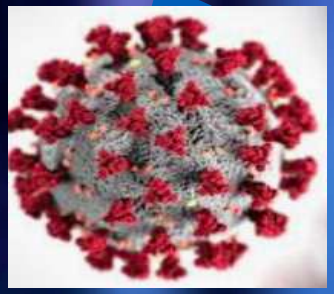
CENADI



COVID-19: menaces sur le Système d'Information des organisations

Mai 2020

Sommaire

Avant-propos

Les premiers patients de la pandémie du COVID-19 ont été signalés en Chine en décembre 2019. Depuis lors, elle s'est répandue dans la quasi-totalité des pays du monde. Etant une pandémie causée par un virus très virulent qui se transmet par simples contacts, de nombreux Etats ont opté pour un confinement (total ou partiel) pour limiter la propagation du virus au sein de la population. Du fait de ce confinement, le télétravail est prescrit pour les activités ne nécessitant pas la présence physique des travailleurs à leurs postes.

De nombreuses problématiques ont donc vu le jour. Nous pouvons citer entre autres :

- La mise en évidence de l'importance d'un plan de continuité des activités et de tests périodiques de ce dernier: au début de la pandémie, de nombreuses organisations se sont retrouvées en très grande difficultés du fait de l'absence de plan de continuité des activités ou de l'existence d'un plan n'ayant jamais été testé ;
- La vulgarisation des outils de téléconférence : le télétravail a permis la vulgarisation des outils de téléconférence dans les organisations. Néanmoins, un certain nombre de mesures doivent être prises pour éviter que ces outils sensés faciliter le travail ne deviennent des vecteurs de cyber attaques ;
- La surutilisation des outils de partage de fichiers: avec le télétravail, la nécessité de partager des fichiers est beaucoup plus élevée que lors du travail sur site. Toutefois, ceci pourrait poser des problèmes si les mesures de sécurité ne sont pas correctement prises en compte ;
- La mise à disposition de plateformes web d'accès distant pour les collaborateurs et les clients: afin de continuer à collaborer avec les clients et partenaires, certaines organisations ont mis à leur disposition des portails web. Toutefois, ceci pourrait poser des problèmes si les mesures de sécurité ne sont pas correctement prises en compte ;
- L'augmentation du nombre de cyber attaques liées au COVID-19: à cause de la situation de peur et d'urgence, le nombre de cyber attaques a considérablement augmenté, en particulier les attaques de type phishing (hameçonnage), les rançongiciels, les vols de données et les attaques de type FOVI (Faux Ordres de Virement) ;

Toutefois, malgré les nombreux défis posés par cette pandémie, elle constitue pour les organisations, une opportunité de digitaliser leurs processus et ainsi de gagner en efficacité. Plus que jamais, les décideurs se rendent compte de l'importance de la digitalisation et sont prêts à y investir.

Nous sommes heureux de partager avec vous ce document dans lequel nous développons ces différentes menaces et opportunités tout en vous proposant des pistes de solutions.
Nous espérons qu'il vous permettra de mieux gérer les risques liés à votre système d'information en ce temps de crise mais aussi à en saisir les opportunités.

Bonne lecture!

Dr Chantal Marguerite MVEH

Directeur du Centre National de Développement de l'Informatique (CENADI)

Email: chantal.mveh@minfi.cm
Téléphone: +237 222 220 766

Plan de continuité des activités

La situation d'urgence sanitaire vécue par le monde entraîne des perturbations susceptibles d'affecter les systèmes d'informations des services publics et des activités économiques. Toutefois, les organisations gouvernementales ont une obligation de continuité du service public.

Ces perturbations peuvent être limitées par une préparation en amont. Cela ne s'improvise pas, et certaines dispositions sont nécessaires, à l'instar de la mise en place d'un Plan de Continuité des Activités (PCA).

Le Plan de Continuité des Activités (PCA) est un document devant permettre à une organisation de fonctionner même en cas de désastre ou de crise majeure ; quitte à ce que ce soit en « mode dégradé ». Il a pour but d'anticiper un événement susceptible de perturber gravement le fonctionnement normal de l'organisation et de mettre en place une stratégie qui permet d'en limiter l'impact.

