fulll

Plan d’assurance sécurité

fulll.io

Ce document décrit les engagements pris par fulll en termes de sécurité des données et de ses applications hébergées sur sa plateforme cloud.

04/09/2026 - version 5.00

Sommaire

Notre histoire

L'histoire de fulll commence lorsque trois éditeurs de logiciels (Ibiza Software, In Extenso Digital et In Extenso Social) forts de leurs expériences respectives, décident de s'unir pour concevoir une solution innovante.

Leur vision commune était de créer un outil 100% web, spécialement conçu pour répondre aux besoins des experts-comptables dans leur production comptable, fiscale, sociale et collaborative.

En 2021, cette collaboration a donné naissance à fulll, marquant le début d'une nouvelle ère dans le domaine des logiciels de gestion.

La mission de fulll était claire : accompagner les experts-comptables dans la gestion de leur activité en leur fournissant des outils à la pointe de la technologie, agiles et évolutifs.

Ces outils devaient non seulement simplifier la collaboration avec leurs clients, les TPE et PME, mais aussi soutenir les cabinets dans l'implémentation de leurs méthodes de travail.

Fulll dispose d'une équipe d'environ 270 personnes, composée de personnel permanent et assure principalement les activités suivantes :

- La gestion de produit / R&D
- L'hébergement et le maintien en condition opérationnelle de ses applications
- Le support applicatif
- La rédaction de la documentation d'exploitation
- La formation des utilisateurs

Notre vision

Les informations des clients et les systèmes d'information qui permettent de les traiter constituent une part essentielle du patrimoine de fulll.

Ces systèmes d'information sont exposés à de multiples menaces pouvant porter atteinte à son activité ou à celle de ses clients. Ces menaces évoluent en permanence.

L'exposition et la complexité des systèmes d'information ainsi que leur interdépendance ne font que croître, dans un environnement ouvert, évolutif et flexible, un contexte de développement de services nouveaux, d'accès à des volumes de données croissants et des modes de restitution en évolution.

La sécurité de l'application et des données est donc d'une importance stratégique.

Fulll est certifiée ISO 27001, norme de référence internationale en matière de système de management de la sécurité de l'information.

Fulll est également certifiée ISO 27701, qui est une extension de la norme ISO 27001 spécifiquement axée sur la protection des données personnelles et de la vie privée. Cette norme fournit des lignes directrices pour la mise en place d'un système de management de la protection de la vie privée (PIMS) dans le cadre de la gestion des risques liés au traitement des données personnelles.

Les certificats, respectivement IS 672984 et PM 815300, ont été délivrés par BSI.

Fulll s'est engagée à garantir la confidentialité, l'intégrité et la disponibilité des informations de ses clients et à protéger leurs données et leur vie privée.

Cet engagement est reconduit chaque année.

Notre solution

Fulll, c'est une application complète avec des modules collaboratifs à la carte, évolutifs et puissants qui interagissent ensemble.

PRODUCTION COMPTABLE

Collecte, révision, saisie, liasses et tableaux de bord

PRODUCTION SOCIALE

Gestion des paies et du déclaratif optimisées

GESTION INTERNE

Des outils collaboratifs qui simplifient la gestion des obligations réglementaires

OUTILS CONNECTÉS

Des outils 100% web qui simplifient la collaboration et gagner en productivité

Et des applications mobiles !

L'application est hébergée en France et en Allemagne, chez AWS.

AWS est un fournisseur de référence dans le domaine des services managés dans le cloud et dispose de nombreuses certifications en faveur de la sécurité de l'information :

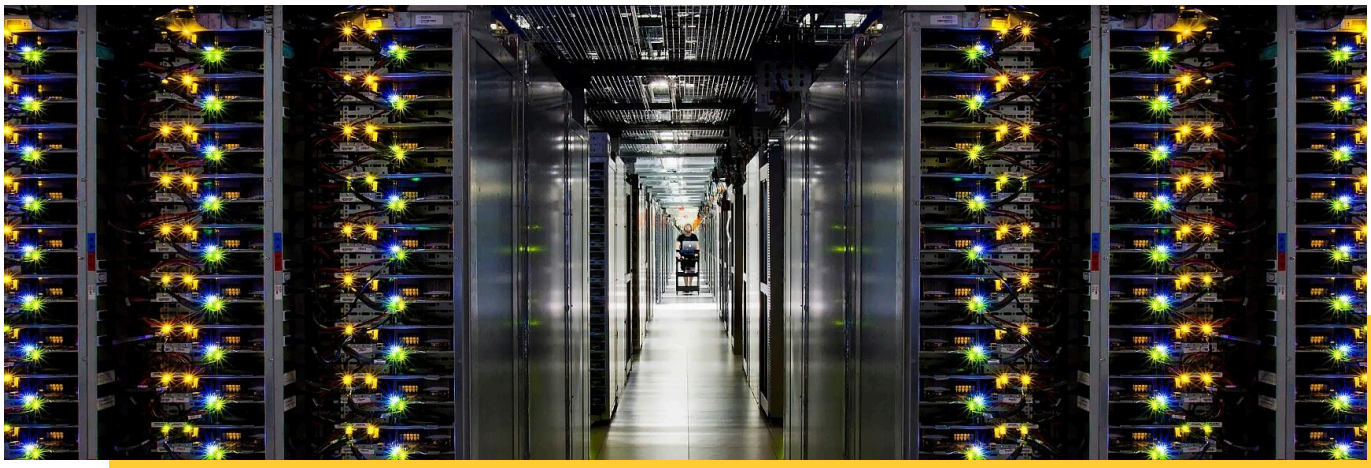
- ISO 27001
- ISO 27701
- ISO 27017
- ISO 27018
- SOC 1 / 2 / 3
- ...

