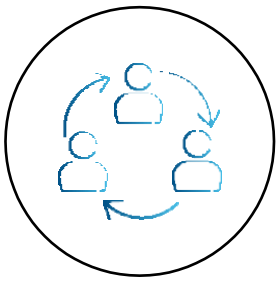
Guide de Survie de la Sécurité informatique pour les entreprises

MISTER-IT.IO

Sommaire



L'humain, l'humain et l'humain

Il est aujourd'hui très facile de mettre en danger la sécurité informatique de son entreprise, et tous les pirates informatiques le savent. Conséquence, l'ingénierie sociale est devenue l'une des principales menaces qui planent au-dessus des entreprises, PME comme multinationales.

Cette pratique vise à s'introduire dans le système informatique de l'entreprise via les postes de travail des utilisateurs, qui sont de fait à l'origine de la majorité des incidents informatiques dans les entreprises.

Il en va donc de la survie des entreprises d'investir aujourd'hui dans leur premier rempart de sécurité : leurs utilisateurs. Sécuriser son entreprise en ne sécurisant que son serveur, n'est plus qu'un lointain souvenir. La priorité est à la formation des utilisateurs et à la sécurisation des postes de travail.

Certains verront à travers ce guide des évidences, des basiques théoriquement maîtrisés, pourtant l'actualité nous le rappelle tous les jours : **il n'a jamais été aussi important qu'aujourd'hui de revenir sur les bases de la sécurité informatique.**

Nous le constatons chaque jour sur le terrain, **l'informatique et ses usages évoluent constamment, et souvent trop rapidement pour les TPE et PME**, qui peinent à s'adapter à la situation en matière de sécurité.

Nous espérons donc que ce guide puisse servir, aussi bien aux plus compétents, comme mémo pour nourrir vos supports de formation, qu'aux moins avertis comme guide pratique vers une meilleure sécurisation de votre informatique.

Bonne lecture.

L'équipe Mister-IT

Les acteurs de la sécurité informatique en entreprise

Contrairement à ce que l'on pourrait croire, les acteurs de la sécurité informatique en entreprise ne sont pas toujours des informaticiens chevronnés. Voici le portrait rapide de deux types de publics bien différents, mais au rôle tout aussi important. Nous y ferons référence tout au long de ce guide.

Le service informatique

Lien entre le système d'information, les utilisateurs et les prestataires techniques, le service informatique d'une PME joue généralement les rôles-clés de « référent technique » et de « fluidificateur » au sein de son entreprise. **Sa mission est à minima de garantir le bon fonctionnement du système informatique et ses évolutions, en faisant en sorte que les collaborateurs soient les moins contrariés possible par leur outil de travail.** Dans une PME, le service informatique est souvent composé…d'une seule personne, qui occupe le rôle de « responsable informatique » parfois à temps partiel et parfois même sans être du métier.

Les utilisateurs

Les utilisateurs constituent l'ensemble du personnel de l'entreprise, ayant accès à un poste de travail informatisé. Via leur poste de travail les utilisateurs sont connectés au système informatique, qu'ils sollicitent quotidiennement pour effectuer les nombreuses tâches liées à leur fonction. **Ils sont à la fois la principale source d'incidents informatiques, et le premier rempart entre l'entreprise et les cyberattaques.**

#1 Ne négliger aucune mise à jour

De nouvelles failles de sécurité sont découvertes tous les jours

S'il y a encore quelques années, il suffisait de sécuriser son serveur pour sécuriser l'informatique de son entreprise, ce temps est désormais révolu. De nouvelles attaques et failles de sécurité apparaissent chaque jour, et demandent une vigilance accrue de la part des équipes informatiques. Des mises à jour sont d'ailleurs régulièrement proposées par les éditeurs et fabricants, pour corriger ces failles. Pourtant, un très grand nombre d'entreprises restent aujourd'hui équipées de systèmes d'exploitation obsolètes (aussi bien côté utilisateur que côté serveur) et/ou de logiciels ou d'équipements mobiles non mis à jour. Une aubaine pour les cybercriminels.

Les risques

L'obsolescence d'un système d'information ou un système d'information non mis à jour, expose davantage une entreprise aux failles de sécurité, de plus en plus dangereuses. Cela augmente considérablement les risques de dysfonctionnement de l'entreprise et menace donc directement la santé de l'activité.

Qui est concerné ?

● ● ● LE SERVICE INFORMATIQUE

● ○ ○ LES UTILISATEURS

Le maintien à jour du système d'information de l'entreprise, ainsi que de l'ensemble des logiciels et périphériques qui le compose, incombe généralement au service informatique. **Les utilisateurs doivent toutefois rester vigilants et signaler tout problème de version obsolète ou d'échec de mise à jour, à leur service informatique.**

#1 Ne négliger aucune mise à jour

Mesures préventives

1. Réalisez un inventaire des appareils et logiciels utilisés dans l'entreprise et **définissez précisément les règles de mises à jour pour chaque outil** ;
2. Vérifiez dès à présent que **l'ensemble de vos appareils et logiciels sont à jour,** et procédez à leur mise à jour si ce n'est pas le cas ;
3. **Faites une sauvegarde de vos données avant toute opération de mise à jour,** afin de pouvoir revenir en arrière en cas de problème de compatibilité entre certains équipements ;
4. **Profitez des périodes d'inactivité** pour réaliser d'éventuelles mises à jour ;
5. N'utilisez, si possible, que des appareils ou des logiciels bénéficiant d'un **support technique actif** et proposant des mises à jour régulières.

Notre avis

Bien sécuriser son serveur reste un prérequis pour protéger son entreprise et ses données, mais cela ne suffit plus. Aujourd'hui la **sécurisation des postes de travail** est également devenue obligatoire et passe impérativement par des mises à jour très régulières.

32%

Soit le pourcentage d'entreprises dans le monde, qui possèderaient encore au moins un terminal mobile équipé de Windows XP, dont la fin du support technique date de 2014. Tout aussi inquiétant, elles sont encore 79% à utiliser Windows 7 (contre 78% pour Windows 10) dont la fin du support est prévue pour le 14 janvier 2020. (Rapport 2019 « The Future of Network and Endpoint Security » de Spiceworks)

#2 Protéger et sauvegarder régulièrement ses données

Données non-protégées = attention danger

Plus une entreprise est informatisée, plus elle crée et gère des données numériques, potentiellement précieuses. Ces données peuvent même, dans certains secteurs d'activité, constituer la matière première de l'entreprise. Malheureusement, le stockage et la protection de ces données n'est très souvent pas à la hauteur de leur valeur. Le stockage unique sur un serveur interne non redondé, sur des disques durs externes ou pire sur un seul poste de travail, sont autant de mauvaises pratiques encore très répandues dans les entreprises. Pourtant les solutions de protection et de sauvegardes des données sont aujourd'hui nombreuses et de très bonne qualité.