Avec la crise liée au COVID-19, les organisations qui ne disposent pas de ce plan très important s'exposent aux risques suivants:

- Interruption d'activité
- Pertes financières
- Perte de la confiance des usagers/clients
- Faillite.

Que devons-nous faire?

En vue de garantir la continuité des activités de votre organisation tout en minimisant l'impact des interruptions, vous devriez mettre en place un plan de continuité des activités et le tester au moins une fois par an.

Le PCA est constitué d'un ensemble de documents à l'instar de :

1) Plan de Gestion de Crise: il définit les éléments liés à la gestion de la crise, communication, etc.

2) Plan de Reprise d'Activité: il définit la stratégie de reprise de l'activité.

3) Plan de Secours Informatique: il a pour but de garantir la survie de l'entreprise en cas de sinistre important touchant le système informatique. Il s'agit de redémarrer l'activité le plus rapidement possible avec le minimum de perte de données.

4) Plan de Repli Logistique: il définit la stratégie de repli en lien avec les biens et les personnes.

5) Plan de test: il définit la stratégie de test du PCA.

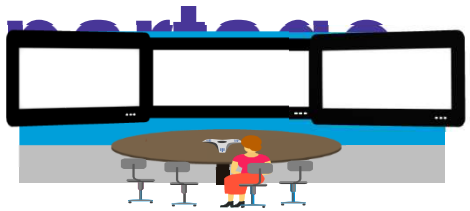
6) Plan de Maintien en Conditions Opérationnelles: il définit l'ensemble des mesures prises pour garantir que la bascule vers un environnement dégradé n'entraîne pas une altération inacceptable des conditions de travail habituelles.

Pour ce qui concerne les systèmes d'information, en ce moment, une attention particulière doit être portée en la capacité de l'entreprise à assurer la continuité en cas d'indisponibilité de certains informaticiens. Ceci d'autant plus, que dans plusieurs organisations, les tâches informatiques ne sont assurées que par une seule personne. Il est important de mettre en place des mesures pour assurer la disponibilité des mots de passe des comptes d'administration en cas d'indisponibilité des informaticiens.

Un PCA non testé n'a aucune valeur. Il est donc nécessaire de tester régulièrement le PCA, au moins à une fréquence annuelle. Ces tests permettent de s'assurer que le PCA rédigé est réalisable et permet effectivement de garantir la continuité de l'activité dans les conditions convenues (délais de reprise, perte maximale de données, etc.).

En plus des tests réguliers, il est important de conduire des **audits annuels de votre PCA** afin d'en déterminer les limites et les axes d'amélioration potentiels.

Outils de téléconférence et de fichiers



Dans un contexte de télétravail, les organisations utilisent diverses plateformes permettant d'effectuer des réunions en ligne (via des appels audio ou vidéo, conversations de groupe ou privées, partage d'écrans) et des partages de fichiers.

Malgré toutes ces fonctionnalités très utiles, ces plateformes présentent parfois des failles de cyber sécurité qui peuvent être exploitées par des hackers. A titre d'exemple, une faille de sécurité a été identifiée dans la plateforme de téléconférence Zoom pendant le mois de mars 2020.

Il a été relevé une augmentation du nombre de cyber attaques depuis le début de cette pandémie. En effet, les hackers profitent de cette situation pour multiplier les attaques de type phishing et attaques par déni de service. A titre d'exemple, entre le 1er et le 23 mars, le spécialiste en cyber sécurité Barracuda Networks a enregistré un bond de 667 % des tentatives d'hameçonnage surfant sur le Covid-19.

Que devons-nous faire?

I – Outil de téléconférence :

Lors du choix des plateformes de téléconférence, les organisations devraient tenir compte des points suivants:

i. Implémentation d'un algorithme de chiffrement de bout en bout;

ii. Utilisation de normes de chiffrement solides, bien connues et testables;

iii. Utilisation de l'authentification multi-facteur (MFA) pour valider l'identité des utilisateurs;

iv. Possibilité pour les utilisateurs de voir et contrôler qui se connecte aux sessions de collaboration;

i. La politique de confidentialité du service ne permet pas au fournisseur de partager des données avec des tiers ou des sociétés affiliées;

i. Possibilité pour les utilisateurs de supprimer en toute sécurité les données du service et de ses référentiels selon leurs besoins;

ii. Outil certifié: ISO 270001, SSAE16, etc.

iii. Réputation de l'outil après une veille technologique.