Les datacenters maintenus par AWS disposent d'une conception intégrant comme fonction des systèmes hautement résilients, et donc la disponibilité des services.

Les datacenters AWS sont répartis sur 3 zones physiquement séparées de plusieurs kilomètres.

Grâce à l'utilisation des zones de disponibilité et de la réplication de données, les temps de récupération et de point de récupération sont extrêmement courts, ainsi que les niveaux les plus élevés de disponibilité des services.

L'application peut s'interconnecter avec des services tiers.



Plateforme Agréée - Facture électronique

La plateforme est enregistrée auprès de la Direction Générale des Finances Publiques (DGFiP) comme Plateforme Agréée.

Les Plateformes Agréées sont soumises à un cadre d'audit et de surveillance strict encadré par décrets, sous le contrôle de la DGFiP :

- **Tests d'interopérabilité et de raccordement** au Portail Public de Facturation (PPF) et à l'annuaire central ;
- **Audits de conformité** (initial et surveillance périodique) réalisés par un organisme indépendant ;
- **Surveillance continue du Service d'Immatriculation des Plateformes** (SIM), qui dispose d'un droit de contrôle et d'un pouvoir de sanction pouvant aller jusqu'à des amendes ou le retrait immédiat du numéro d'immatriculation en cas de manquements.

Pour la réalisation des audits de conformité, fulll a contractualisé avec INFOCERT, organisme d'audit indépendant et le secrétariat technique d'AFNOR Certification spécialisé dans les logiciels et les systèmes d'information.

Conservation à valeur probante des documents

Les documents sont conservés dans un coffre-fort numérique à valeur probante dont le dispositif technique est certifié AFNOR NF203 CCFN (Composant Coffre-Fort Numérique).

Cette norme atteste qu'il respecte les exigences légales et techniques d'un coffre-fort numérique et constitue la preuve formelle de conformité aux réglementations françaises sur le stockage numérique sécurisé et l'archivage à valeur probante.

Les documents archivés peuvent ainsi être produits et invoqués comme preuve, conformément au Code civil et au décret n°2016-1673.

Ingénierie de la sécurité des systèmes

La sécurité est considérée par les équipes techniques de fulll en charge de l'infrastructure selon des principes d'efficacité reconnue.

Ce chapitre décrit les principes de sécurités standards qui sont considérés dès la phase de conception.

Défense en profondeur

Le principe de défense en profondeur part du postulat qu'une seule défense ne peut pas faire face à toutes les menaces et qu'il est plus efficace d'accumuler des barrières de protection entre l'assaillant et l'objet à protéger.

Le nombre de barrières devant être en rapport avec la valeur de la ressource à protéger.

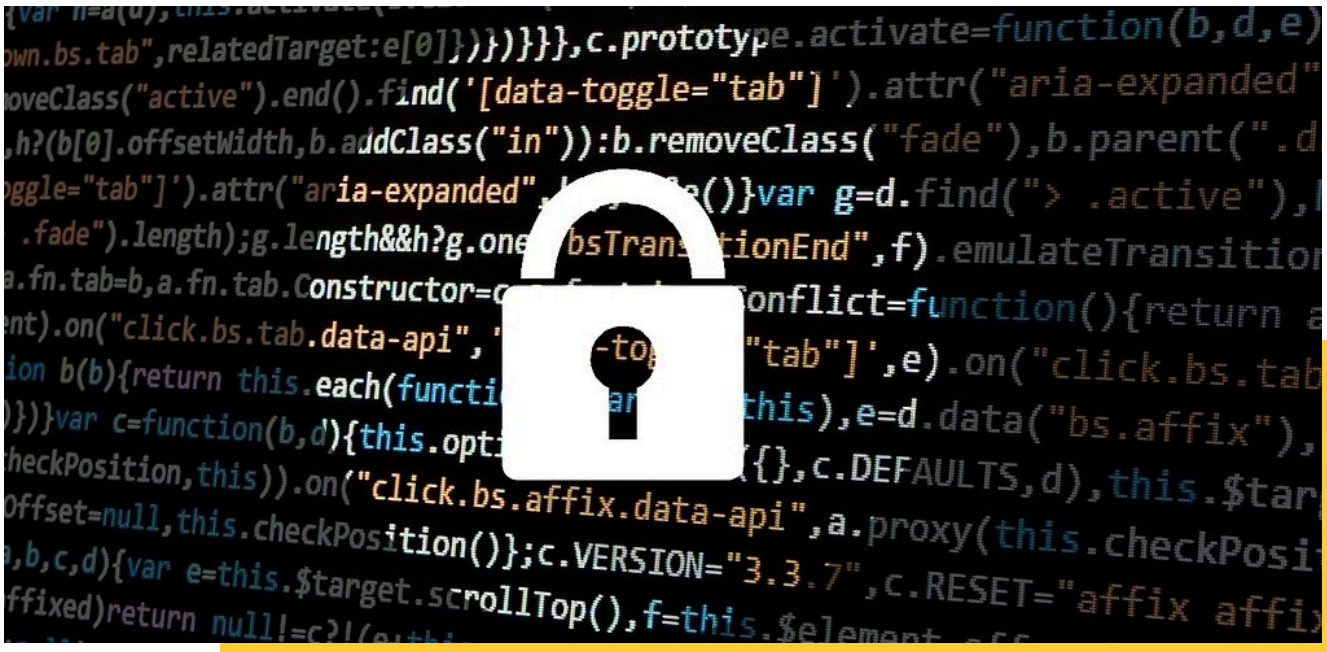
Les barrières de sécurité mises en œuvre sont de plusieurs natures :