Les risques

Une entreprise dont les données ne sont pas correctement protégées risque une perte de données irréversible, pouvant mener jusqu'à la faillite. Des causes diverses et variées peuvent être à l'origine d'une perte de données : **un virus de type ransomware, une simple erreur de manipulation ou un sinistre important comme un incendie ou une inondation.**

Qui est concerné ?

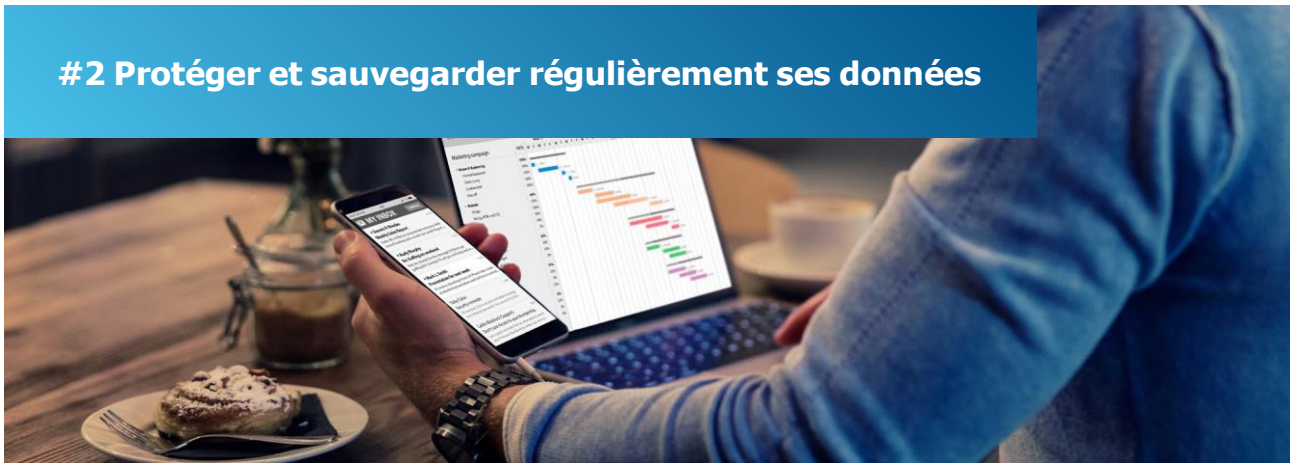
- LE SERVICE INFORMATIQUE
- LES UTILISATEURS

La protection des données doit être l'une des principales missions du service informatique de l'entreprise, que celui-ci soit composé de plusieurs ou d'une seule personne. De leur côté, les utilisateurs se doivent d'appliquer les consignes de stockage de l'entreprise, pour sécuriser toutes leurs données dans le plan de sauvegarde.

27%

Soit, en 2018, le pourcentage des entreprises mondiales qui ont rencontré une faille de sécurité entrainant une perte de données irréversible. (Selon l'étude « Global Data Protection Index », Dell et Vanson Bourne, 2018)

#2 Protéger et sauvegarder régulièrement ses données



Mesures préventives

1. Effectuez des sauvegardes **régulières, planifiées et contrôlées** de vos données ;
2. Equipez-vous d'une **solution de sauvegarde performante**, proposant si possible le chiffrement des données lors des transferts, plusieurs niveaux de rétention et une restauration instantanée en cas d'incident ;
3. Privilégiez les **sauvegardes hors du site de production** pour protéger vos données en cas de sinistre (incendie ou inondation) ;
4. Protégez également vos sauvegardes **en les multipliant** ;
5. **Réalisez un inventaire** des appareils et supports (disque dur, clé USB…) qui contiennent des données ;
6. **Mettez en place un PRA** (Plan de Reprise d'Activité) si vous pensez que votre activité supporterait difficilement une interruption d'activité.

Et le Cloud dans tout ça ?

L'intérêt de mettre en place des sauvegardes hors site de production est aujourd'hui admis par la plupart des DSI. Malheureusement, il est généralement trop coûteux et trop complexe pour des PME de se doter d'un site informatique déporté, dédié à son activité. C'est pourquoi **il existe aujourd'hui de nombreuses solutions de sauvegarde de données dans le Cloud, éprouvées, facile à mettre en œuvre, et qui permettent de répondre aux plus hautes exigences de transparence, de sécurité et de fiabilité.**

Notre avis

Il y a 10 ans déjà, 80% des entreprises qui perdaient leurs données informatiques faisaient faillite dans les 12 mois qui suivaient. Cette statistique reste plus que jamais d'actualité. Aujourd'hui encore, **la majorité des PME n'ont pas conscience de la valeur de leurs données**. Mal équipées en termes de sauvegarde et de sécurisation des datas, elles se mettent par conséquent en danger.

#3 Savoir identifier les attaques par messagerie

Méfiez-vous des apparences

Les emails et leurs pièces jointes ont toujours constitué des menaces potentielles pour l'informatique des entreprises, à travers des attaques de type « phishing » (pour « hameçonnage ») ou « ransomware » (pour « logiciel d'extorsion »). Ces attaques prennent très souvent la forme d'un message alarmant, provenant a priori d'une organisation ou d'une personne de confiance, qui vous invite à cliquer sur un lien et/ou à télécharger une pièce jointe. Cette technique de leurre incite à communiquer des données personnelles et/ou professionnelles (comptes d'accès, mots de passe…) dans l'objectif dans faire un usage frauduleux.

— Note : Il existe également des attaques de type « scam » (ou « Nigeria 419 » ou « fraude 419 »), dont le contenu de l'email propose généralement de gagner une importante somme d'argent, qu'un mystérieux et très riche étranger souhaiterait nous léguer.

Les risques

L'entreprise et l'utilisateur se retrouvent directement exposés au vol d'informations personnelles ou professionnelles (identifiants de connexions, mots de passe, données bancaires…), avec **compromission potentielle du système informatique.**

Qui est concerné ?

● ○ ○ **LE SERVICE INFORMATIQUE**

● ● ● **LES UTILISATEURS**

Le rôle du service informatique est ici d'informer et de former les utilisateurs à la bonne gestion de leur(s) messagerie(s), voire de mettre en place une solution de type anti-spam ou filtrage de contenus. **C'est ensuite et surtout à chaque utilisateur d'être vigilant sur la bonne utilisation de sa(ses) messagerie(s).**

#3 Savoir identifier les attaques par messagerie

Mesures préventives

1. Ne cliquez jamais sur un lien avant d'avoir **vérifié l'URL de destination** (en laissant votre souris dessus, le lien complet apparaitra) et soyez particulièrement vigilant aux noms de domaine de type « impots.gouvv.fr » ou « infocaf.org » au lieu de « www.caf.fr » par exemple. A noter que cette vérification est impossible à effectuer depuis un écran de smartphone. Dans ce cas, au moindre doute, abstenez-vous et transférez le message au service informatique ;
2. Vérifiez, en cas de clic, si l'URL du site correspond à celle sur laquelle vous avez cliqué et si **la connexion est sécurisée** (présence du cadenas en haut à gauche de votre navigateur) ;
3. Vérifiez si le mail que vous venez de recevoir **vous est réellement destiné** et qu'il n'évoque pas un dossier, une facture ou un sujet qui ne vous parle pas ;
4. Ne vous fiez pas automatiquement à **l'adresse de messagerie de l'expéditeur**, celle-ci pouvant être facilement usurpée ;
5. Soyez attentif au **niveau de langage et/ou aux fautes de frappe**, surtout si le message provient a priori d'un organisme crédible (banque, administration ...) ;
6. Méfiez-vous des **demandes « étranges » ou paraissant peu légitimes** (demande de code de carte bancaire ou de mot de passe), même si cela semble provenir d'une personne de votre entourage.

