

# Elaborer et mettre en oeuvre une démarche de cybersécurité

RS6986 · RS · Publiée

## L'essentiel

|                       |                            |
|-----------------------|----------------------------|
| Code(s) NSF           | 326                        |
| Formacode(s)          | 31045                      |
| Type d'enregistrement | Enregistrement sur demande |
| Date d'enregistrement | 18/12/2024                 |
| Date d'échéance       | 18/12/2029                 |

## Certificateur(s)

ECOLE SUP INFORM COMMERCE · SIRET : 45303523000094

## Partenaires habilités

4 organismes habilités, d'après la liste publiée par France compétences : 1 à former et organiser l'évaluation et 3 à former.

| Organisme                 | SIRET          | Habilitation                     |
|---------------------------|----------------|----------------------------------|
| CERTYOU                   | 80450946100013 | Former                           |
| CONNECT LEARNING          | 90469485800013 | Former                           |
| ECOLE SUP INFORM COMMERCE | 45303523000094 | Former et organiser l'évaluation |
| EVOLUTION5                | 84999183100025 | Former                           |

## Résumé de la certification

### OBJECTIFS ET CONTEXTE

Avec l'augmentation exponentielle des interactions et des activités économiques numériques, ainsi que l'évolution et l'intensification des menaces cybernétiques, il est crucial pour les petites et moyennes entreprises (PME) et les très petites entreprises (TPE) d'être équipées pour faire face à ces défis. La cybersécurité est un enjeu majeur, vital, pour ces TPE et PME, mais elle est également fondamentale pour la santé économique du pays. En protégeant leurs propres opérations et celles de leurs partenaires, ces entreprises renforcent leur pérennité et instaurent une confiance mutuelle avec toutes leurs parties prenantes.

Néanmoins, la perception et la gestion du risque cybernétique sont souvent insuffisantes au sein de ces petites et moyennes entreprises. Leur vulnérabilité les rend de plus en plus attractives pour les cybercriminels. Pour évoluer de manière sécurisée dans ce paysage numérique, ces entreprises doivent impérativement renforcer leur cybersécurité, en tenant compte de leur taille, de leur secteur d'activité et du budget qu'elles peuvent allouer à la cybersécurité. Cependant, elles ne peuvent pas toujours se permettre de recruter du personnel dédié exclusivement à la cybersécurité.

C'est là que cette certification entre en jeu ;

elle s'adresse aux professionnels des TPE et PME qui, sans occuper un poste dédié à la cybersécurité, vont être chargés d'élaborer et de mettre en œuvre une démarche de cybersécurité, c'est-à-dire détecter, gérer, défendre et réagir à toute forme d'attaque cybernétique. Elle est destinée aux professionnels travaillant dans les domaines de l'informatique qui souhaitent acquérir des compétences spécifiques en matière de cybersécurité : Au sein des TPE, ces profils occupent la fonction de responsable informatique ; Au sein des PME, ces profils occupent la fonction de responsable informatique, ou de directeur technique (CTO) ; Lorsque le sujet de la cybersécurité est entièrement

externalisé, cela concerne un public de consultants, salariés d'entreprises spécialisées en technologies de l'information et de la communication, occupant la fonction de consultant en systèmes informatiques, ou de technicien en support informatique, chargés de comptes comme des TPE et PME.

#### COMPÉTENCES ATTESTÉES

Analyser la vulnérabilité de l'entreprise en réalisant un inventaire des équipements, des logiciels et des interconnexions avec l'extérieur, en identifiant les vulnérabilités et les menaces par rapport au système d'information de l'entreprise, en élaborant et en appliquant une politique de veille sur les menaces et les risques internes et externes liés aux attaques de chaîne d'approvisionnement (altération du code, diffusion massive de code malveillant, détournement d'applications légitimes), et en mobilisant les méthodes d'analyse de risques (EBIOS RM, ISO 27005), afin d'évaluer les risques associés à ces vulnérabilités.

Établir un état des lieux du niveau de sécurité de l'entreprise et du respect de ses obligations réglementaires, en analysant les responsabilités juridiques de l'entreprise en matière de cybersécurité, en identifiant les bonnes pratiques ainsi que les points de sécurisation à envisager,

et en dressant un plan de sécurisation du SI et en sensibilisant la direction de l'organisation sur les mesures de protection à adopter et sur la conduite à tenir en cas de crise cyber, afin d'évaluer les besoins et conditions de mise en œuvre d'un futur plan d'amélioration.