- Humaines
- Technologiques
- Opérationnelles

Angle fonctionnel

L'accès utilisateur à l'application est basé sur une authentification préalable, aucune opération ne peut être effectuée sans cette authentification.

Chaque utilisateur ne peut accéder qu'aux fonctions et aux données auxquelles il a strictement besoin.



Angle données

Les données peuvent être confidentielles ou personnelles, elles sont séparées de la partie application, en s'appuyant autant que possible sur des SGBD standards.

L'accès aux données par un autre mécanisme que l'application est réservé aux tâches d'administration, par le personnel fulll habilité.

Les mécanismes de mise en production permettent le changement du code de l'application indépendamment de la mise à jour des données.

Selon leur nature, les données sont sauvegardées selon une politique formelle.

Angle applicatif

Les modules de l'application fulll permettent la connexion des utilisateurs en protégeant leurs informations d'authentification, en se basant sur des protocoles chiffrement autorisés.

Le code source est non modifiable par l'utilisateur.

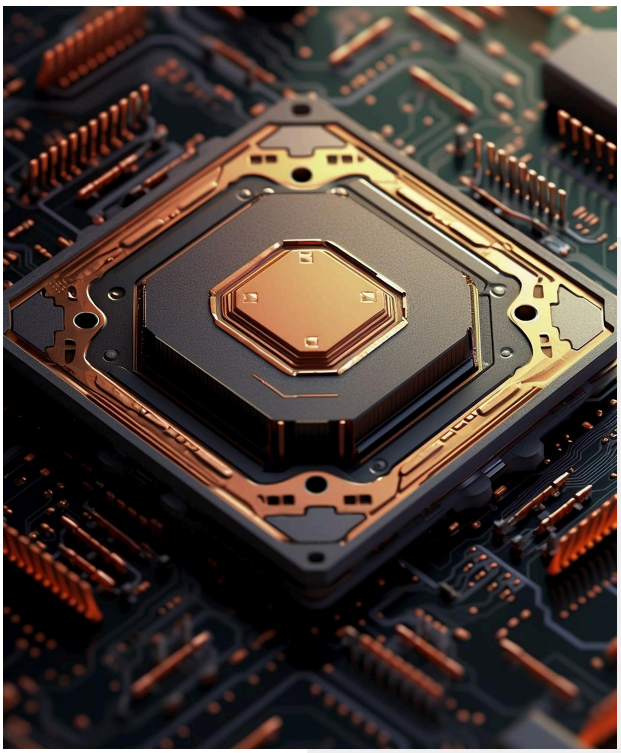
Les paramètres de configuration sont accessibles uniquement aux administrateurs concernés.

Les journaux de débogage sont accessibles qu'au personnel fulll habilité.

Angle technologies

Fulll veille à concevoir des applications qui s'appuient sur des technologies reconnues, maintenables et offrant la résilience requise.

Les services et solutions technologiques choisies sont validés par la direction technique.



Les politiques de sécurité

Fulll a formalisé ses politiques de sécurité.

Ces documents ne sont pas en accès public et leur diffusion nécessite l'accord préalable de la direction de fulll. Ce chapitre résume une partie de ces politiques.

Politique générale de sécurité de l'information

En matière de sécurité, l'objectif de fulll est d'assurer la disponibilité, la confidentialité et l'intégrité des applications et des informations qu'elles contiennent sur les systèmes d'information qu'elle met en œuvre pour ses clients.

Pour atteindre cet objectif, plusieurs grands principes de sécurité sont définis pour lutter contre les menaces pesant sur les systèmes d'information, en tenant compte des activités et des enjeux.