Notre avis

Selon plusieurs études, le taux de clic sur un email de type phishing serait compris entre 20 et 30%. C'est énorme. C'est pourquoi **le rôle du service informatique est plus que jamais d'assurer un travail de prévention et de formation des utilisateurs.**

52%

En 2018, le spam représentait encore 52,48 % du volume de courriers électroniques reçu dans une boîte email (Rapport 2018 « Spam & phishing » de Kaspersky). Si certains spams ne sont que de simples courriers publicitaires non sollicités mais inoffensifs, beaucoup d'entre eux sont des tentatives de phishing.

#4 Choisir des mots de passe sécurisés

Ne rendez pas la vie simple aux cybercriminels

Nous sommes tous quotidiennement amenés à nous connecter à un nombre toujours plus important de services numériques, via mot de passe. Malheureusement, devant cette profusion de mots de passe à gérer, il est extrêmement tentant de « faire simple », en choisissant des mots de passe peu sécurisés ou en utilisant le même mot de passe pour tous ses accès. Et à ce petit jeu, les entreprises ne sont pas forcément plus vigilantes que les particuliers.

Les risques

L'entreprise et l'utilisateur peuvent se retrouver directement exposés à l'usurpation de compte, d'identité ou au vol d'informations personnelles ou professionnelles (identifiants de connexions, mots de passe, données bancaires…), avec **compromission potentielle du système informatique.**

Qui est concerné ?

● ○ ○ **LE SERVICE INFORMATIQUE**

● ● ● **LES UTILISATEURS**

Le rôle du service informatique est ici d'informer et de former les utilisateurs à la bonne gestion de leurs mots de passe, et/ou de mettre en place des gestionnaires de mots de passe sur les postes de travail. C'est ensuite et surtout à chaque utilisateur d'être vigilant sur la création et sur la gestion de ses mots de passe.

Mesures préventives

1. Assurez prioritairement la sécurisation du **mot de passe de votre messagerie**, qui est généralement associée à la plupart de vos comptes en ligne ;
2. Choisissez des **mots de passe d'au moins 8 signes** mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux* ;
3. **Changez régulièrement** vos mots de passe les plus importants ;
4. Activez si possible la **double authentification**, procédé qui vous permet de confirmer que vous êtes bien la personne qui tente d'accéder au service ;
5. Evitez les connexions à vos comptes sensibles lorsque vous utilisez un ordinateur public/partagé, et **n'oubliez surtout pas de vous déconnecter en fin de session** ;
6. Utilisez un **mot de passe différent pour chaque plateforme**.

#4 Choisir des mots de passe sécurisés

Comment créer un mot de passe sécurisé ?

L'ANSSI recommande deux méthodes pour créer des mots de passe solides :

- **La méthode « des premières lettres » :** « Un tiens vaut mieux que deux tu l'auras » = 1tvmQ2tl'A
- **La méthode phonétique :** « J'ai acheté huit CD pour cent euros cet après-midi » = ght8CD%E7am

Néanmoins, ces méthodes nous semblent difficiles à appliquer. Plutôt que de chercher désespérément un mot de passe infaillible ET facile à mémoriser, **obligez-vous à mettre en place les mesures préventives ci-dessus.**

Les gestionnaires de mots de passe

Mémoriser des dizaines de mots de passe longs et complexes est impossible, c'est pourquoi il est aujourd'hui conseillé d'utiliser un gestionnaire de mot de passe sécurisé comme Keepass (recommandé par l'ANSSI) ou LockPass. Ces derniers vous permettront de ne retenir qu'un seul mot de passe…à changer régulièrement. Bien évidemment, **il est très fortement recommandé de ne jamais noter ses mots de passe sur un carnet papier, sur son smartphone ou dans un fichier non protégé** de son ordinateur.

123456

Soit le mot de passe le plus utilisé…et le plus piraté, depuis des années. (« Mots de passe les plus utilisés en 2018 : toujours la même rengaine », Les Numériques, 17/12/2018)

Notre avis

On se dit souvent « il faudrait vraiment que je change mes mots de passe » mais il est très rare que l'on prenne le temps de le faire, jusqu'au jour où…un piratage met en difficulté l'entreprise. **Prenez la mesure des enjeux et ne lésinez pas sur la sécurisation des accès à vos comptes.**

*L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) recommande même de choisir des mots de passe d'au moins 12 caractères dans un alphabet de 90 symboles ou d'au moins 16 caractères dans un alphabet de 36 symboles. (« Calculer la force d'un mot de passe », Site de l'ANSSI)

#5 Mettre en place une architecture sécurisée pour les travailleurs nomades

Faites rimer mobilité et sécurité

Grâce à Internet et aux performances des périphériques mobiles actuels (que ce soit en termes de puissance ou de portabilité), il est aujourd'hui très facile de travailler hors de l'entreprise, tout en ayant accès à ses données professionnelles à jour. Bien évidemment, travailler en « mode nomade » n'éloigne pas des menaces de sécurité et demande même une vigilance toute particulière. Malheureusement beaucoup d'entreprises se retrouvent dépassées par ces nouvelles pratiques et s'exposent aux attaques.

Les risques

Une entreprise mal protégée en situation mobilité, s'expose à des **vols ou à des pertes d'informations sensibles pouvant avoir de graves conséquences sur son activité.**

Qui est concerné ?