II – Outils de partage de fichiers :

Lors du choix des outils de partage de fichiers, les organisations devraient tenir compte des points suivants:

i. Chiffrement de bout en bout des fichiers envoyés;

ii. Utilisation de normes de chiffrement solides, bien connues et testables;

iii. Expiration des fichiers transmis après un certain temps: afin d'éviter qu'une personne malveillante ait accès aux fichiers transmis après son utilisation, l'outil devrait être capable de supprimer le fichier de la plateforme après expiration;

iv. Robustesse du mécanisme d'authentification.

v. Outil certifié: ISO 270001, SSAE16, etc.

En cas de doute sur la sécurité de l'outil de partage de fichier utilisé, nous vous recommandons de crypter les fichiers à échanger avant leur envoi et bien sur en utilisant un mot de passe robuste (au moins 8 caractères, un caractère spécial, un chiffre et une lettre majuscule).

Accès aux ressources du réseau

Avec le télétravail, les employés, pour réaliser leurs activités, ont besoin d'accéder à distance aux ressources internes de l'organisation.
Si des mécanismes de sécurité ne sont pas correctement conçus et implémentés, il pourrait se poser un problème d'accès non autorisé aux ressources de l'organisation. Ces ressources pourraient aussi bien être des données stratégiques, des données personnelles des employés ou même des données personnelles des usagers et partenaires.

Les organisations n'ayant pas pris de dispositions suffisantes pour garantir la sécurité de l'accès à ces ressources pourraient avoir des problèmes de divers ordres:

- Non conformité aux lois et règlements applicables, pouvant entrainer de lourdes amendes ;
- Plaintes des usagers et partenaires, pouvant conduire à la perte de confiance des usagers;
- Informations stratégiques utilisées par les personnes malveillantes;
- Réputation ternie, pouvant facilement entrainer la faillite de l'organisation (notamment pour des entreprises de services).

De nos jours, l'accès au ressources internes de l'entreprise ne se fait plus seulement à l'aide d'un ordinateur, mais aussi à l'aide de terminaux mobiles (smartphones, tablettes). Par ailleurs, avec la naissance du concept **BYOD (Bring Your Own Device)** qui est appliqué dans de nombreuses organisations, les employés ont la possibilité d'utiliser leurs propres appareils mobiles pour accéder aux ressources. Il est donc indispensable de penser aussi à sécuriser cette porte d'entrée au réseau de l'organisation.

Que devons-nous faire?

Afin de sécuriser l'accès à leurs ressources, les organisations devraient penser aux pistes de solutions suivantes:

- Utilisation d'une solution VPN sécurisée, c'est-à-dire ayant les caractéristiques suivantes: être un VPN SSL, utiliser l'authentification et le chiffrement SSL, utiliser des certificats valides;
- En cas d'utilisation d'adresses IP publiques, s'assurer que celles-ci ont fait l'objet de tests d'intrusion;
- Sécuriser les fichiers au sein du réseau interne en donnant des accès aux collaborateurs en fonction de leur entité au sein de l'organisation (Direction, Département) de manière à ce que seuls les membres d'une entité aient accès aux fichiers de ladite entité;
- En cas d'utilisation d'un terminal mobile comme modem de connexion internet, changer le mot de passe par défaut lors du partage de la connexion. Le mot de passe devrait être fort (voir la partie « *Disponibilité et sécurité des portails web* » de cet article pour les caractéristiques d'un mot de passe fort);
- En cas d'utilisation d'un terminal mobile, installer un client EndPoint d'un antivirus, et indiquer un moyen pour mettre à jour cet antivirus à une fréquence journalière;
- Encourager les collaborateurs à n'utiliser les terminaux de l'organisation que pour des raisons professionnelles;
- Implémenter des mécanismes d'authentification multi-facteurs sur les terminaux alloués aux collaborateurs pour le télétravail;
- Mettre en place un protocole de sécurité permettant d'autoriser ou non les appareils mobiles des employés à se connecter au SI de l'organisation.

