

Elaborer et mettre en oeuvre une démarche de cybersécurité

RS5332 · RS · Publiée

L'essentiel

Code(s) NSF	326
Formacode(s)	31006, 14297
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	20/01/2021
Date d'échéance	20/01/2023

Certificateur(s)

ECOLE SUP INFORM COMMERCE · SIRET : 45303523000094

Partenaires habilités

2 organismes habilités, d'après la liste publiée par France compétences : 2 à former.

Organisme	SIRET	Habilitation
CERTYOU	80450946100013	Former
MICHEL KARTNER	79333268500023	Former

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le numérique occupe une place grandissante dans notre société. Avec ces évolutions, les cyberattaques sont de plus en plus importantes, tant en nombre qu'en intensité. Elles visent les particuliers, les entreprises, les administrations ou les États. Pour faire face à ces cyber-attaques des nouveaux métiers se créent. Ces métiers liés à la cybersécurité sont très divers, mais s'organisent autour d'activités et de compétences communes. On peut notamment citer les métiers de : Consultant cybersécurité, Évaluateur sécurité, Analyste de la menace, Expert réponse à incident, Chef de projet sécurité, Architecte sécurité, Administrateur sécurité, etc.

Cette certification permet d'acquérir les compétences transversales des métiers de la cybersécurité, et répond ainsi au besoin :

- o des entreprises, des administrations et de l'État (Internet, marketing, commerce, industrie...) et à leur forte demande de profils experts de la cybersécurité ;
- o des salariés, demandeurs d'emploi, personnes en reconversion, étudiants souhaitant développer des compétences pour intégrer ce secteur porteur.

COMPÉTENCES ATTESTÉES

Pilotage de la gouvernance de la cybersécurité

- Définir les orientations de cybersécurité
- Définir les moyens alloués à la cybersécurité
- Établir une cartographie fonctionnelle
- Définir l'organisation et les responsabilités en matière de cybersécurité
- Établir la documentation de cybersécurité
- Intégrer la cybersécurité dans les projets
- Définir et utiliser des indicateurs cybersécurité

- Communiquer en interne et sensibiliser le personnel
- Responsabiliser le personnel
- Gérer les autorisations du personnel
- Protéger les biens des clients et des partenaires
- Gérer les achats
- Choisir des prestataires de confiance
- Gérer les interfaces

Gestion des systèmes d'information sécurisés

- Cartographier les systèmes
- Sécuriser la manipulation des informations sensibles
- Concevoir et développer des systèmes sûrs
- Gérer les chaînes d'approvisionnement
- Valider la cybersécurité lors de la recette
- Exploiter de manière sécurisée
- Gérer la maintenance et le maintien en condition de sécurité
- Encadrer l'évolution des systèmes
- Garantir la sécurité lors du retrait de service
- Définir les principes de maîtrise des droits d'accès
- Définir les principes d'identification et d'authentification
- Définir les rôles et les profils
- Limiter l'accès selon des principes d'habilitation
- Gérer les droits utilisateurs selon leur cycle de vie
- Contrôler les droits d'accès

Gestion des risques et protection des systèmes

- Analyser les risques cyber relatifs aux systèmes
- Homologuer les systèmes d'information
- Confirmer le développement de confiance des composants
- Utiliser des composants qualifiés
- Configurer correctement ses composants
- Utiliser des services cryptographiques à l'état de l'art et protéger ses clés
- Garantir la robustesse des authentifiants et mots de passe
- Garantir la disponibilité des servitudes
- Résister aux événements naturels, incidents et attaques physiques
- Protéger les accès physiques
- Contrôler l'accès physique des personnes
- Se prémunir contre les risques électromagnétiques
- Se prémunir contre les codes malveillants
- Protéger les réseaux
- Protéger les équipements
- Protéger les données
- Protéger les supports de données
- Contrôler les accès logiques
- Protéger l'administration des systèmes
- Garantir la non-répudiation des actions
- Renforcer la vigilance et la protection

Évaluation du niveau de sécurité

- Identifier les écarts au référentiel
- Évaluer par rapport à l'état de l'art
- Rechercher des traces de compromission
- Corriger les problèmes identifiés
- Organiser des entraînements et des exercices à destination du personnel afin de vérifier que des procédures adaptées aux crises sont correctement mises en place et opérationnelles
- Organiser des entraînements et des exercices à destination des prestataires externes afin de vérifier que des procédures adaptées aux crises sont correctement mises en place et opérationnelles

Gestion des incidents de cybersécurité

- Disposer d'une chaîne opérationnelle de gestion des incidents
- Collecter les événements de sécurité
- Détecter les événements anormaux
- Reconstituer le scénario des incidents, les vecteurs et leur étendue
- Évaluer l'impact et le périmètre de l'incident sur l'activité
- Organiser la réaction
- Préparer des mesures de réaction
- Conduire la réaction
- Réaliser un retour d'expérience
- Se préparer à un sinistre
- Garantir la résilience de ses systèmes
- Réagir face à un sinistre

Voies d'accès

MODALITÉS D'ACCÈS

Formation initiale, Formation continue

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE

- 2 professionnel(le)s du secteur non intervenant dans l'établissement, dont l'un est président du jury (1 membre du collège employeur et 1 membre du collège employés)
- 1 membre du centre de formation (Directeur(trice) ou Responsable pédagogique)

Base légale

Date de décision	20/01/2021
Durée de l'enregistrement	2 ans
Date d'échéance de l'enregistrement	20/01/2023

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)

RS6986

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://esic-online.com/certification-cyber-securite/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/5332/>

Entrées et sorties de formation

Entrées en formation	491
Parcours menés à terme	484
Taux d'achèvement	99 %
Période	02/2022 – 09/2023

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

Demande CPF — formations engagées

Dossiers CPF engagés	533
Montant total engagé	1 119 080 €
Coût moyen par dossier	2 100 €
Durée moyenne	25 h
Période	02/2021 – 01/2023
France compétences	93 %
Reste à charge titulaire	5 %
France Travail	1 %
Régions	0 %
Entreprise	0 %
Compte d'engagement citoyen	0 %

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