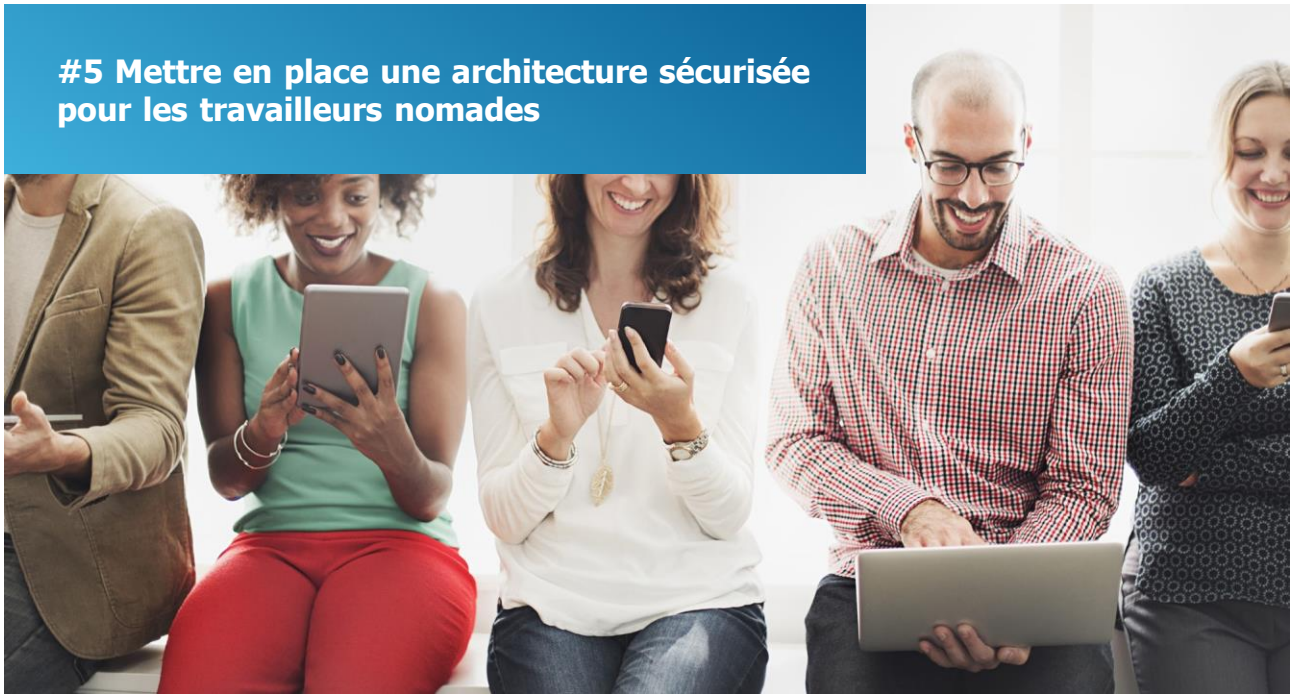
- **LE SERVICE INFORMATIQUE**
- **LES UTILISATEURS**

Le rôle du service informatique est ici d'informer et de former les utilisateurs aux bonnes pratiques du travail en mobilité, **en ayant préalablement sécurisé les appareils mobiles (ordinateurs, smartphones, ...) et les accès au système d'information.** C'est ensuite à chaque utilisateur d'être vigilant sur l'accès à ses données professionnelles en situation de mobilité, aussi bien en déplacement qu'à son domicile.

71%

Soit le pourcentage de personnes affirmant ne pas se préoccuper des questions de sécurité lorsqu'elles se connectent à un réseau Wi-Fi public. (Selon la dernière étude du cabinet américain Decision Data, 2019)

#5 Mettre en place une architecture sécurisée pour les travailleurs nomades



Mesures préventives

1. Maintenez votre poste de travail en permanence **à jour en termes de sécurité** ;
2. Activez les **options de chiffrement** de données de vos appareils ;
3. Disposez d'une **connexion VPN** pour accéder aux applications et données de l'entreprise en toute sécurité ;
4. Évitez de transporter des **données superflues**, notamment sur des clés USB, et n'utilisez que du matériel **dédié à la mission ;**
5. Evitez les connexions aux **réseaux Wi-Fi publics ou non protégés ;**
6. Ne stockez jamais de fichiers **uniquement sur le disque dur** de votre poste de travail.

Notre avis

Même si la mobilité peut être assimilé à plus de liberté, elle demande paradoxalement une vigilance accrue. Qu'il s'agisse de télétravail ou d'un déplacement, **le travailleur nomade devient seul responsable des données qu'il transporte.**

#6 Séparer les usages personnels et professionnels

En termes de sécurité, perso et pro ne font pas bon ménage

Avec le développement des technologies mobiles et connectées, la frontière entre la vie personnelle et la vie professionnelle n'a jamais été aussi poreuse. Il est aujourd'hui aussi facile de consulter ses données personnelles sur son lieu de travail, que d'accéder à ses données professionnelles depuis chez soi. Une tolérance s'est également installée dans certaines entreprises, concernant l'utilisation de matériels personnels pour effectuer des tâches professionnelles (ce que l'on appelle communément le BYOD pour « Bring Your Own Device »), sans pour autant que cette tolérance soit maîtrisée. Le problème est que les usages en matière de sécurité sont généralement beaucoup plus rigoureux dans la sphère pro que dans la sphère perso. Ce déséquilibre, en termes de vigilance, peut donc mettre l'entreprise en difficulté.

Les risques

Vol, perte ou fuite de données, risques d'intrusion au niveau du système d'information... les problèmes potentiels liés à la non-séparation des usages personnels et professionnels, sont nombreux pour l'entreprise.

Qui est concerné ?

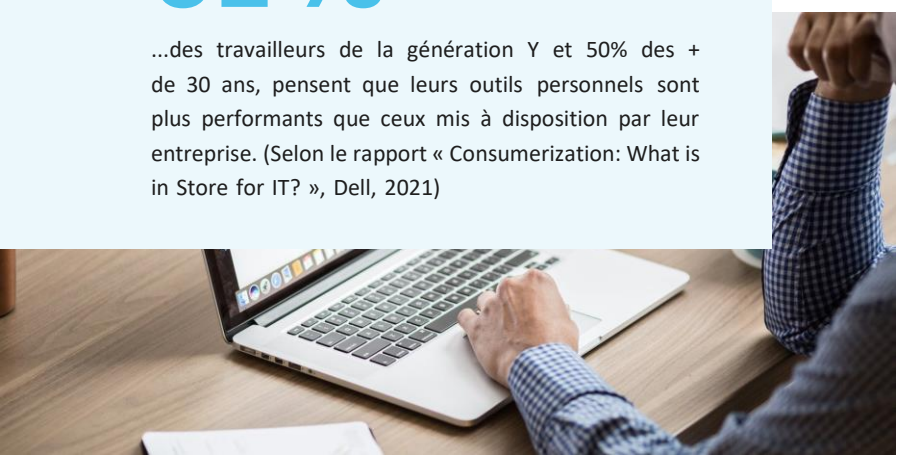
- LE SERVICE INFORMATIQUE
- LES UTILISATEURS

Le service informatique par l'intermédiaire de sa direction, doit être en mesure de **proposer du matériel suffisamment performant à ses utilisateurs pour, à la fois limiter les frustrations et également pour lui permettre de manager en tout sécurité son parc informatique*.** De leur côté, les utilisateurs doivent impérativement « jouer le jeu » en respectant rigoureusement les règles établies par le service informatique.

*Opter pour le CYOD (Choose Your Own Device) est aujourd'hui une alternative intéressante, permettant de satisfaire à la fois le service informatique et l'utilisateur.