Définir une politique de sécurité, en préconisant une solution de surveillance adaptée (EDR, SIEM...), et en établissant les règles de sécurité de l'entreprise relatives à l'utilisation des SI, aux mises à jour des appareils, des logiciels et des antivirus, et à la gestion des sauvegardes, afin de sécuriser les données

Gérer les identités et contrôles d'accès, en définissant leurs modalités de gestion, et en contrôlant tout équipement et personne ayant une relation technique avec le SI, afin de limiter l'accès aux données sensible.

Sensibiliser les collaborateurs de l'entreprise, en établissant un code de bonne conduite comprenant les comportements adaptés et les précautions techniques et juridiques à appliquer, en organisant la diffusion des bonnes pratiques d'acculturation aux règles d'hygiène fondamentales de la cybersécurité, en prenant les dispositions nécessaires pour l'acculturation des collaborateurs en situation de handicap, et en vérifiant la bonne compréhension des enjeux associés à la cybersécurité par l'ensemble des parties prenantes, sur les différents types de risques et leurs moyens de prévention, l'impact sur la réputation de l'entreprise et les conséquences financières, afin d'infuser une culture de la cybersécurité au sein de l'entreprise.

Gérer une situation d'urgence par l'alerte et la sécurisation, en sécurisant les collaborateurs, les lieux et les équipements, en évacuant les lieux si nécessaire, en alertant les autorités et les organisations pertinentes (banques, CNIL, parties prenantes dont les données personnelles sont exposées...), en mettant en place une cellule de crise centralisant la réponse à l'incident, et en établissant des outils de communication et de partage d'information, indépendants du système attaqué, et en déclenchant un plan de continuité de l'activité en prenant en compte les difficultés observées et les optimisations envisagées dans le déroulement de la crise, afin d'assurer une coordination rapide avec les parties prenantes et de minimiser les conséquences négatives de la situation.

Réaliser les opérations de réponse à incident sans destruction de données ou de traces, en identifiant des indicateurs de compromission issus des données de surveillance, en évaluant l'étendue et la nature de l'incident, et en isolant l'élément compromis, en mettant en œuvre un plan d'action et en restaurant les opérations normales, en documentant les actions réalisées afin de fournir un rapport d'incident détaillé, et en fournissant ensuite aux collaborateurs les outils, la documentation et les méthodes pour éviter le récurrence, afin de remédier à la situation et d'assurer la reprise de l'activité.

## Secteur d'activité et type d'emploi

#### RÉGLEMENTATIONS D'ACTIVITÉ

Celles couvrant les obligations réglementaires et normatives en lien avec les activités

## Voies d'accès

#### COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE

2 professionnels du secteur non intervenant dans l'établissement, dont l'un est président du jury, et 1 membre de l'organisme certificateur (Directeur ou Responsable pédagogique)

## Base légale

|                                      |            |
|--------------------------------------|------------|
| Date de décision                     | 18/12/2024 |
| Durée de l'enregistrement            | 5 ans      |
| Date d'échéance de l'enregistrement  | 18/12/2029 |
| Date de dernière délivrance possible | 17/06/2030 |

## Liens avec d'autres certifications

ANCIENNES VERSIONS  
RS5332

## Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.esic-online.com/nos-certifications/elaborer-une-dmarche-de-cyberscurit-26>

### Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/6986/>

## Où se former

|                        |                    |
|------------------------|--------------------|
| Formations référencées | 38                 |
| Organismes             | 4                  |
| Régions couvertes      | 1                  |
| Prix indicatif         | 1 650 € – 14 400 € |
| Durée                  | 21 – 175 h         |

Offre de formation — MonCompteFormation (Caisse des Dépôts), licence ouverte.

## Entrées et sorties de formation

|                        |                   |
|------------------------|-------------------|
| Entrées en formation   | 314               |
| Parcours menés à terme | 300               |
| Taux d'achèvement      | 96 %              |
| Période                | 01/2025 – 09/2026 |

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

## Demande CPF — formations engagées

|                        |                   |
|------------------------|-------------------|
| Dossiers CPF engagés   | 386               |
| Montant total engagé   | 990 625 €         |
| Coût moyen par dossier | 2 566 €           |
| Durée moyenne          | 28 h              |
| Période                | 01/2025 – 09/2026 |
| France compétences     | 71 %              |

|                                    |      |
|------------------------------------|------|
| <b>OPCO</b>                        | 16 % |
| <b>Reste à charge titulaire</b>    | 8 %  |
| <b>France Travail</b>              | 3 %  |
| <b>Entreprise</b>                  | 3 %  |
| <b>Compte d'engagement citoyen</b> | 0 %  |

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