Ces principes sont guidés par les exigences et les bonnes pratiques définies dans les normes relatives à la sécurité de l'information.

Ces principes sont :

- Instaurer une culture de la sécurité et de la protection de la vie privée
- Maîtriser les actifs, les traitements et le cycle de vie des données
- Suivre le niveau de sécurité du système d'information et de la protection des données personnelles
- Garantir la conformité légale et le respect des droits des personnes
- Faire contribuer les fournisseurs et les prestataires à la sécurité du système d'information
- Rationaliser les solutions et les coûts

Organisation de la sécurité

La direction de fulll est fortement engagée dans la sécurité de l'information.

Un RSSI et un service dédié ont la charge de maintenir et de faire évoluer le Système de Management de la Sécurité de l'Information (SMSI), avec l'appui de la direction et des managers.

Les politiques de sécurité sont revues une fois par an.

La stratégie de la sécurité de l'information est pilotée à minima annuellement, lors d'une revue de direction dédiée.

Au niveau opérationnel, des revues et contrôles sont effectués mensuellement, selon un programme défini et validé par la direction de fulll.

Le SMSI est audité deux fois par an, par un prestataire externe et par un organisme certificateur (BSI).

Gestion des risques

Une analyse de risques est réalisée selon le catalogue EBIOS de menaces et une méthodologie formalisée.

Elle est revue à minima annuellement et donne lieu à de nouveaux plans d'actions, favorisant ainsi l'amélioration continue.

Sécurité dans les ressources humaines

Fulll s'appuie sur une équipe permanente de collaborateurs qualifiés et engagés.

Chaque salarié est doté d'une fiche de poste qui décrit ses missions, son positionnement au sein de l'organisation, ses principales activités, et les savoir-faire et savoir-être qu'il doit maîtriser pour mener à bien ses missions. Cela inclut sa participation à la sécurité de l'information.

Tous les contrats de travail incluent des clauses de confidentialité et de secret professionnel.

Chaque nouveau collaborateur suit une formation interne de sensibilisation à la sécurité et à la protection des données personnelles (RGPD) dispensée par l'équipe sécurité.

Des processus formels encadrent l'arrivée et le départ de collaborateurs, incluant l'affectation et la restitution d'actifs et d'accès logiques.

Fulll peut faire appel à des prestataires, notamment pour renforcer ses équipes de développement.

Ces prestataires ont des accès très limités et contrôlés, ils sont également sensibilisés à la sécurité et à la protection des données personnelles et ne peuvent accéder aux données clients sans l'accord formel de la direction.

Gestion des actifs

Tous les actifs constituant la plateforme et ceux des collaborateurs fulll sont identifiés et répertoriés. Des inventaires sont effectués régulièrement par l'équipe sécurité.

Les supports amovibles tels que les clés USB sont limités et encadrés.

La mise au rebut / destruction est contrôlée par un processus formel, sous la responsabilité de la direction technique.

Les dispositifs de stockage des informations client sont classés comme critiques et sont traités comme des éléments à fort impact tout au long de leur cycle de vie.

Pour exemple, les dispositifs de stockage sont mis hors service par AWS selon les techniques définies dans la spécification NIST 800-88.

Gestions des accès logiques

Fulll applique le principe du juste besoin.

Les accès aux systèmes d'information et aux données clients sont limités et contrôlés.

Les demandes d'accès suivent un processus formel et doivent être validées par la direction fulll lorsqu'elles concernent des éléments du système d'information contenant des informations client.

Les droits d'accès aux données clients et aux éléments de l'infrastructure sont contrôlés régulièrement.

Fulll dispose d'une politique de gestion des mots de passe, précisant les règles de stockage, d'utilisation de comptes nominatifs et favorisant autant que possible les mécanismes de double d'authentification.

Les modules de l'application fulll utilisent un mécanisme d'authentification pour effectuer toutes les actions sur le système. L'authentification renvoie un ensemble de droits pour un utilisateur donné limitant ses actions possibles par l'application.

Cryptographie et sécurité des télécommunications

Les échanges entre les modules et les postes clients s'effectuent via HTTPS/TLS 1.2 et utilisent des mécanismes d'authentification, sous forme de token à durée de vie limitée dans le temps.

Les échanges avec les API tierces sont également sécurisés (token, HTTPS/TLS 1.2).

Les bases de données de la plateforme sont chiffrées, utilisant notamment l'algorithme de chiffrement AES-256 standard.

Les documents client sont stockés sur des dispositifs chiffrés (chiffrement AWS SSE-KMS).

La gestion des clés de chiffrement de la plateforme est encadrée par la direction technique de fulll.

Fulll met en œuvre des réseaux VPN cloisonnés pour accéder aux éléments de la plateforme, à des fins de maintenance.

Les stations de travail des collaborateurs et les réseaux internes WiFi sont également chiffrés.