61%

...des travailleurs de la génération Y et 50% des + de 30 ans, pensent que leurs outils personnels sont plus performants que ceux mis à disposition par leur entreprise. (Selon le rapport « Consumerization: What is in Store for IT? », Dell, 2021)



#6 Séparer les usages personnels et professionnels

Mesures préventives

Coté service informatique :

1. Limitez un maximum le recours au BYOD et privilégiez si possible le CYOD*, avec la mise à disposition d'un appareil sécurisé et administrable, pouvant être utilisé dans la sphère privée ;
2. Soyez toujours en mesure d'administrer l'ensemble des appareils connectés à votre système d'information ;

Coté utilisateurs :

3. Evitez de vous connecter au système d'information de votre entreprise via un appareil personnel ;
4. Ne faites jamais suivre vos emails professionnels sur des messageries personnelles ;
5. N'hébergez jamais de données professionnelles sur des équipements de stockage personnels et évitez de connecter des supports de stockage personnels aux ordinateurs de l'entreprise.

Et la RGPD dans tout ça ?

Avec le BYOD, faire la distinction entre les données privées et les données professionnelles est quasiment impossible. **Or la RGPD pose désormais la question de la conformité en plus de celle de la sécurité.** Selon la CNIL « L'employeur est responsable de la sécurité des données personnelles de son entreprise, y compris lorsqu'elles sont stockées sur des terminaux dont il n'a pas la maîtrise physique ou juridique… », de plus, toujours selon la CNIL « si l'employeur peut prévoir un effacement à distance de la partie du terminal personnel spécifiquement dédiée à l'accès distant aux ressources de l'entreprise, il ne peut en revanche s'arroger le droit d'effacer à distance l'ensemble des données présentes sur le terminal de l'employé ». **Si elle n'est pas en capacité d'administrer l'ensemble des appareils connectés à son SI, l'entreprise s'expose donc, en plus des risques de sécurité, à des risques juridiques.**

Notre avis

Les entreprises doivent aujourd'hui être en mesure de proposer une certaine liberté d'action à leurs utilisateurs, sans jamais perdre le contrôle de la sécurisation de leur SI. **Le BYOD est donc clairement déconseillé, sauf sur du très court terme et dans un cadre parfaitement maîtrisé.**

*Pour « Choose Your Own Device ». L'objectif est de permettre à l'utilisateur de choisir un périphérique à la fois adapté à ses besoins(sur catalogue) et sécurisé par le service informatique. Ce périphérique appartient à l'entreprise mais peut-être utilisé dans la sphère privée.

#7 Sécuriser l'accès à son réseau Wi-Fi

N'ouvrez pas la porte à n'importe qui

Largement répandu chez les particuliers, le Wi-Fi est également plébiscité par les entreprises pour sa commodité notamment en termes de mobilité, mais aussi pour les économies qu'il permet de réaliser par rapport la mise en place d'une infrastructure filaire. Toutefois, alors qu'il est souvent possible de procéder assez simplement à un paramétrage robuste et sécurisé d'un réseau Wi-Fi, leur sécurisation laisse souvent à désirer. Cela rend bien évidemment l'entreprise vulnérable aux attaques de personnes malveillantes.

Les risques

La compromission d'un réseau Wi-Fi peut permettre à des personnes malintentionnées d'**intercepter des données sensibles ou d'utiliser cette connexion Wi-Fi à l'insu de l'entreprise** pour réaliser des opérations malveillantes.

Qui est concerné ?

- ● ● ● LE SERVICE INFORMATIQUE
- ○ ○ ○ LES UTILISATEURS

La responsabilité de la sécurisation du Wi-Fi **incombe directement à l'entreprise** par l'intermédiaire de son équipe informatique.

#7 Sécuriser l'accès à son réseau Wi-Fi

Mesures préventives

1. Privilégiez, lorsque cela est possible, une **installation filaire, plus sécurisée et plus performante ;**
2. Mettez en place un **réseau Wi-Fi dédié aux personnes extérieures à l'entreprise,** et donc ne laissez aucune personne extérieure à l'entreprise se connecter au réseau Wi-Fi principal ;
3. Configurez votre réseau Wi-Fi avec le **mode de chiffrement robuste WPA2 couplé au mode d'authentification WPA-Entreprise**, dédié aux environnements professionnels ;
4. Définissez une **politique de sécurité** pour chaque réseau Wi-Fi de l'entreprise (« interne » et « invité » par exemple) ;
5. Mettez en place **un identifiant de connexion au réseau unique** pour chaque utilisateur ;
6. Vérifiez que tous les périphériques de l'entreprise, potentiellement connectés au réseau, **sont sécurisés ;**

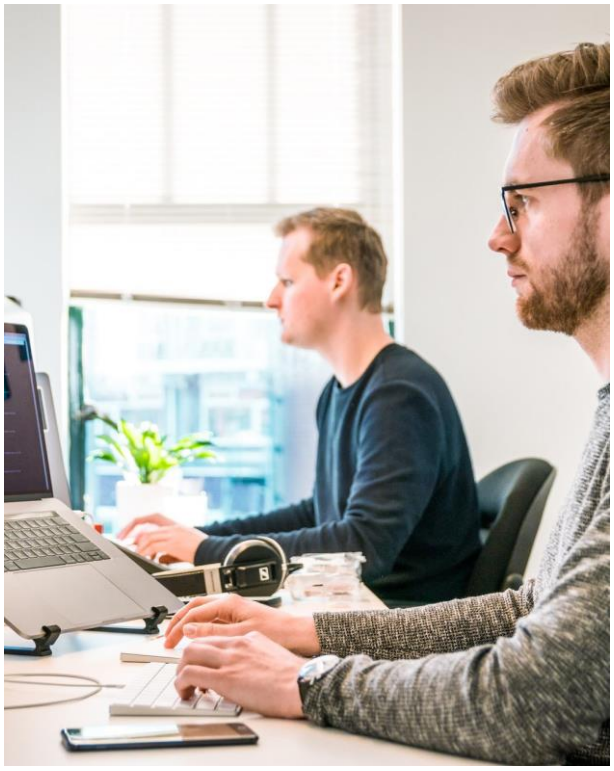
Notre avis

Cassons le mythe : **la mise en place d'un réseau Wi-Fi dans une entreprise n'est absolument pas une opération anodine.** Elle doit se dérouler dans un cadre extrêmement bien défini, selon vos objectifs de sécurité.

#8 Bien gérer les droits d'utilisation des postes de travail

Avoir tous les droits n'est jamais une bonne chose

Il existe communément deux types de comptes sur un poste de travail professionnel : l'administrateur et l'utilisateur. Chaque profil confère des droits plus ou moins étendus sur l'utilisation de son appareil. Le profil (ou compte) administrateur permet d'intervenir sur le fonctionnement global du poste de travail, ses mises à jour et sa sécurisation. Le profil utilisateur quant à lui limite le poste de travail à une utilisation « opérationnelle », suffisante pour réaliser ses tâches professionnelles. Une bonne gestion des droits utilisateurs permet, entre autres, de centraliser et d'assurer les mises à jour régulières de ses postes de travail, ou de limiter l'installation et l'exécution de programmes ne provenant pas de sources sûres.



