Projet SAS
Autoconcept

En collaboration avec

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Intervenants

Argentini Gabriel
BERNARDO Filipe
BERSWEILER Gregory
SALMERON Marianne

Sommaire

Présentation

TechnoSAS

TechnoSAS est une entreprise de prestations informatiques aux petites et très petites entreprises. Elle est dotée de 29 ans d'expérience en maintenance informatique avec des dirigeants orientés sur la réactivité et l'expérience garantissant une prise en charge optimal des requêtes.

Le relationnel et la complémentarité des équipes permettent à TechnoSAS de proposer à ses clients une offre globale basé sur la performance et l'innovation technologiques de l'information tout en respectant au maximum les besoins de l'entreprise à moindre frais.

Légalité et Sécurité

Les outils informatiques sont aujourd'hui un avantage pour toutes les entreprises, ils permettent d'avoir une ouverture vers l'extérieur pour une meilleure communication et un meilleur travail. En contrepartie, ils peuvent aussi nuire au bon fonctionnement de l'entreprise suite à une ou plusieurs mauvaises utilisations de la part des utilisateurs. Comme par exemple la perte de productivité et de rentabilité.

L'informatique est comme tout dans la vie, elle à des règles. C'est pour cela que nous avons préparé une note de synthèse avec quelques règles, solutions et articles extrais de la loi informatique.

Nous avons donc abordé pour votre entreprise les sujets suivants :

- Les moyens légaux à mettre en place pour la sécurité des fichiers ;
- Les informations devant être connus des employés concernant l'usage des outils informatiques ;
- La mise en place d'une solution de filtrage ;
- Une charte informatique à signer par les employés dès leurs embauches.

Moyens légaux pour la sécurité des fichiers

Comme le dit l'article 34 de la Loi informatique et libertés ci-dessous, l'entreprise Autoconcept est responsable d'assurer la sécurité des fichiers et des données personnelles. C'est pourquoi nous mettons en place des solutions pour appliquer cette même Loi.

Article 34 de la Loi informatique et libertés :

« Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »

Pourquoi assurer la sécurité de son entreprise et des données personnelles ?

- Aujourd'hui, tout est « données » : nos activités personnelles et professionnelles sont complètement dépendantes de nos systèmes d'information ;
- Les attaques sont nombreuses et en croissance : un nouveau virus serait lancé toutes les 15 secondes et on dénombre plus d'un milliard d'attaques informatiques en 2017 ;
- Les conséquences peuvent être dramatiques : des entreprises peuvent voir leur activité arrêtée, leur image fortement dégradée, devoir payer des fortes sommes pour récupérer des suites d'un sinistre, voire mettre la clé sous la porte. Certaines personnes peuvent perdre leur argent, leur emploi, leur santé, etc.

La sécurité des systèmes d'information devient donc un enjeu primordial pour l'entreprise

Les 12 règles essentielles à appliquer pour la sécurité des fichiers :

1. Choisir avec soin ses mots de passe ;
2. Mettre à jour régulièrement vos logiciels ;
3. Bien connaître ses utilisateurs et ses prestataires ;
4. Effectuer des sauvegardes régulières ;
5. Sécuriser l'accès Wi-Fi de votre entreprise ;
6. Être aussi prudent avec son ordiphone (smartphone) ou sa tablette qu'avec son ordinateur ;
7. Protéger ses données lors de ses déplacements ;
8. Être prudent lors de l'utilisation de sa messagerie ;
9. Télécharger ses programmes sur les sites officiels des éditeurs ;
10. Être vigilant lors d'un paiement sur Internet ;
11. Séparer les usages personnels des usages professionnels ;
12. Prendre soin de ses informations personnelles, professionnelles et de son identité numérique.

Informations devant être connus de la part des utilisateurs

Un moyen informatique, peu importe sa nature, est soumis à des règles précises et définies. Dans le milieu professionnel, certaines mesures légales et morales doivent être appliquées en sus de celles imposées à toute personne en respect de la législation française.

L'employeur tire de son pouvoir de direction, le droit de surveiller et de contrôler l'activité de ses salariés sur le lieu et pendant le temps de travail. Il peut notamment contrôler l'utilisation par ses salariés des outils mis à leur disposition pour l'exécution de leur travail.

L'employeur ou le dirigeant autorise l'employé ou l'exécutant à utiliser les moyens qui sont mis à sa disposition à de strictes fins professionnelles. En retour, l'employé ou l'exécutant s'engage à utiliser ce matériel, durant les heures de travail, exclusivement pour des activités qui sont liés à sa profession. L'utilisateur a cependant le droit à une sphère d'intimité, dans laquelle il peut utiliser son appareil professionnel à des fins personnelles tant que cette activité reste ponctuelle et mesurée.