Sécurité physique et environnementale

Fulll dispose de systèmes de sécurité anti-intrusion, anti-incendie et d'un accès internet redondé pour ses propres locaux.

Les données clients d'exploitation sont hébergées dans les datacenters d'AWS.

Les datacenters AWS sont conçus de façon à anticiper les pannes et à y résister, tout en maintenant des niveaux de service optimaux.

Les défaillances matérielles sont détectées par AWS, qui réagit selon ses procédures internes.

Si des services critiques sont impactés, fulll est alertée par emails/système de notifications rapides.

Les datacenters sont dotés d'équipements de détection et d'extinction automatiques des incendies.

Les systèmes d'alimentation électrique des datacenters sont conçus pour être totalement redondants et gérables sans que cela ait une quelconque incidence sur les opérations, 24h/24.

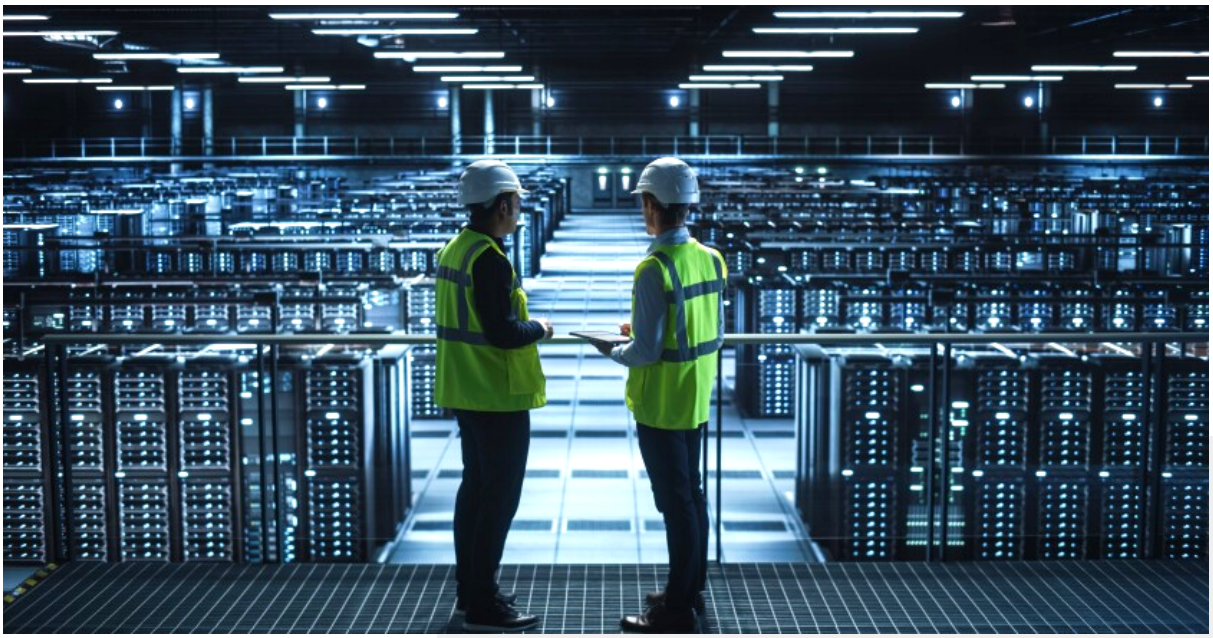
Les infrastructures d'AWS reposent sur des régions et des zones de disponibilité.

Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance.

En cas de défaillance, le trafic des données est réacheminé automatiquement.

AWS a identifié des composants système critiques nécessaires au maintien de la disponibilité de ses systèmes et son service de récupération en cas de panne.

Les composants système critiques sont sauvegardés sur plusieurs emplacements isolés, appelés zones de disponibilité.



Sécurité liée à l'exploitation

Supervision et journalisation

Les équipements et l'application sont respectivement supervisés par les équipes AWS et par l'équipe technique de fulll.

Les membres du service support de fulll peuvent également alerter en cas d'anomalie constatée par les utilisateurs.

L'équipe technique de fulll dispose d'outils de journalisation permettant des analyses en profondeur.

Cette journalisation suit une politique formelle et tient compte des exigences légales en la matière.

L'accès aux journaux est limité et encadré.

Dimensionnement

La plateforme profite des fonctions de scalabilité offertes par AWS.

Ceci permet de dimensionner automatiquement, en fonction de la charge ou sur période, les éléments d'infrastructure sollicités. Cela concerne également les capacités des dispositifs de stockage.

Le redimensionnement est effectué à la volée, sans interruption sur la plupart des services.

Le bon dimensionnement des éléments est surveillé par l'équipe technique de fulll, grâce aux fonctions de monitoring et d'alarme sur seuil proposées par les services et les outils mis à disposition par AWS.

Gestion des mises à jour

La gestion des mises à jour suit une politique formelle de gestion des changements.

Celle-ci couvre les mises à jour des systèmes, les mises à jour de sécurité et les mises à jour de l'application.

