Aligner son système d'information (SI) sur le RGPD

Référence : **SECSSI** Durée : **2 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Avoir suivi la formation SECDPO - Data Protection Officier est un plus. • Avoir suivi la formation SECGDPR - sensibilisation RGPD..

PROFIL DES STAGIAIRES

• Déléqués à la Protection des Données ou Data Protection Officer, DSI, RSSI, toute personne amenée à aligner son système d'information sur le RGPD.

OBJECTIFS

• Acquérir les bonnes pratiques de sécurisation du SI en cohérence avec le RGPD. • Comprendre comment sécuriser l'accès physique au système d'information et aux données. • Connaître les points de vigilance concernant les sous-traitants/fournisseurs (clauses contractuels, audits…). • Etre capable de mettre en place des solutions techniques permettant de répondre aux demandes des personnes (droit à l'oubli, anonymisation…). • Etre capable de sécuriser l'accès physique au système d'information. • Prévenir les risques d'intrusion, d'usurpation, de détournement.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Management de la sécurité

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Types de risques physiques

- Comment éviter les intrusions physiques dans les locaux et dans le datacenter ou salle serveur
- Comment éviter la perte ou le vol d'un équipement

Identifier les risques qui pèsent sur le réseau

- Comment éviter la destruction d'un équipement, physique, d'un composant software ou de GED
- Comment sauvegarder / archiver les fichiers partagés (messagerie, données sortie / données source)
- Comment cadre les transferts de données hors UE

Types de risques par composants SI

- Comment protéger les données : cartographier les données et les traitements
- Comment détecter les vulnérabilités
- Comment tracer un incident ou des accès non autorisés
- Comment détecter une atteinte aux données
- Comment se prémunir d'une gestion défaillante des droits d'accès
- Comment éviter/identifier l'usurpation d'identité d'un compte utilisateur, d'un compte administrateur
- Comment éviter/identifier l'exfiltration de données
- Comment éviter l'interception d'échanges
- Comment appliquer les mises à jour de sécurité

- Identifier l'absence de cloisonnement des données personnelles
- Définir des règles de rétention des données (durée de conservation)
- Transférer de manière sécurisée des données personnelles

Relations avec les sous-traitants et fournisseurs

- Comment piloter un sous-traitant / fournisseur
- Comment se prémunir de la négligence d'un sous-traitant / fournisseur
- Comment se prémunir de l'intervention frauduleuse d'un sous-traitant

Comment répondre aux demandes d'application des droits de la personne

- Preuve du consentement, retrait du consentement (opposition ou suppression)
- Accès – rectification – effacement
- Anonymiser / pseudonymiser