L'employeur est également tenu de prévenir son personnel de tout moyen de surveillance lié à son activité professionnelle : sauvegarde de logs et historique internet, filtrage de contenu.

En aucun cas, et peu importe les circonstances l'employeur ne peut consulter les mails d'un employé sans son autorisation explicite – même si cette correspondance est envoyée depuis un mail professionnel. Cela relève de la sphère d'intimité citée précédemment.

D'une part, en vertu de l'exigence de loyauté dans les relations contractuelles, les salariés doivent être informés préalablement des moyens de contrôle mis en place par l'employeur dès lors

qu'ils peuvent être utilisés dans une procédure visant à sanctionner leur comportement (Cass. Soc., 22 mai 1995, n° 93-44.078). Ainsi le règlement intérieur ou une charte informatique portée à la connaissance des salariés, peuvent prévoir les conditions d'utilisation des outils informatiques, encadrer leur utilisation à des fins personnelles et préciser les moyens de contrôle.

D'autre part, sur le fondement de l'article L. 1121-1 du Code du travail, le contrôle de l'utilisation du matériel informatique opéré par l'employeur ne doit pas apporter aux droits et libertés des salariés des restrictions disproportionnées et non justifiées par la nature de la tâche à accomplir. Ainsi le droit au respect de la vie privée et le droit au secret des correspondances consacrés à l'article 9 du Code civil et à l'article 8 de la Convention européenne de Sauvegarde des droits de l'homme, peuvent être invoqués par le salarié qui estimerait le contrôle de son activité par l'employeur contraire au respect de l'intimité de sa vie privée. C'est en effet le célèbre arrêt Nikon qui a consacré le droit du salarié au respect de l'intimité de sa vie privée même au temps et au lieu de travail (Cass. Soc., 2 oct. 2001, n° 99-42.942).

Filtrage du contenu

Dans le cadre d'une utilisation des outils informatiques professionnelle, l'accès à certains sites et outils se doit d'être régulé.

Cela vaut évidemment pour les sites à contenu illégal ou illicite (pédopornographie, terrorisme, jeux d'argents illégaux…) mais également pour les sites dits de loisir (plateformes de jeux, réseaux sociaux…).

Article 1241 du Code Civil
"Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence."

Article 1242 du Code Civil
"On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde."

Il est donc crucial de réguler l'utilisation du moyen informatique et les accès des utilisateurs. Pour cela, le filtrage par proxy est l'une des solutions les plus préconisées. Il en existe deux types :

- **Le filtrage par liste noire**

Il fonctionne en deux étapes : tout d'abord, le proxy compare l'adresse du site qui tente d'envoyer des données à l'utilisateur à sa base de données de sites inaccessibles (sites frauduleux, dangereux ou spécifiquement interdits par l'entreprise tels que les réseaux sociaux). Si celui-ci n'est pas présent dans cette base de données, une intelligence artificielle analyse son contenu (mots récurrents, analyse du code…) afin de déterminer si l'accès peut être obtenu.

A noter : les intelligences artificielles ne sont pas encore aujourd'hui capables de la nuance d'un être humain. Des services se sont donc spécialisés dans l'analyse manuelle de sites internet afin de constituer des profils de bases de données adaptées aux besoins de leurs entreprises clientes.

- **Le filtrage par liste Blanche**

Cette méthode est plus utilisée dans des structures nécessitant des accès à un panel de sites spécifique. La base de données se constitue de sites dont la consultation est autorisée – toute demande émanant d'une adresse différente de celles strictement acceptées par cette base de données sera refusée.

Bien que populaire, le filtrage par liste blanche possède un défaut majeur : son manque de versatilité. Parfois, un utilisateur confronté à un bug ou s'interrogeant sur un sujet lié à sa profession se tentera une recherche via un moteur de recherche, pour qu'il ne puisse au final accéder qu'à certains sites bien définis, qui ne contiennent pas nécessairement les réponses à ses questions.

Ces solutions sont spécialisées dans le filtrage web, relevant strictement de la navigation sur internet. Il est également important de noter que certains logiciels peuvent relever des cas d'interdiction précédemment cités ; l'impossibilité d'installer des solutions informatiques sans compte administrateur est également à préconiser afin de contrôler leur bien-fondé.

