

LIVRE BLANC

Guide Maintenance TMA & Run

Sécurité • Disponibilité • Pérennité de vos projets digitaux

Transformer un client ponctuel en client récurrent — Lecture 10 minutes

Ce document contient

- 6 sections opérationnelles sur la maintenance digitale
- 1 tableau complet des types de maintenance (correctif, préventif, sécurité...)
- 1 guide d'organisation des demandes et du reporting
- 3 modèles d'engagement avec grille tarifaire comparative
- 10 signaux d'alerte à détecter chez vos clients
- 1 checklist finale de 28 points avec niveaux de priorité

Version 1.0 — 2026

Contexte et objectifs

La maintenance d'un projet digital est souvent le parent pauvre des relations client-prestataire. Livrée, la solution est considérée comme « terminée ». Or, un site ou une application sans maintenance active est un projet qui se dégrade silencieusement.

Ce guide a un double objectif : aider les équipes techniques à formaliser une offre de maintenance solide, et fournir aux clients les arguments pour comprendre pourquoi la TMA n'est pas un coût optionnel, mais un investissement de protection.

Objectif stratégique : transformer un projet livré en relation récurrente. Une maintenance bien structurée est la base d'une relation client durable, prévisible et à haute valeur ajoutée.

01 Pourquoi la maintenance est critique

Les risques réels d'un projet sans TMA

Un projet digital non maintenu est exposé à quatre catégories de risques majeurs. Chacune peut avoir des conséquences directes sur la continuité d'activité et la réputation du client.

1.1 — Failles de sécurité

Les vulnérabilités logicielles sont découvertes et publiées quotidiennement. Sans mise à jour régulière, un projet devient une cible accessible. Les conséquences peuvent être immédiates et graves.

Type de faille	Origine	Impact potentiel	Fréquence
Injection SQL	Plugin ou code non patché	Vol ou destruction de données	Très élevée
XSS (Cross-Site Scripting)	Librairie JavaScript obsolète	Détournement de sessions utilisateur	Élevée
Accès non autorisé	Mot de passe par défaut non changé	Prise de contrôle du back-office	Élevée
Déni de service (DDoS)	Absence de protection CDN/WAF	Indisponibilité totale du site	Moyenne
Infection malware	Core CMS non mis à jour	Blacklist Google, perte de SEO	Élevée

1.2 — Mises à jour incompatibles

L'écosystème digital évolue en permanence. PHP, Node.js, les frameworks, les CMS et leurs dépendances publient régulièrement des nouvelles versions. Sans suivi, les incompatibilités s'accumulent et rendent chaque mise à jour plus dangereuse.

- Un plugin mis à jour sans tester la compatibilité peut casser une fonctionnalité critique
- Une version PHP en fin de support n'est plus patchée et expose le serveur
- Une dépendance abandonnée par son mainteneur représente une dette technique sûreléevée
- La dette technique s'accumule exponentiellement : plus on attend, plus la remise à niveau coûte cher

1.3 — Incidents en production

Un incident en production sans plan de réponse défini se transforme systématiquement en crise. Le temps de résolution est directement corrélé à la qualité de la supervision mise en place en amont.

Scénario d'incident	Sans maintenance	Avec maintenance
Site inaccessible	Découverte par le client ou ses utilisateurs	Alerte automatique en quelques minutes
Formulaire de contact cassé	Détecté après perte de leads (jours, semaines)	Détecté via monitoring fonctionnel
Pic de trafic inattendu	Saturation serveur, site hors ligne	Autoscaling ou intervention préventive
Erreur après déploiement	Rollback manuel risqué et long	Procédure de rollback testée et documentée
Certificat SSL expiré	Alerte sécurité navigateur, perte de confiance	Renouvellement automatique surveillé

1.4 — Dette technique

La dette technique est invisible jusqu'au jour où elle bloque. Elle se constitue progressivement : chaque correctif rapide, chaque dépendance gardée trop longtemps, chaque fonctionnalité ajoutée sans refactoring contribue à la dégrader.

Règle des 1-5-15 : résoudre un problème immédiatement coûte 1. Le résoudre après 6 mois coûte 5. Le résoudre après 2 ans coûte 15. La maintenance préventive est économiquement rationnelle.

02

Ce qu’une vraie maintenance doit inclure

Les 5 dimensions d’une TMA complète

Une maintenance réduite aux corrections d’urgence n’est pas une TMA : c’est de la réactivité. Une offre de maintenance structurée couvre cinq dimensions complémentaires qui, ensemble, garantissent la pérennité et la performance du projet.

