



Livre blanc Altevia Tech

Édition cabinets d'avocats

Cybersécurité
et cabinets d'avocats

Protéger vos dossiers, sécuriser votre activité, préserver votre responsabilité

Préambule

Dans un cabinet d'avocats, la confiance est un actif fondamental.

Elle repose sur la compétence juridique, la déontologie, le secret professionnel et la capacité à accompagner les clients sans rupture ni exposition.

Aujourd'hui, cette confiance dépend aussi d'un élément devenu central mais encore trop souvent mal maîtrisé

le système informatique.

La cybersécurité n'est plus un sujet technique ni un simple enjeu réglementaire.

Elle est devenue une **composante directe de la responsabilité professionnelle du cabinet.**

Ce livre blanc s'adresse aux dirigeants de cabinets qui souhaitent:

- comprendre les risques réels
- structurer une approche claire
- assumer un cadre durable et maîtrisé
- sans céder à la complexité ni à la peur.

L'informatique comme outil de production juridique

Un cabinet d'avocats moderne repose intégralement sur son système informatique pour

- l'accès aux dossiers
- la production des actes
- la gestion des délais
- la facturation
- la communication avec les clients et les juridictions

L'activité juridique est désormais continue, numérique et souvent nomade.

La moindre indisponibilité peut avoir un impact immédiat sur

- la continuité de l'activité
- le respect des délais
- la relation client
- la responsabilité du cabinet

**Dans ce contexte, l'informatique n'est plus un support.
C'est un outil de production juridique critique.**

La nature spécifique des risques cyber pour les cabinets d'avocats

Des données à très haute valeur

Les cabinets d'avocats détiennent des informations sensibles par nature

- stratégies de défense
- contentieux en cours
- données personnelles
- éléments financiers
- documents confidentiels

Ces données intéressent particulièrement les cybercriminels, les acteurs opportunistes ou les attaques ciblées.

Une exposition juridique directe

Une fuite, une perte ou une indisponibilité de données peut entraîner

- une mise en cause de la responsabilité professionnelle
- des sanctions réglementaires
- une perte de confiance immédiate des clients
- un préjudice réputationnel durable

Dans un cabinet d'avocats, les conséquences d'un incident* cyber dépassent largement le cadre technique.

Les fausses certitudes les plus répandues

Ce que beaucoup de cabinets pensent

De nombreux cabinets pensent être protégés car

- ils ont un antivirus
- ils font des sauvegardes
- ils utilisent des outils reconnus
- ils n'ont jamais eu d'incident

Ces éléments sont nécessaires mais très insuffisants.

Ce que montrent les incidents réels

La majorité des incidents graves surviennent dans des environnements

- partiellement protégés
- mal configurés
- mal compris par leurs utilisateurs
- sans responsabilité clairement définie

**La cybersécurité ne se résume pas à des outils.
Elle repose avant tout sur une organisation claire et assumée.**

Le changement de paradigme nécessaire

La cybersécurité efficace repose sur trois principes fondamentaux.

La simplicité

- Un système simple, documenté et compris est plus sécurisé qu'un système complexe et mal maîtrisé.

L'intégration

- La sécurité ne doit pas être ajoutée après coup.
- Elle doit être intégrée au fonctionnement normal du cabinet.

La responsabilité: quelqu'un doit assumer clairement

- le bon fonctionnement
- la sécurité
- la continuité
- la réaction en cas d'incident

La cybersécurité est un cadre de responsabilité à poser, pas un empilement de solutions à subir.

Questions clés pour les dirigeants de cabinets d'avocats

Pouvez vous répondre clairement à ces questions

- savez vous exactement où sont stockées vos données sensibles ?
- pouvez vous garantir l'accès aux dossiers en cas d'incident majeur ?
- les accès sont ils strictement maîtrisés ?
- les sauvegardes sont elles réellement exploitables ?
- les responsabilités sont elles clairement définies ?
- savez vous qui pilote votre informatique au quotidien ?
- vous sentez vous serein sur ce sujet ?

Si ces réponses ne sont pas immédiates, le risque existe déjà.

L'approche Altevia Tech pour les cabinets d'avocats

Altevia Tech accompagne les cabinets d'avocats avec une approche pensée pour les dirigeants

- claire
- progressive
- sans jargon inutile
- orientée responsabilité et sérénité.

Nous prenons en charge l'ensemble du système informatique du cabinet

- la gestion du parc informatique
- le support utilisateurs
- la supervision continue
- les sauvegardes et la continuité d'activité
- la gestion des accès et des identités

La cybersécurité est intégrée par défaut.

Elle fait partie du fonctionnement quotidien, pas d'un projet ponctuel.

Objectif

- un système stable, prévisible et pilotable
- une exposition réduite
- un cadre clair
- de la sérénité pour le dirigeant.

Nous assumons la responsabilité du bon fonctionnement de votre informatique.

Une méthode progressive et durable

Notre démarche repose sur une progression maîtrisée

- comprendre l'existant
- identifier les risques
- stabiliser le socle
- définir une trajectoire réaliste
- superviser et faire évoluer dans le temps

Vous démarrez simplement.
Nous construisons dans la durée.

Conclusion

La cybersécurité n'est pas une contrainte supplémentaire.

C'est un choix de gouvernance.

Un cabinet d'avocats qui maîtrise son informatique

- protège ses clients
- assume sa responsabilité
- préserve sa réputation
- travaille sereinement

Avec Altevia Tech, vous faites le choix

- d'un partenaire responsable
- d'un cadre clair
- d'une sécurité intégrée
- d'une informatique qui ne soit plus jamais un sujet.

Prochaines étapes

Un diagnostic cybersécurité confidentiel pour cabinets d'avocats

- une analyse factuelle
- des priorités claires
- une vision maîtrisée

Pour en discuter

contact@altevia-tech.com
www.altevia-tech.com