Des environnements dédiés au développement et aux tests permettent la validation des mises à jour avant leur mise en production. Les tests sont réalisés par les équipes qualité sous la responsabilité des chefs de produit.

Les mises à jour sont automatisées (*continuous delivery*), autant que possible, afin de limiter le risque d'erreurs humaines et soumises à des restrictions d'accès.

Les mises à jour majeures, entraînant une potentielle interruption de service, sont effectuées en dehors des horaires d'exploitation et après une communication préalable auprès des utilisateurs.

Fulll veille toujours à garder la possibilité de retour en arrière (*rollback*) suite à la défaillance d'une de ses applications.

Gestion des vulnérabilités

La plateforme dispose de protections telles que le cloisonnement, les pare-feux, filtrage IP et systèmes de détection d'intrusion.

Les stations de travail des collaborateurs disposent d'un antivirus à jour et d'un système de détection de code malveillant.

Afin de prévenir les vulnérabilités :

- Une veille est réalisée afin de maintenir les systèmes d'exploitation et les applications des stations de travail.
- Le processus de développement des applications de fulll tient également compte de la mise à jour des codes/librairies tierces.

Audits techniques de sécurité

Fulll effectue annuellement un audit technique de sécurité (*pentest*).

Les résultats de cet audit sont portés à la connaissance de la direction, qui valide, s'il y a lieu, des plans d'actions menés par la direction technique.

Le RSSI est systématiquement informé des constats et suit l'avancement des plans d'actions.

Sauvegardes

Les données clients sont sauvegardées à minima une fois par jour, en dehors des horaires d'exploitation et de façon automatique.

Les archives de sauvegarde sont stockées en Union Européenne, dans une localité distante de l'infrastructure d'exploitation.

Les sauvegardes sont conservées pendant deux semaines à minima. Leur accès est protégé et limité à la direction et à la direction technique.

Aussi, le code sources des applications et les éléments d'infrastructure de la plateforme sont versionnés et disposent de leur propre plan de sauvegarde.

Les sauvegardes sont contrôlées périodiquement par l'équipe technique, selon un programme validé par la direction de fulll.

Rétention

Les données clients sont conservées à minima 10 ans, durant l'exécution du contrat.

Les données sont supprimées 3 mois après la résiliation effective du contrat par le cabinet.

Utilisation des données clients

Le client reste le seul propriétaire de ses données.

Les données ne sont pas cédées par fulll sans le consentement du client.

Fulll peut toutefois être amenée à utiliser ces données pour :

- La résolution d'anomalies remontées par le client ;
- L'amélioration de ses applications, dans le cadre de demandes d'évolution émises par le client.

Fulll s'efforce d'utiliser autant que possible des fausses données et des données anonymisées aux fins de test de ses applications.

Politique de développement sécurisé

Fulll utilise des méthodes et outils dits agiles et s'efforce d'inclure dans ses applications les concepts de *security by design* et *privacy by design*.

Fulll a formalisé une politique de développement sécurisé et des standards de bonnes pratiques qu'elle met à disposition de l'ensemble de ses développeurs, chefs de produits et de ses prestataires.

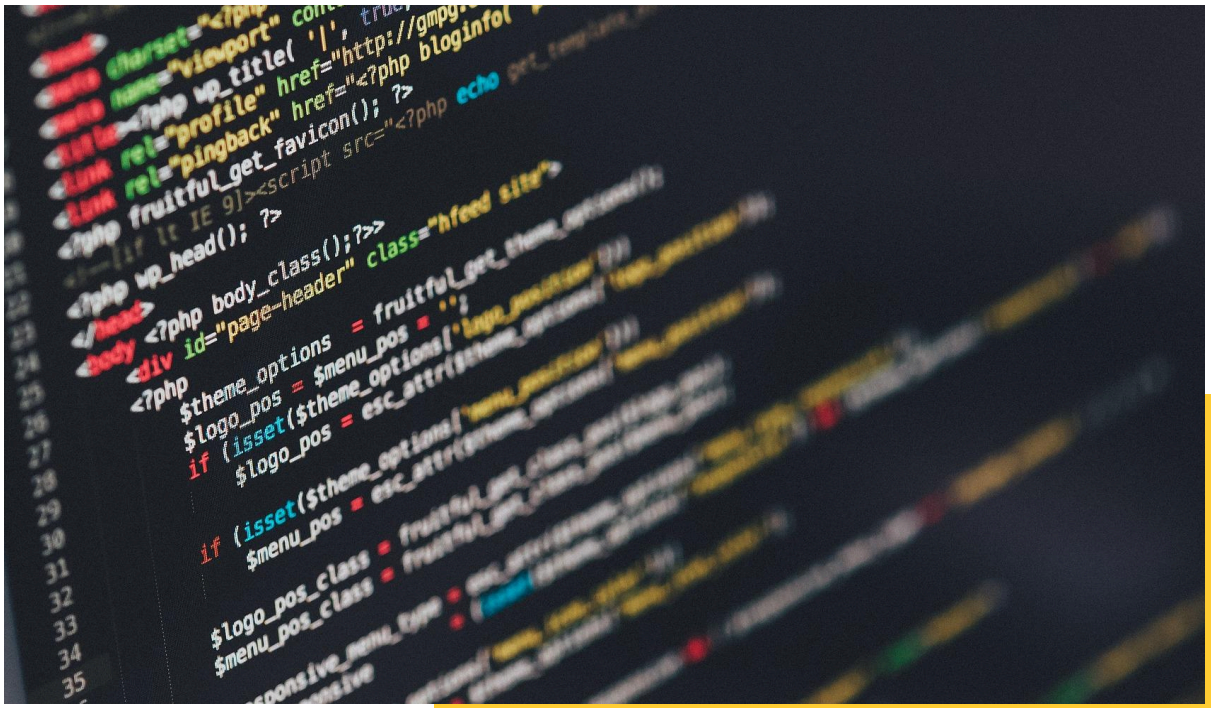
Le standard de bonnes pratiques tient compte notamment du top 10 OWASP, de l'état de l'art, des codes et outils déjà mis en œuvre par fulll.