Dimension	Définition	Exemples d’actions	Fréquence
Correctif	Résolution des anomalies et incidents détectés en production	Correction de bug, incident serveur, erreur 500, formulaire cassé	À la demande / SLA défini
Préventif	Anticipation des problèmes avant qu’ils surviennent	Mises à jour CMS, plugins, dépendances, PHP/Node sur staging	Mensuel ou trimestriel
Sécurité	Protection active contre les menaces et vulnérabilités	Patch critique, audit dépendances (npm audit, WPScan), revue permissions	Continu + urgence
Supervision	Surveillance en temps réel de la disponibilité et des performances	Monitoring uptime, alertes, logs applicatifs, suivi Lighthouse	Continu
Évolutif (Run)	Améliorations fonctionnelles légères dans le cadre du contrat	Ajout d’un champ, modification de wording, petite feature UX	Selon forfait

2.1 — Ce qui ne doit PAS être inclus dans une TMA

Définir les limites de la TMA est aussi important que définir son contenu. Une confusion entre maintenance et développement génère des tensions, des dérives de périmètre et une rentabilité érodée.

Nature de la demande	Classification correcte	Traitement
Correction d’un bug en production	Maintenance correctif	Inclus dans le contrat TMA
Mise à jour d’un plugin existant	Maintenance préventif	Inclus dans le contrat TMA
Ajout d’une nouvelle page ou section	Développement évolutif majeur	Devis spécifique ou ticket Run si forfait évolutif
Refonte graphique partielle	Projet	Hors contrat TMA, devis dédié
Nouvelle intégration API tierce	Développement	Hors contrat TMA, devis dédié
Amélioration légère d’UX (< 1h)	Run évolutif	Inclus si forfait évolutif, sinon devis

03 Organisation recommandée

Process, traçabilité et reporting

La qualité d'une maintenance se juge autant à son organisation qu'à sa technique. Un client qui ne voit pas les actions réalisées perçoit la maintenance comme un coût opaque. La visibilité est un élément clé de la valeur perçue.

3.1 — Canal de demande unique

Toute demande de maintenance doit passer par un canal formalisé. L'email ou le téléphone comme unique canal de communication est un anti-pattern : les demandes se perdent, la traçabilité est nulle et la facturation devient impossible à justifier.

Canal	Avantages	Inconvénients	Recommandation
Email uniquement	Simple pour le client	Zéro traçabilité, perte de demandes, impossible à prioriser	[--] À éviter
Outil de ticketing (Jira, Linear, Notion...)	Traçabilité complète, historique, priorisation	Courbe d'apprentissage client	[OK] Recommandé
Portail client dédié	Expérience client optimale, reporting intégré	Mise en place plus lourde	[OK] Idéal
Chat (Slack, Teams)	Réactivité, relation informelle	Confusion urgence / non-urgence, no tracking	⚠ En complément uniquement

3.2 — Matrice de priorisation des demandes

Toutes les demandes ne sont pas égales. Définir une matrice de priorisation claire, acceptée contractuellement, évite les conflits et permet de gérer les attentes.

Priorité	Définition	Exemples	Délai d'intervention
P0 — Critique	Service totalement indisponible ou données compromises	Site hors ligne, faille active exploitée, données exposées	< 2h
P1 — Urgent	Fonctionnalité critique dégradée	Tunnel de commande cassé, formulaire ne s'envoyant plus	< 8h ouvrables
P2 — Normal	Anomalie visible mais non bloquante	Affichage incorrect sur mobile, lien cassé	< 3 jours ouvrables
P3 — Bas	Amélioration, évolution légère ou question	Wording à modifier, petite retouche CSS	Prochain sprint / lot

3.3 — Traçabilité et reporting mensuel

Un rapport mensuel est le meilleur outil de rétention client. Il transforme un service invisible en preuve de valeur tangible. Il doit être simple, visuel et orienté business.

Rubrique du rapport	Contenu	Format
Résumé exécutif	Statut global du projet, faits marquants du mois	3 lignes max
Tickets traités	Liste avec titre, priorité, temps passé, statut	Tableau
Consommation du forfait	Crédits utilisés vs disponibles, report éventuel	Jauge visuelle
Mises à jour effectuées	CMS, plugins, dépendances mis à jour ce mois	Liste
Disponibilité (uptime)	% uptime du mois, incidents éventuels	Chiffre clé
Alertes et recommandations	Points d'attention pour le mois suivant	Section dédiée
Prévisions mois suivant	Actions planifiées, échéances	Planning

04 Modèles d'engagement

Forfaits, SLA et structures tarifaires

Il n'existe pas de modèle universel de contrat de maintenance. Le bon modèle dépend de la criticité du projet, du profil du client et du niveau de service attendu. Voici trois approches éprouvées, complémentaires ou alternatives selon les contextes.

