la mise en place d'un parcours modulaire. Il a un rôle de formateur accompagnateur. Il réajuste en permanence le contenu de la formation en fonction des avancées du stagiaire. Il reste à l'écoute des besoins et répond au mieux aux attentes.

La formation est assurée par un formateur référent, spécialisé dans le domaine de la formation, sélectionné pour ses compétences pédagogiques et son expérience professionnelle. Son identité, son curriculum vitae et ses qualifications sont communiqués au stagiaire avant le démarrage de l'action et annexés à la convention de formation.

FORMATION CYBERSÉCURITÉ ET IA : RISQUES ET BONNES PRATIQUES

CONTENU DE LA FORMATION

PARTIE 1 - COMPRENDRE LE NOUVEAU PAYSAGE DES MENACES À L'ÈRE DE L'IA

- Comment l'IA a industrialisé la cybercriminalité : attaques plus rapides, plus crédibles, plus massives
- Le phishing nouvelle génération : e-mails parfaits, sites clonés et messages hyper-personnalisés
- Deepfakes audio et vidéo : la fraude au président et l'usurpation d'identité de dirigeants
- Les chiffres clés et cas réels récents pour mesurer l'exposition de son entreprise

PARTIE 2 - DÉTECTER LES ATTAQUES ASSISTÉES PAR IA

- Les signaux qui trahissent un e-mail ou un message frauduleux même très bien rédigé
- Reconnaître un deepfake vocal ou vidéo : indices techniques et procédures de contre-vérification
- Les procédures de validation à double canal pour les demandes sensibles : virements, accès, données
- Entraîner ses équipes : transformer chaque collaborateur en première ligne de défense

PARTIE 3 - UTILISER LES OUTILS D'IA SANS METTRE SES DONNÉES EN DANGER

- Ce que deviennent les données saisies dans ChatGPT, Copilot, Gemini et les autres outils grand public
- Les règles d'or : quelles informations ne jamais confier à une IA publique
- Paramétrer correctement ses outils : historique, entraînement, offres professionnelles et clauses de confidentialité
- Le shadow AI : reprendre le contrôle sur les usages non déclarés dans l'entreprise
- Les injections de prompt et manipulations d'agents IA : comprendre ces nouvelles attaques

PARTIE 4 - PROTÉGER SON ENTREPRISE AU QUOTIDIEN

- Les fondamentaux d'hygiène numérique renforcés : mots de passe, double authentification, mises à jour, sauvegardes
- L'IA au service de la défense : outils de détection et de protection accessibles aux PME
- Rédiger une charte d'usage de l'IA claire et applicable pour ses équipes
- Réagir en cas d'incident : les premiers gestes, les obligations de notification et les contacts utiles

PARTIE 5 - MAÎTRISER LE CADRE RÉGLEMENTAIRE

- RGPD et outils d'IA : responsabilités, bases légales et droits des personnes
- L'IA Act européen : classification des risques et obligations pour les entreprises utilisatrices
- La directive NIS2 et les obligations de sécurité qui concernent de plus en plus d'organisations
- Construire son plan d'action cybersécurité et IA : prioriser les mesures selon ses risques réels

SUIVI ET ÉVALUATION

EXÉCUTION DE L'ACTION

Les moyens permettant de suivre l'exécution de l'action sont :

- Feuilles de présence émargées par les stagiaires et le formateur

FORMATION CYBERSÉCURITÉ ET IA : RISQUES ET BONNES PRATIQUES

- Attestation remise aux stagiaires ayant suivi la formation Cybersécurité et IA : risques et bonnes pratiques avec assiduité

MODALITÉS D'ÉVALUATION DES RÉSULTATS (OU D'ACQUISITION DES COMPÉTENCES)

Les moyens mis en place pour déterminer si le stagiaire a acquis les connaissances ou les gestes professionnels précisés dans les objectifs sont :

- Questions orales et exercices pratiques
- Analyses de cas et exercices de détection validant les acquis tout au long de la formation
- Mise en situation finale

LC FORMATIONS
CONSEIL & DEVELOPPEMENT