FICHE DE FORMATION

Certification Qualiopi — Indicateur 1

Intitulé de la formation	**Droit du numérique — Législation, réglementation et criminalistique informatique**
Référence	DN-2026-001
Durée	1 jour — 7 heures (09h00 à 17h00)
Tarif	300 € par apprenant (net de taxe — organisme non soumis à TVA)
Modalité pédagogique	Présentiel uniquement
Public cible	Techniciens, administrateurs réseau, responsables informatiques, juristes, personnels des établissements de santé (GHT, hôpitaux, cliniques)
Prérequis	Notions de base en informatique et réseaux — Exercer dans un environnement numérique professionnel
Effectif max.	15 apprenants

1. CONTEXTE ET PRÉSENTATION DE LA FORMATION

Cette formation d'une journée offre une approche complète du droit du numérique appliqué aux environnements professionnels, et plus particulièrement aux établissements de santé.

Elle couvre la législation et la réglementation générales, le dispositif cyber national, les obligations et droits des administrateurs, les situations d'attaques réelles (cas concrets sur les hôpitaux), ainsi que les protocoles de criminalistique numérique utilisés par les enquêteurs et experts judiciaires.

2. OBJECTIFS PÉDAGOGIQUES

À l'issue de cette formation, le stagiaire sera capable de :

- Identifier le cadre législatif et réglementaire applicable au numérique (RGPD, NIS 1 & 2, Code de la Santé Publique, OIV)
- Connaître le dispositif national de cybersécurité et les rôles des acteurs (ANSSI, Cyber-préfet, Police, Gendarmerie, Douanes)
- Maîtriser les droits et obligations des administrateurs réseau (confidentialité, traçabilité, article 40 CPP, cybersurveillance)
- Analyser des cas concrets d'attaques cyber dans le secteur de la santé

- Comprendre et appliquer les protocoles de criminalistique numérique (gel de lieux, collecte de preuve, DFIR, ISO 20037)
- Appréhender la recevabilité de la preuve numérique en justice

3. PROGRAMME DÉTAILLÉ

09h00 – 10h30	**Rappel législatif, réglementaire et dispositif national cyber** OIV et législation associée — Plan blanc cyber — Directives NIS 1 et NIS 2 — RGPD — Code de la Santé Publique — Cadre propre au GHT — Rôle de l'ANSSI et de ses équipes d'intervention — Présentation du dispositif national Cyber — Rôle des acteurs : Cyber-préfet, Police, Gendarmerie, Douanes, DIRECTE
10h30 – 12h00	**Droits et obligations des techniciens et administrateurs réseau** Notion de DICP — Principe de moindre gêne — Confidentialité — Responsabilité et faute de service — Obligation de transparence — Traçabilité des opérations de maintenance — Arrêt NIKON et droit à la vie privée résiduelle — Secret des correspondances (courriel) — Article 40 CPP — Perquisition informatique — Droit pénal du numérique — Cybersurveillance — Notion de Hack Back
12h00 – 13h00	*Pause repas (non-prise en charge)*
13h00 – 15h00	**Études de cas pratiques — Attaques cyber dans le secteur de la santé** Analyse d'attaques réelles visant des hôpitaux et cliniques — Résultats d'enquêtes judiciaires dans la sphère cyber — Approche des techniques d'intervention des services spécialisés
15h00 – 17h00	**Criminalistique informatique (Digital Forensics)** Protocoles des cyber-enquêteurs et experts judiciaires — Gel de lieux numériques — Copies de sauvegarde et artefacts — Logiciels et matériels dédiés (bloqueurs en écriture, mallettes CELLEBRITE et XRY) — Notion de DFIR — Cycle : Identification, préservation, acquisition, analyse, documentation, présentation judiciaire — Standard ISO 20037 — Loyauté et intégrité de la preuve — Traçabilité des collectes — Recevabilité en justice — Live Forensics vs Dead Forensics

4. MÉTHODES ET MOYENS PÉDAGOGIQUES

Apports théoriques	Mises en situation	Supports et outils
• Cours magistraux illustrés • Présentation des textes de loi • Documentation ANSSI officielle	• Études de cas réels (hôpitaux) • Démonstrations de matériel forensique • Questions / réponses interactifs	• Support de cours remis au stagiaire • Matériel forensique (mallettes CELLEBRITE, XRY, bloqueurs) • Vidéoprojecteur, tableau blanc

5. MODALITÉS D'ÉVALUATION ET DE SUIVI

Positionnement	Recueil des attentes et évaluation des prérequis en début de journée (questionnaire oral ou écrit)
Évaluation formative	Quiz et questions/réponses tout au long de la formation — Mises en situation sur les études de cas
Évaluation sommative	QCM de fin de journée permettant de valider les acquis — Grille d'évaluation des compétences
Satisfaction	Questionnaire de satisfaction à chaud remis en fin de formation
Attestation	Attestation de fin de formation individuelle délivrée à chaque stagiaire ayant suivi l'intégralité de la journée
Feuille d'émargement	Signature obligatoire par demi-journée (matin et après-midi)

6. ACCESSIBILITÉ ET CONDITIONS D'ACCÈS

Délai d'accès	Inscription possible jusqu'à 5 jours ouvrés avant le début de la formation
Accessibilité PSH	Notre organisme prend en compte les situations de handicap. Merci de nous contacter avant l'inscription pour étudier les adaptations possibles (référent handicap disponible sur demande)
Lieu	Présentiel — Salle de formation équipée fournie par l'organisateur ou dans les locaux du commanditaire (sur accord préalable)

7. PROFIL DU FORMATEUR

- Expert en droit du numérique et cybersécurité
- Ancien membre ou collaborateur de services enquêteurs spécialisés (Cybercriminalité)
- Expérience terrain en criminalistique numérique (DFIR) et interventions judiciaires
- Formateur régulier auprès d'établissements de santé, collectivités et administrations

Document établi conformément au référentiel national Qualiopi — Indicateur 1 (Information du public) | Version 1.0 — 2024