Le code source des applications est protégé contre les changements et toute évolution doit faire l'objet d'une expression formelle du besoin, sous la responsabilité des chefs de produit.

Des outils permettent de vérifier automatiquement le code source et de garantir la qualité des changements réalisés.

Le code source est versionné et géré par un des outils de référence du marché. Son accès est limité et contrôlé.

Des environnements dédiés aux développements et aux tests sont mis en œuvre et sont séparés de l'environnement de production.



Relation avec les fournisseurs

La relation avec les fournisseurs est gérée par la direction de fulll, selon une politique formelle.

Les contrats avec les fournisseurs contiennent des clauses de sécurité, en fonction du niveau de risque.

Une revue des fournisseurs est effectuée chaque année par l'équipe sécurité.

Gestion des incidents de sécurité

Fulll a formalisé sa politique de gestion des incidents de sécurité, définissant l'organisation et la gestion de la crise. La direction et l'ensemble des collaborateurs de fulll sont impliqués dans cette gestion.

Dans les cas les plus graves, des analyses d'incident sont réalisées par le RSSI et validées par la direction. Elles conduisent à des plans d'actions visant à éliminer, dans la mesure du possible, les causes racines de l'incident.

Une politique de relation avec les autorités et groupes de travail spécialisés est formalisée.

Elle tient compte notamment des exigences légales de déclaration des incidents de sécurité.

Gestion de la continuité d'activité

Fulll dispose d'un Plan de Reprise et de Continuité d'Activité (PRA/PCA).

Ce document décrit l'organisation de la cellule de crise, autour de la direction de fulll avec tous les acteurs nécessaires à la remédiation.

Ce document fait également état des mesures préventives, des éléments de redondances en couvrant les éléments de l'infrastructure et les processus de fulll.

Les scenarii envisagés de crise concernent les moyens matériels et humains : destruction de datacenters, indisponibilité totale des locaux de fulll, pandémie, etc.

Le PRA/PCA est mis à jour annuellement ou sur événement.

Des tests de scénario sont réalisés chaque année, selon le plan de revues validé par la direction de fulll.

A noter qu'AWS dispose de son propre PRA/PCA.

Gestion de la conformité

Toutes les politiques de sécurité sont revues annuellement, sous la responsabilité du RSSI, et validées par la direction de fulll.

La conformité du système de management de la sécurité de l'information est contrôlée annuellement par BSI, organisme certificateur ISO 27001 et ISO 27701.

Fulll a mis en place une structure interne dédiée à la conformité réglementaire et à la protection des données personnelles. Cette structure est chargée de :

- Assurer une veille juridique constante sur les évolutions des lois et réglementations applicables, notamment le RGPD, la loi Informatique et Libertés, et les directives pertinentes.
- Analyser et interpréter les exigences légales et réglementaires pour les traduire en spécifications techniques et organisationnelles concrètes.
- Communiquer de manière proactive et régulière avec les équipes de développement et d'exploitation de la plateforme pour garantir l'intégration des exigences de conformité dès la conception (*Privacy by Design*).
- Effectuer des audits internes réguliers pour vérifier la conformité de l'application aux normes en vigueur.

Cette approche intégrée permet à fulll de maintenir un niveau élevé de conformité, tout en adaptant continuellement ses pratiques aux évolutions réglementaires.

La transmission systématique des exigences à l'équipe de développement de la plateforme garantit que la conformité est intégrée à chaque étape du cycle de vie des applications.