Les risques

Une mauvaise gestion des droits utilisateurs sur les postes de travail, expose l'entreprise à des mauvaises manipulations, pouvant entraîner des **problèmes de sécurité au niveau du système d'information.**

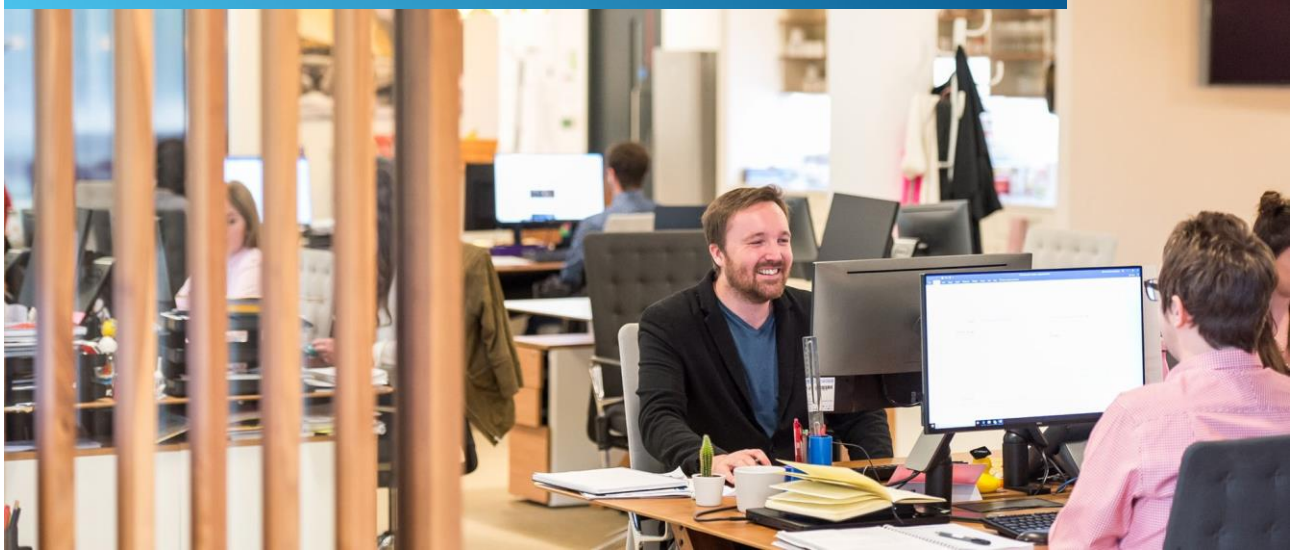
Qui est concerné ?

● ● ● LE SERVICE INFORMATIQUE

○ ○ ○ LES UTILISATEURS

La responsabilité de la gestion des droits utilisateurs **incombe directement à l'entreprise** par l'intermédiaire de son équipe informatique.

#8 Bien gérer les droits d'utilisation des postes de travail



Mesures préventives

1. Identifiez clairement chaque utilisateur du système informatique afin de leur attribuer les **droits/privilèges adéquat** et supprimez les éventuels comptes anonymes ou génériques ;
2. Réservez l'utilisation des **comptes administrateurs uniquement au service informatique** ou au prestataire en charge de la gestion de votre informatique ;
3. Mettez en place une **politique d'encadrement des arrivées et des départs** de personnel, pour maîtriser la gestion des droits sur l'ensemble des postes de travail connectés au système d'information ;
4. Soyez à l'écoute des utilisateurs et mettez en place, si possible, un **système d'assistance technique réactive.** Ne tombez pas dans un excès de sécurisation qui pourrait mener les utilisateurs à la frustration, et au contournement des règles ou au BYOD.

Notre avis

Dans la gestion des droits utilisateurs, on peut être tenté de suivre le vieil adage « qui peut le plus peut le moins » en attribuant facilement des droits administrateurs, mais ce serait une très mauvaise idée. **Chaque ouverture de droit supplémentaire, hors service informatique, doit être sérieusement étudiée et encadrée.** Cela demande évidemment une bonne organisation.

#9 Se former continuellement (service informatique et utilisateurs)

Un utilisateur averti est un excellent premier rempart contre les menaces

Cloud, cybersécurité, RGPD, multiplication des « devices » ou télétravail ont créé de nouvelles problématiques et donc de nouvelles expertises à maîtriser. Le rôle du service informatique se complexifie et il doit désormais pouvoir s'appuyer sur des utilisateurs correctement formés aux bonnes pratiques de base. Grâce à une gestion et une responsabilité partagée du système d'information entre le service informatique et les utilisateurs, l'informatique de l'entreprise est généralement moins sujette aux incidents. **De plus cela permet au service informatique, moins sollicité sur des opérations de maintenance, de se concentrer sur des tâches à plus forte valeur ajoutée, comme des projets d'optimisation du système d'information.**

Pourtant dans beaucoup de PME, les services informatiques, souvent composés d'une seule personne, passent l'essentiel de leur temps à « faire du correctif » auprès d'utilisateurs mal formés à l'utilisation du système d'information. Un cercle vicieux dans lequel il est dangereux de s'installer.

Les risques

Une équipe informatique trop occupée à gérer des incidents, souvent provoqués par des utilisateurs peu ou pas formés à la sécurité informatique, **dispose de moins de temps pour optimiser et sécuriser son SI sur le long terme.** Ce qui expose potentiellement le système informatique à des failles de sécurité plus ou moins importantes.

Qui est concerné ?

●●● LE SERVICE INFORMATIQUE

●●○ LES UTILISATEURS

Dans un environnement professionnel, **la sécurité informatique est plus que jamais l'affaire de tous.** Chacun à leur niveau, service informatique comme utilisateurs doivent être formés à la bonne gestion de leur système d'information.

#9 Se former continuellement (service informatique et utilisateurs)

Mesures préventives

1. Mettez en place **un plan de formation, continu et ludique,** autour de la sécurité informatique, et dédié aux utilisateurs.
2. Faites de la veille et organisez des **actions de prévention en fonction des actualités** liées à la sécurité informatique .
3. Faites en sorte que la formation et la prévention des utilisateurs deviennent les **missions principales du responsable informatique.**
4. Visez une gestion/maintenance partagée du système d'information entre le service informatique et les utilisateurs, pour que **chaque utilisateur devienne « responsable du système d'information » à son niveau.**
5. Si vos effectifs sont réduits, ou que votre budget le permet, confiez tout ou partie de la gestion technique de votre système informatique à un **prestataire externe spécialisé disposant d'une expertise technique toujours à jour.** Dans tous les cas, délaisser la maintenance opérationnelle du système d'information ne doit jamais être à l'ordre du jour.