4.1 — Comparatif des modèles

Modèle	Principe	Avantages client	Avantages prestataire	Adapté pour
Forfait mensuel fixe	Montant fixe couvrant un périmètre défini (surveillance, mises à jour, X tickets)	Budget prévisible, service garanti	Revenu récurrent, planification possible	Projets stables, clients b-to-b
Crédit-temps	Achat d'un volume d'heures prépayées, consommées à la demande	Flexibilité, paiement au réel	Simple à vendre, faible risque	Petits projets, clients c&ad'achat ponctuel
Contrat SLA	Engagements contractuels sur les délais de réponse et de résolution selon la criticité	Garanties mesurables et opposables	Premium justifié, relation structurée	E-commerce, secteurs réglementés, fort enjeu

4.2 — Structure type d'un forfait mensuel

Un forfait maintenance bien structuré comprend trois niveaux, permettant au client de choisir selon la criticité de son projet et son budget.

Composante	Forfait Essentiel	Forfait Business	Forfait Critique
Surveillance uptime	[OK] 24/7	[OK] 24/7	[OK] 24/7 + alertes SMS
Mises à jour sécurité	[OK] Urgentes	[OK] Urgentes + mensuelles	[OK] Continues
Mises à jour préventives	[--]	[OK] Trimestrielles	[OK] Mensuelles
Tickets correctifs	2 tickets/mois	5 tickets/mois	Illimité
Run évolutif	[--]	2h/mois	4h/mois
Rapport mensuel	[--]	[OK] Simplifié	[OK] Détaillé
Délai réponse P0	< 8h ouvrables	< 4h ouvrables	< 2h (24/7)
Sauvegarde vérifiée	Mensuelle	Hebdomadaire	Quotidienne
Environnement staging	[--]	[OK]	[OK]

4.3 — Engagements SLA recommandés

Les SLA (Service Level Agreements) sont des engagements contractuels mesurables. Ils doivent être réalistes, atteignables, et assortis d'une compensation claire en cas de non-respect.

Indicateur	Définition	Cible recommandée	Compensation si non-respect
Disponibilité (uptime)	% de temps où le service est accessible	>= 99,5% / mois	Avoir sur facturation suivante
Délai de prise en charge P0	Délai entre ouverture du ticket et 1ère réponse	< 2h (heures convenues)	Escalade automatique
Délai de résolution P0	Délai entre prise en charge et correction	< 8h	Avoir proportionnel
Délai de prise en charge P1	Idem pour incidents urgents	< 8h ouvrables	Mention au rapport mensuel
Délai de livraison ticket P2/P3	Livraison de la correction en staging	< 5 jours ouvrables	Report planifié documenté

05 Signaux d'alerte

Détecter une maintenance insuffisante chez un client

Ces signaux sont des indicateurs que la maintenance en place est insuffisante ou inexistante. Ils constituent autant d'arguments pour proposer une offre TMA adaptée, ou pour déclencher un audit avant de prendre en charge le projet.

Signal d'alerte	Ce que ça révèle	Risque associé	Niveau
Tout passe par email	Zéro traçabilité, pas de priorisation	Perte de demandes, facturation opaque	[!] Élevé
Pas de suivi des tickets	Aucun historique des interventions	Impossible de justifier la valeur	[!] Élevé
Pas d'environnement de staging	Tests en production directement	Régressions non détectées avant mise en ligne	[X] Critique
Mises à jour jamais faites (> 6 mois)	Accumulation de vulnérabilités connues	Piratage, infection, blacklist Google	[X] Critique
Aucune sauvegarde testée	Fausse sécurité, sauvegardes potentiellement corrompues	Perte irréversible de données	[X] Critique
Pas de monitoring uptime	Les incidents sont signalés par les utilisateurs	Réaction toujours tardive, image dégradée	[!] Élevé
Pas de rapport d'activité	Le client ne voit pas ce qui est fait	Érosion de la valeur perçue, résiliation	[!] Élevé
Pas de SLA défini	Attentes non alignées entre client et prestataire	Conflits récurrents sur les délais	[~] Moyen
Aucune documentation	Dépendance totale au prestataire actuel	Difficulté à changer, risque de blocage	[~] Moyen
Pas de procédure d'urgence	Pas de plan B en cas d'incident majeur	Improvisation coûteuse en temps de crise	[!] Élevé

Règle des 3 critiques : si les 3 signaux 'Critique' (staging absent, mises à jour non faites, sauvegardes non testées) sont présents simultanément, un incident majeur n'est pas possible — il est probable. Déclencher un audit immédiatement.