En complément des mesures générales de sécurité, fulll met en œuvre des actions spécifiques pour la protection des données personnelles :

Minimisation des données

- Collecte et traitement limités aux données strictement nécessaires aux finalités déclarées
- Mise en place de procédures d'anonymisation des données autant que possible

Gestion des droits des personnes concernées

- Procédure documentée pour répondre aux demandes d'exercice des droits (accès, rectification, effacement, portabilité)
- Ces droits peuvent être exercés par mail à dpo@fulll.fr ou par courrier postal envoyé au siège social, à l'adresse suivante : 14 rue Rhin et Danube 69009 LYON, en justifiant de son identité
- DPO nommé au sein de l'équipe Sécurité et déclaré à la CNIL

Gestion des incidents

- Procédure spécifique de notification des violations de données personnelles
- Tenue d'un registre des incidents de sécurité impliquant des données personnelles

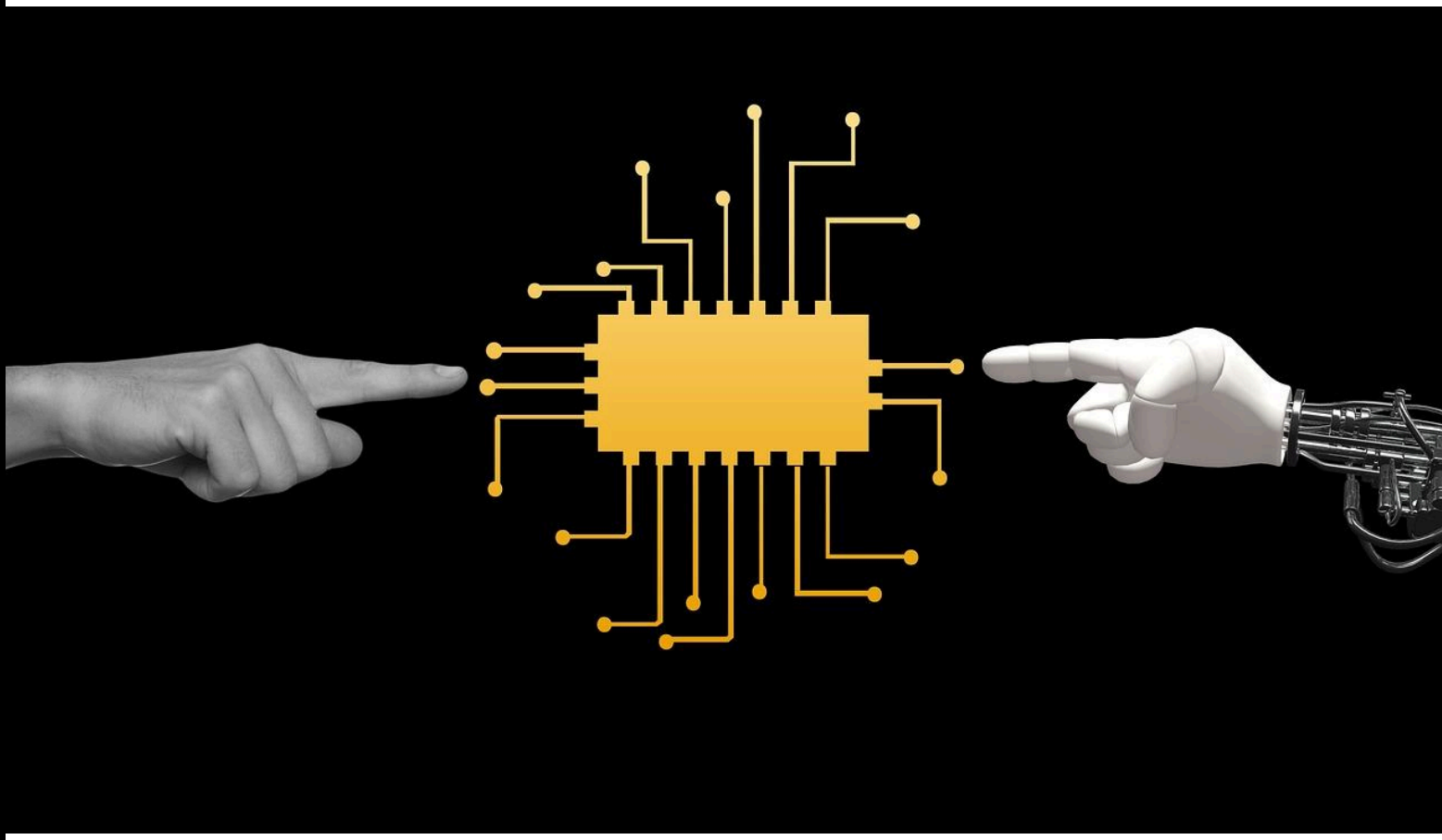
Formation et sensibilisation

- Programme de formation continue sur la protection des données pour tous les employés
- Sensibilisation régulière aux bonnes pratiques de sécurité et de confidentialité

Évaluation et amélioration

- Analyses d'impact relatives à la protection des données (AIPD) pour les traitements à risque
- Revue annuelle des mesures de protection des données personnelles et mise à jour du registre des traitements

Ces mesures sont régulièrement évaluées et ajustées pour garantir un niveau de protection optimal des données personnelles, conformément aux exigences réglementaires et aux meilleures pratiques du secteur.



Disclaimer