CHARTE INFORMATIQUE

Sécurisation des données

Un plan de sécurisation des données a pour objectif de fournir une sécurité optimale tout en respectant les lois en vigueur. Conformément à l'article 34 de la loi du 6 Janvier 1978 modifiée, dite loi Informatique et Libertés, déterminer les précautions à prendre "au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données". Le règlement européen 2016/679 du 27 Avril 2016 (RGPD : Règlement Général sur la Protection des Données) précise que la protection des données personnelles nécessite de prendre des "mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque" (Art. 32)

Stratégie de Mot de Passe

La protection de l'information nécessite des systèmes de sécurité telle que l'utilisation de mots de passe suffisamment difficiles pour être retrouvés par un robot ou une tierce personne. L'utilisation d'un mot de passe unique et régulièrement mis à jour est recommandée, ce qui nécessitera une réinitialisation régulière. Il est également conseillé d'éviter de stocker ces mots de passe dans la base de données de l'ordinateur.

Pour permettre une protection optimale, le mot de passe devrait pouvoir être référencé de la manière suivante :

- Un minimum de 8 caractères pour limiter les risques de récupération du mot de passe de la part d'un tiers ;
- Comporter au moins un chiffre, une lettre et un caractère spécial ;
- Différent des informations suivantes : Nom/Prénom/Date de Naissance de l'utilisateur ou de l'un de ses proches.

Pour une protection maximale des mots de passes, un ensemble de règles sont à prendre en compte et s'y tenir pour ne pas avoir de fuite.

- Ne pas communiquer son mot de passe par téléphone ou mail sans l'accord du service informatique ;
- Se déconnecter de l'ordinateur ou verrouiller votre session Windows avant de quitter l'ordinateur ;
- Empêcher le navigateur de stocker les mots de passe dans la base de données ;
- Activer la double authentification si le service le permet.

Pour terminer, le mot de passe d'un compte devrait être changé tous les 3 mois. En cas d'échec d'authentification du mot de passe à plusieurs reprise, le compte sera désactivé jusqu'à réactivation du compte avec réinitialisation du mot de passe par le service informatique.

Modalités de communication aux utilisateurs et de mise œuvre

Pour garantir la sécurité de l'information, les utilisateurs seront amenés à lire et signer une charte informatique, ainsi que de respecter les obligations liées au règlement général sur la protection des données. Cette charte a pour rôle de réglementer l'usage des systèmes d'informations des salariés.

Nous recommandons cette procédure interne afin d'assurer la protection des données personnelles en permanence quel que soit le risque encouru (gestion des demandes d'accès, faille de sécurité, etc..).

Gestion des dossiers et fichiers sécurisés

Plusieurs solutions peuvent résoudre les soucis de gestion des dossiers et fichiers sécurisés. L'installation d'un serveur de stockage en réseau (NAS) permet d'avoir un serveur physique dans l'entreprise. Le serveur possède une adresse locale (IP) et peut être consulté uniquement par des appareils connectés au serveur en IP dit "Local".

La connexion locale permet d'éviter tout type d'intrusion n'ayant pas accès à un ordinateur du réseau privé. Afin d'assurer davantage la sécurité du réseau, certaines fonctionnalités ne sont exécutables que par les comptes faisant partie du groupe "Administrateur".

En conséquence, l'accès à différent dossiers et fichiers sécurisés est filtré en fonction du groupe d'appartenance du profil utilisateur.

Utilisation de logiciel de Sécurité

Les postes informatiques utilisés par les utilisateurs doivent posséder un antivirus pour filtrer les fichiers vulnérables pouvant endommager le matériel.

Les postes doivent aussi proposer un bon paramétrage du pare feu. Celui-ci bloquera les ports entrant et sortants non-utilisés sur le poste pour éviter toute attaque informatique au sein de l'entreprise.

L'ajout d'un anti-spam permet de sécuriser la messagerie des usagers et est conseillée pour une protection optimale de l'entreprise.

Sécurisation physique des données

Les données, bien que virtuelles, sont également physiquement présentes en étant stockées dans les disques durs que possède le serveur. La sécurisation du matériel reste une étape à considérer.

Plusieurs types de dégâts peuvent mener à la destruction ou au vol des données :

- Le vol par effraction
    - Accès à la salle par badge ou clé ;
    - Vidéosurveillance de la zone ;
    - Alarme liée à un SMTP.
- L'accident technique
    - Un onduleur alimente le serveur en cas de coupure de courant ;
    - Climatisation afin de refroidir le matériel.
- L'intempérie
    - Détecteur de fumée ;
    - Local ignifugé.

Mesures immédiates de sauvegarde

Malgré des mesures prises pour la sécurisation des données, il est impossible de prévoir un piratage. Il en va de même pour tout type de panne. Les solutions qui peuvent être mises en place ne sont que préventives.

- L'utilisation d'un système de sauvegardes interne ;
- Des sauvegardes régulières et journalières ou hebdomadaires selon la criticité ;
- Vérifier la période d'amortissement des disques serveurs.