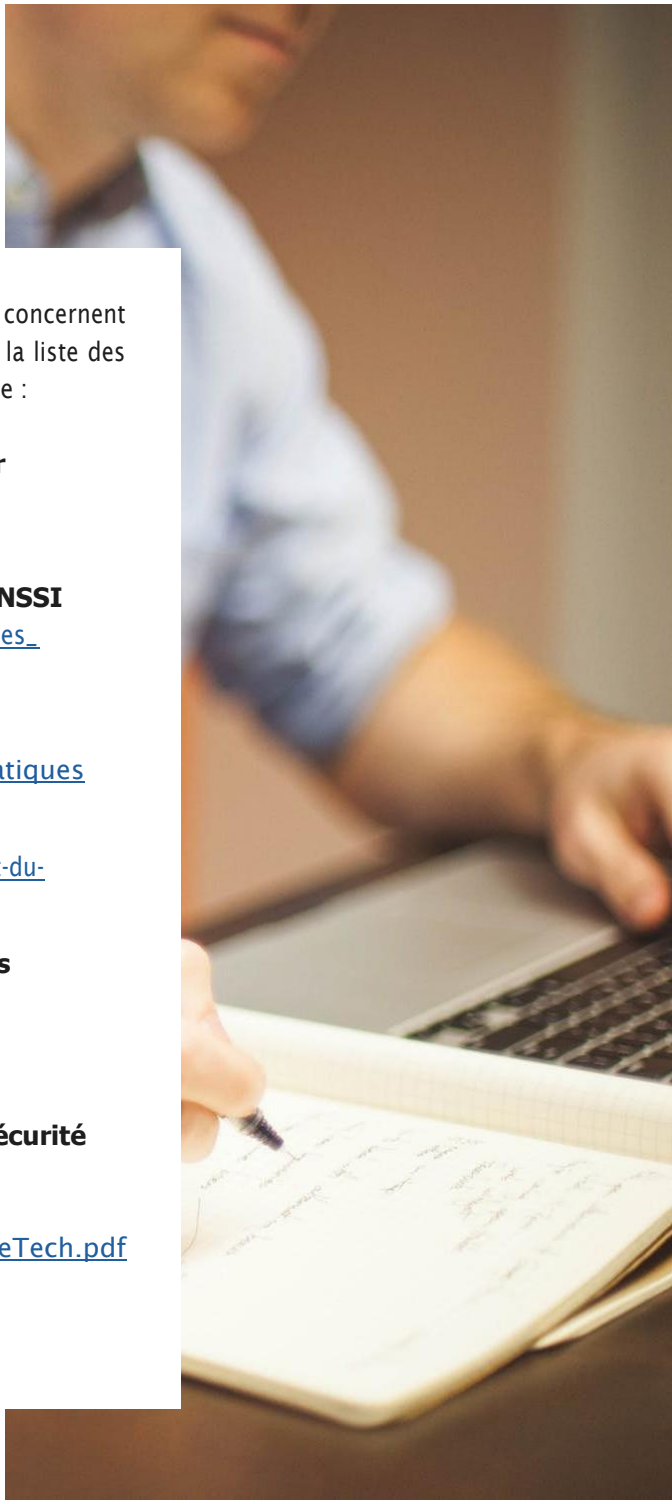
80%

Selon l'ANSSI, 80% des problèmes informatiques dans les entreprises seraient aujourd'hui liés au seul facteur humain. (Source ANSSI - Agence Nationale de la Sécurité des Systèmes d'Information, 2019)

Notre avis

La formation et la prévention permettent de limiter grandement les risques d'incidents informatiques en entreprise. La bonne stratégie consiste donc à **mettre en place un cercle vertueux, collectif, de bonne gestion du système d'information.** Cette mission nécessite une participation de l'ensemble des collaborateurs de l'entreprise. Un défi qui en vaut la peine, sans aucun doute, au vu de la multiplication des cyberattaques ces dernières années.

Bibliographie



Nous sommes experts, mais pas hermétiques aux informations qui concernent notre cœur d'activité, surtout si elles peuvent aussi vous aider. Voici la liste des supports qui nous ont servi en partie pour la rédaction de ce guide :

- **Dispositif d'assistance aux victimes d'actes de cyber malveillance**
  https://www.cybermalveillance.gouv.fr/
- **Guide des bonnes pratiques informatiques CPME/ANSSI**
  https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf
- **BYOD : quelles sont les bonnes pratiques ?**
  https://www.cnil.fr/fr/byod-quelles-sont-les-bonnes-pratiques
- **L'évolution du BYOD, c'est la mort du BYOD**
  https://www.zdnet.fr/actualites/l-evolution-du-byod-c-est-la-mort-du-byod-39875761.htm
- **Sécurité numérique : Bonnes pratiques à l'usage des professionnels en déplacement**
  https://www.ssi.gouv.fr/uploads/2014/09/anssi_passeport_2019_1.0.pdf
- **Note technique de l'ANSSI : Recommandations de sécurité relatives aux réseaux Wi-Fi**
  https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_WIFI_NoteTech.pdf
- **Le site de Mister-IT**
  www.Mister-IT.io

À propos de Mister-IT

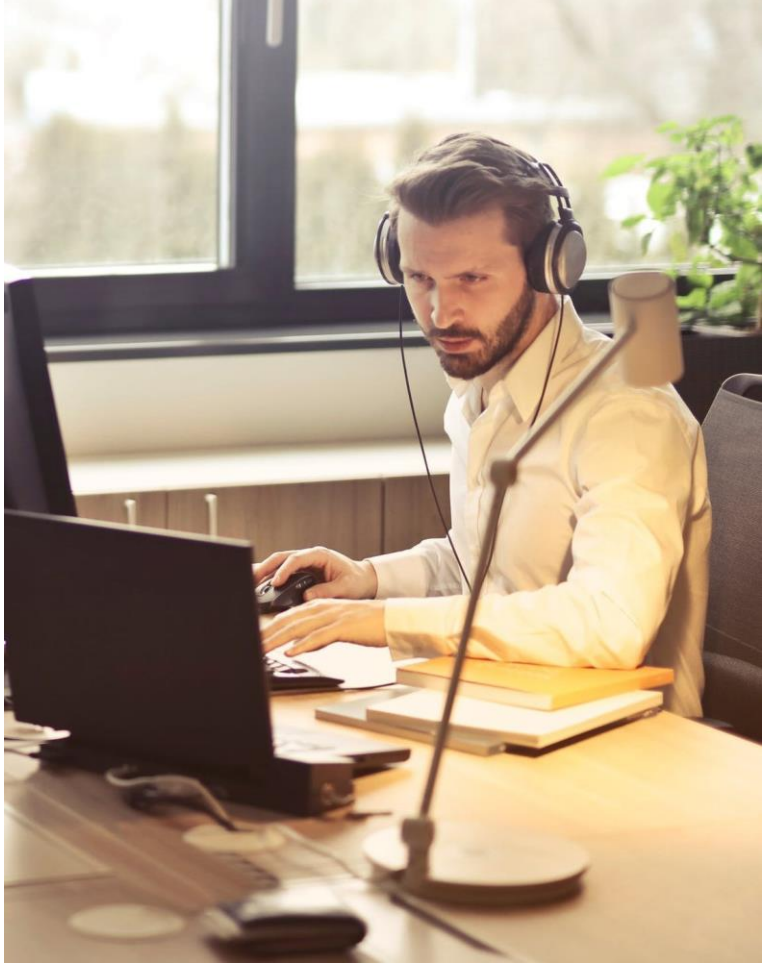
Depuis 10 ans, le projet d'ouvrir une structure dite « idéale » mûrissait, Julien CHAMPION a su s'entourer de nombreux talents et de nombreuses expériences de projets informatiques réussis au côté de clients et partenaires via de la prestation de service, nous permettant de vous garantir un haut niveau d'expertise. Nous attachons beaucoup d'importance à l'humain et aux machines.

