# PROTECTION NUMÉRIQUE DES ENTREPRISES (PNE)

GESTIC FORMATION
Formation Professionnelle • Logiciel • Solution Informatique

## Prérequis

> Savoir utiliser un ordinateur (basique).
> Savoir naviguer sur Internet (basique).
> Posséder des notions sur la sécurité informatique.

## Objectifs

> Mieux appréhender la sûreté informatique et ainsi être en mesure de sécuriser votre entreprise.
> Comprendre les risques malveillants informatiques en interne et en externe de l'entreprise en prise directe avec l'humain.
> Comprendre ce qu'est la cybercriminalité.
> Identifier les risques informatiques.
> Savoir prendre en compte les failles de sécurité et en aviser son responsable qualité-sécurité et informaticien afin qu'il mette en place les mesures sécuritaires adaptées.
> Être pro-réactif par rapport à une attaque informatique.
> Être force de proposition en matière de sécurité informatique.
> Anticiper un risque informatique.
> Pouvoir suivre la sécurité mise en œuvre par un prestataire informatique.
> Savoir maîtriser son système d'information.
> Pouvoir anticiper une Gestion de Crise (GC).
> Être sensible à la mise en place d'un PRA et PCA et pouvoir indiquer le processus de la création de ces 2 plans.

## Modalités d'évaluation

> Un questionnaire initial pour les apprenants pour tester leurs connaissances.
> Des questionnaires au fil de l'eau sous format numérique seront effectués sur les thématiques abordées (100 questions).
> Un questionnaire final pour évaluer les nouvelles connaissances des apprenants.

*Ces questionnaires seront soumis soit en format papier soit par l'intermédiaire d'une application anonymisée.*

## Public

> Salarié, non salarié, gérant, gérant non salarié, artisan, demandeur d'emploi.

## Compétences

> Utilisation de l'outil informatique (ordinateur, tablette, smartphone).
> Sensibilité aux nouvelles technologies numériques.
> Appétence à l'environnement numérique.
> Être à l'écoute des progrès technologiques.

## Qualités - Aptitudes

> Veille.
> Assiduité.
> Vigilance.
> Autonomie.
> Écoute.
> Pertinence.

## Délai d'accès

> Selon le calendrier en cours - Merci de prendre contact avec notre service.

## Durée

> 3 jours soit 21 heures.

## Tarif

> 790€HT/jour soit 948€TTC/jour en intra-entreprise - Nous consulter.

## Lieu

> En nos locaux à Biard. Possibilités en vos locaux sous conditions - nous contacter.

## Méthodes mobilisées

> 100% face à face pédagogique.
> Notre pédagogie est basée sur la mise en pratique de cas professionnels avec alternance d'apports théoriques et de mise en pratique informatique tout au long des modules afin de valider les acquis.
> Des démonstrations techniques pourront être réalisées.
> Des présentations et des cas concrets seront explicités, analysés pour une meilleure compréhension des risques et permettront de formater une mise en place des parades.
> Les stagiaires disposeront en fin de séance d'un support en trois parties « bons réflexes » permettant de sécuriser l'entreprise le soir à la fermeture des bureaux.
> Chaque stagiaire travail sur un PC.
> Intra-Entreprise ou Inter-Entreprises.
> 100% Présentiel ou distanciel (visio) - Nous contacter.

## Contenu

*La première journée se focalise sur les données, les locaux, les prestataires,*

*« Selon le rythme de pratique, il faut de 1 à 3 mois pour acquérir solidement le contenu d'un déroulé pédagogique »*



Gestic Formation - 1 Rue de la Tardiverie - ZAE Larnay - 86580 Biard- Tél. : 05 49 52 55 04 - Mail : info@gestic-formation.com

*le télétravail et toutes les possibilités permettant d'être davantage sécurisé. Un exemple de Plan de Continuité d'Activité (PCA) et Plan de Reprise d'Activité (PRA) sera abordé lors de la seconde journée qui permettra de limiter les impacts des attaques malveillantes ou de dysfonctionnement numérique.*

*Une approche de la sécurisation de vos données sera effectuée par le biais de fondamentaux édités par la CNIL.*
*Cette formation s'effectue sur 22 modules pouvant être présentés aléatoirement suivant les besoins des apprenants*

*Audit de positionnement - questionnaire numérique*

***Partie 1 : sécuriser les systèmes d'information***

> Sécuriser le poste de travail.
> Comment protéger les postes nomades, BYOD et mobiles.
> Comment sécuriser votre réseau informatique.
> Une des priorités : la protection de vos serveurs.
> Un vecteur de communication, votre site WEB.
> Un plan de sécurité du système d'information.

***Partie 2 : les personnels***

> La priorité : sensibiliser vos utilisateurs.
> Authentifier vos utilisateurs.
> Comment gérer les habilitations.
> Comment tracer les accès et gérer les incidents.

***Partie 3 : vos données, vos locaux et vos prestataires***

> Pensez à la sécurisation de vos archives.
> Maintenance et destruction de vos données.
> Comment gérer votre sous-traitance.
> Échanger en sécurité avec les tiers.
> Et vos locaux, y avez-vous pensé ?
> Les développements informatiques.
> Le chiffrement des données et leur intégrité.
> Plan de secours informatique – sauvegarde.
> PCA – PRA (études dossiers) - la gestion de crise (information).
> Le SOC (information).
> Le télétravail.
> Le bien-être sur la protection de vos données.

*Audit de positionnement - questionnaire numérique*

## Votre contact

> **Marina Laurent** • Assistante Administrative et Commerciale :
**m.laurent@gestic-formation.com**
**05 49 52 55 04**

## Accessibilité

> Nos locaux sont accessibles au public en situation de handicap.
> Centre Handi-Accueillant.

> **Amélie Bertin** • Référente Handicap :
**a.bertin@gestic-formation.com**

*« Selon le rythme de pratique, il faut de 1 à 3 mois pour acquérir solidement le contenu d'un déroulé pédagogique »*