En cas de problème non-solvable par le service informatique

Dans le cas où le service informatique de l'entreprise n'a plus la capacité de gérer le problème de sécurité, il revient au prestataire de procéder à la maintenance.

L'accès à l'entreprise pour gérer l'incident peut être établit de deux manières :

- La prise en main à distance d'un expert ;
- La présence d'un expert sur le terrain.

L'expert aura pour mission de diagnostiquer le problème rencontré et d'établir un plan de maîtrise dans la résolution de celui-ci. L'expert ne sera contacté qu'en cas de non-possibilité de maintenance par le service informatique.

Authentification

L'authentification vise à prouver l'identité d'un individu et peut s'exécuter de différentes manières :

- Ce que vous savez (mot de passe, code PIN, etc.)
- Ce que vous avez (carte magnétique, lecteur de carte, etc.)
- Ce que vous êtes (empreintes digitales, lecteur rétinien, etc.)

Deux de ces facteurs d'identification seront nécessaires pour une authentification forte.

Retour sur Investissement

Dans le cas de la protection des données, nous parlerons plus souvent d'une diminution au retour sur investissement désignant un ratio financier mesurant le montant d'argent gagné ou perdu par rapport à la somme initialement investie.

Le retour sur investissement attendu en moyenne s'élève à environ 8%.

Une intervention longue durée peut impacter le rendement de l'entreprise et, par conséquent, le retour sur investissement causant des pertes plus ou moins denses. Un service rapide et efficace permet de réduire les risques d'intervention longue.

Une formation pour tenir les techniciens à jour ainsi que requalifier les compétences acquises est plus que conseillée pour les entreprises.

Charte qualité service client

La continuité de service en cas de panne

Vous offrir une prestation réalisée selon les engagements définis ensemble : nature des tâches à effectuer, ponctualité, respect des consignes, durée de la prestation…

Assurer le remplacement du matériel de qualité identique en cas de panne, pour permettre la continuité du service.

Assurer grâce à un logiciel de gestion, l'archivage des différentes pannes/interventions rencontrées. Afin d'avoir la solution si jamais le problème se répète.

Le relationnel client

Garantir la qualité des conditions de l'accueil en agence ou au téléphone.

Dès le premier accueil, vous délivrer une information claire sur notre identité, nos services, nos prestations, nos tarifications.

Vous écouter et prendre en compte vos besoins pour vous conseiller, vous apporter le service et l'intervenant correspondant à vos attentes.

Le cas échéant, vous orienter vers un prestataire pouvant prendre en charge votre demande.

Mesurer régulièrement votre satisfaction.

La sécurité et la productivité

Analyser et proposer les meilleures solutions techniques au bénéfice du client

Développer de nouvelles offres de services pour satisfaire vos futurs besoins

Vous garantir une réactivité, une souplesse et une adaptation à vos besoins et attentes.

Garantir le respect de votre entreprise et de la confidentialité de vos projets

Vous assurer la continuité de l'intervention : remplacement de l'intervenant en cas d'indisponibilité.

Règlement interne

L'image de l'entreprise TechnoSAS est reflétée en grande partie par l'apparence des intervenants chez les clients et de leur attitude. Ce mémo concerne tous les employés de l'entreprise et devra donc être signé. Le non-respect de celles-ci donnera suite à des sanctions.

Apparence et Attitude

Le comportement auprès des clients doit être irréprochable et cela passe par :

- Le port d'une tenue vestimentaire correcte est obligatoire lors des contacts avec le client ;
- Une attitude irréprochable est attendue lors d'un contact direct ou par téléphone ;
- La simplification du langage utilisé afin de répondre aux attentes du client de façon claire et compréhensible ;
- Le respect des horaires. Une ponctualité constante vous sera demandée.

Confidentialité

Vous accédez à des données privées et à ce titre il est vous demandé la plus grande discrétion lors :

- Des interventions sur les postes utilisateurs, les techniciens n'ont en aucun cas l'autorisation de parcourir les dossiers et fichiers privés des clients ni de les divulguer.

Organisation

- L'utilisation d'un système de ticketing servira à définir la priorité des demandes, les clients seront tenus informés de l'avancement de leurs demandes.

Conclusion

En conclusion, Faire appel à nous, c'est faire appel à l'efficacité. Nous vous proposons donc des services permettant à votre entreprise d'être à jour au niveau informatique, d'être au point sur la loi et de travailler en toute sécurité.

Nous nous engageons à avoir une attitude professionnelle durant toute notre intervention.

Remerciements

Nous vous remercions de nous avoir choisi en tant que prestataires, nous vous remercions également de votre attention portée sur notre projet et on espère que cela vous à plut.

Annexes