06 Checklist maintenance

Votre maintenance est-elle suffisante ?

Cette checklist permet d'évaluer rapidement la qualité de la maintenance en place sur un projet. Elle peut être utilisée en audit client, en phase de reprise, ou comme grille d'autodiagnostic.

BLOC A — Sécurité

#	Vérification	Priorité	Statut
A1	Les dépendances sont auditées régulièrement (npm audit, WPScan ou équivalent)	Critique	☐
A2	Les mises à jour de sécurité sont appliquées dans les 72h après publication	Critique	☐
A3	Le certificat SSL est valide et son renouvellement est automatisé	Élevé	☐
A4	Les accès (admin, SSH, BDD) ont été vérifiés et nettoyés dans les 12 derniers mois	Critique	☐
A5	Un pare-feu applicatif (WAF) ou une protection CDN est en place	Élevé	☐

BLOC B — Disponibilité et supervision

#	Vérification	Priorité	Statut
B1	Un monitoring uptime est actif avec alertes automatiques	Critique	☐
B2	Les logs applicatifs et serveur sont accessibles et consultés régulièrement	Élevé	☐
B3	Un outil de tracking d'erreurs (Sentry ou équivalent) est en place	Élevé	☐
B4	Le temps de chargement est surveillé (Lighthouse, Core Web Vitals)	Moyen	☐
B5	Une procédure d'urgence (contacts, rollback, escalade) est documentée	Critique	☐

BLOC C — Sauvegardes

#	Vérification	Priorité	Statut
C1	Des sauvegardes automatiques de la BDD sont en place (fréquence définie)	Critique	☐
C2	Les sauvegardes sont stockées off-site (ne pas sauvegarder sur le même serveur)	Critique	☐

#	Vérification	Priorité	Statut
C3	Une restauration a été testée et validée dans les 3 derniers mois	Critique	☐
C4	La durée de rétention des sauvegardes est définie et respectée	Élevé	☐

BLOC D — Mises à jour préventives

#	Vérification	Priorité	Statut
D1	Un environnement de staging existe et est maintenu à jour	Critique	☐
D2	Toutes les mises à jour sont testées sur staging avant la production	Critique	☐
D3	Le CMS ou framework principal est sur une version supportée (< 2 versions majeures)	Élevé	☐
D4	Les plugins/dépendances obsolètes ou abandonnés sont identifiés	Élevé	☐
D5	Un calendrier de mises à jour préventives est planifié (mensuel ou trimestriel)	Moyen	☐

BLOC E — Organisation et gouvernance

#	Vérification	Priorité	Statut
E1	Toutes les demandes passent par un outil de ticketing (pas uniquement par email)	Élevé	☐
E2	Une matrice de priorisation (P0 à P3) est définie et acceptée contractuellement	Élevé	☐
E3	Les SLA de réponse et de résolution sont écrits dans le contrat	Élevé	☐
E4	Un rapport mensuel est envoyé au client avec la consommation du forfait	Élevé	☐
E5	La documentation technique est à jour (architecture, procédures, contacts)	Moyen	☐
E6	Le client a été formé ou briefé sur le bon usage du canal de demande	Moyen	☐
E7	Les accès critiques sont sauvegardés dans un gestionnaire de mots de passe partagé	Élevé	☐
E8	Une revue de maintenance est organisée avec le client au moins une fois par an	Moyen	☐
E9	Le contrat précise explicitement ce qui est hors périmètre TMA	Élevé	☐

Interprétation : tous les points 'Critique' doivent être au vert pour considérer la maintenance comme suffisante. Les points 'Élevé' doivent être couverts dans les 30 jours. Les points 'Moyen' constituent les bonnes pratiques à viser.

Synthèse — Les 4 piliers d'une maintenance réussie

[1] Sécurité active Patcher, auditer, protéger en continu	[2] Prévention Anticiper avant que ça casse	[3] Visibilité Monitoring + reporting = confiance client	[4] Organisation Tickets, SLA, documentation = pérennité
--	--	---	--

Une maintenance bien structurée n'est pas un centre de coût pour le client : c'est une assurance. Elle préserve la valeur du projet, garantit la continuité d'activité et libère les équipes métier de l'anxiété technique.

Pour le prestataire, elle est le fondement d'une relation client durable : récurrente, prévisible et à haute valeur ajoutée. Un client en maintenance est un client qui reste.