Notre mantra, Réactivité, Transparence et Expertise.

Parce qu'une réponse immédiate est primordiale, nous assurons également une assistance technique déclinée en plusieurs solutions. Un service de télémaintenance accessible en un simple clic depuis notre site web ou par voie téléphonique pour une prise en main immédiate et sécurisée de votre poste à distance par un de nos techniciens. Pour des structures plus importantes nécessitants une maintenance et une assistance opérationnelle quotidienne, nous proposons la mise à disposition d'un responsable informatique à temps partagé vous apportant confort et flexibilité.

Nos objectifs étant de vous faire profiter pleinement de vos outils et des nouvelles technologies, pour cela nous répondons aux 4 principales problématiques que vous pouvez rencontrer :

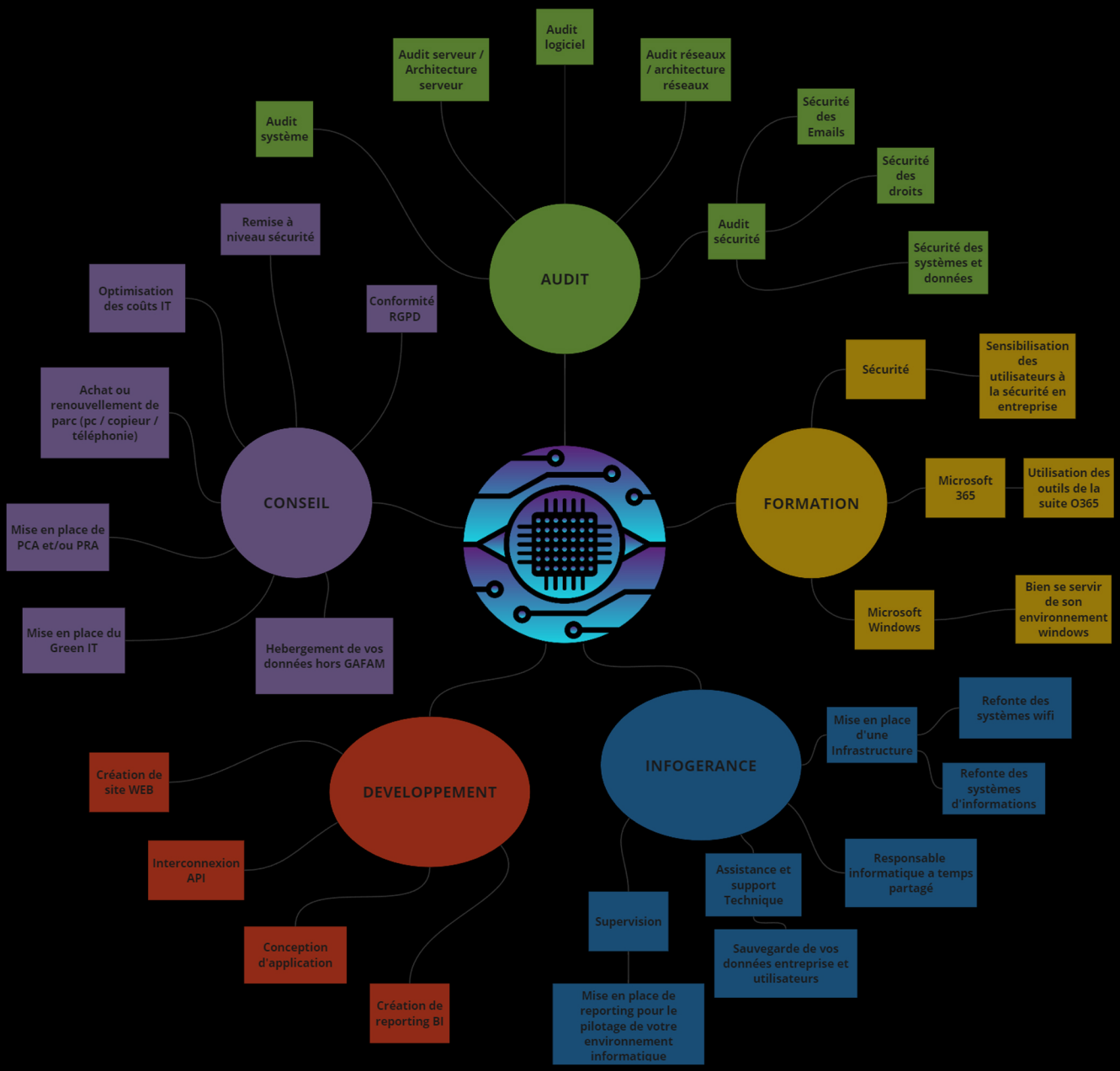
1. La disponibilité et la fiabilité de votre système d'information.
2. La sécurité de vos données d'entreprises.
3. Le renouvellement de votre infrastructure informatique et de vos matériels.
4. Bénéficier de conseils et d'expertise sur des solutions adaptées, concrètes et transparentes.



Nous souhaitons avant tout fournir des services d'excellence au meilleur rapport qualité / prix en bâtissant une relation transparente de confiance à long terme avec nos clients et nos collaborateurs. Toutes nos démarches visent à vous soumettre des solutions toujours plus simples et rapides à mettre en œuvre pour accélérer votre retour sur investissement et accroître les performances de vos équipes à l'aide d'outils ajustés à leurs réels besoins. (Audit approfondi commençant par une identification et un recensement complet de votre parc informatique, ses applications et usages avec une vraie prise en considération du retour utilisateur).

Vous avez des questions ou des projets ? Contactez-nous pour fiabiliser l'exploitation de vos outils informatiques et en faire un outil de travail performant plutôt qu'une source d'énervement ou d'incompréhension !

Au plaisir de vous accompagner ou de vous venir en aide



06.25.54.16.15

contact@mister-it.io

www.mister-it.io