Disponibilité et sécurité des portails web

Avec le télétravail et même avant, certaines organisations ont mis à la disposition de leurs usagers et partenaires des portails web accessibles via internet, afin de leur permettre de rester en relation et d'effectuer des procédures/opérations tous en limitant les déplacements de personnes.
De telles initiatives sont à féliciter, mais il est toutefois à noter que si des mécanismes de sécurité ne sont pas correctement conçus et implémentés, il pourrait se poser un problème d'accès non autorisé aux ressources de l'organisation.
Ces ressources pourraient aussi bien être des données personnelles des usagers et partenaires que des données sensibles de l'organisation.
Des personnes malveillantes pourraient également empêcher les usagers d'accéder à ces plateformes par des attaques de type dénie de service.

Les organisations n'ayant pas pris de dispositions suffisantes pour éviter cela pourraient avoir des problèmes de divers ordres (voir la rubrique « *Accès aux ressources du réseau* » pour les risques encourus).

Disponibilité:
Les portails web doivent être disponibles chaque fois que l'usager a besoin de l'utiliser.

Confidentialité et intégrité:
En temps que porte d'entrée de l'organisation, les portails web de l'organisation doivent garantir la confidentialité et l'intégrité. En effet, une forte augmentation des cyber attaques a été relevée depuis le début de cette pandémie.

Que devons-nous faire?

Afin d'avoir un portail web disponible, l'organisation devrait mettre en place les mesures suivantes:

- Disposer d'un serveur de secours géographiquement éloigné.
- S'assurer de faire des sauvegardes régulières (en fonction de l'utilité du portail, les sauvegardes peuvent être faites quotidiennement, à chaque heure, ou répliquée en temps réel);
- S'assurer d'avoir une source d'énergie de secours (serveurs connectés à un onduleur et un groupe électrogène);
- Garder une copie des données sauvegardées sur deux sites géographiquement éloignés.

Afin d'avoir un portail web sécurisé, l'organisation devrait par ailleurs mettre en place les mesures suivantes:

- Implémenter un certificat SSL sur le serveur web : ceci permet le chiffrement des données échangées entre le navigateur et le serveur web;
- Ne laisser ouverts que des ports utilisés: les ports non utilisés ne devraient pas être ouverts sur le serveur web;
- Utiliser des protocoles sécurisés pour l'échanges des données (exemples: SSH, SFTP, …);
- Utiliser l'authentification à double facteur pour la connexion au portail web;
- Définir des paramètres de sécurité des mots de passe au moins conformes aux bonnes pratiques tel que décrits dans le tableau ci-dessous:

Paramètres	Valeurs
Longueur minimale	8
Complexité	Chiffre, majuscule, minuscule & caractères spéciaux, pas plus de 3 caractères consécutifs peuvent être utilisés
Nombre maximum de tentatives infructueuses	6
Durée de verrouillage du compte	15 minutes
Historique de mot de passe	8
Durée de vie minimum	1 jour
Durée de vie maximum	90 jours
Nombre de sessions simultanées	1

Messagerie électronique

A cause des informations échangées, la messagerie électronique d'une organisation constitue une mine d'or en terme d'informations sur l'organisation. Avec les mesures de distanciation sociale, les systèmes de messagerie électronique prennent une place de choix dans nos systèmes d'information. Il est donc important de choisir une messagerie électronique sécurisée.
Ce d'autant plus que les messageries électroniques sont principalement la cible de cyber attaques telles que: l'interception d'emails envoyés, les attaques de type phishing pour pénétrer le système de l'organisation, les attaques de type FOVI (Faux Ordres de Virement).
D'après Interpol, ce dernier type de cyber attaque a occasionné plus d'un milliard de dollars de pertes en 2018 seulement et demeure assez méconnu pourtant plusieurs cas ont été enregistrés au Cameroun.

Les signes suivants peuvent vous indiquer que vous subissez une attaque de type FOVI:

- Une demande de virement, non planifiée, au caractère urgent et confidentiel : dans ce cas, contacter son interlocuteur habituel avec les coordonnées connues de la société;
- Un changement de coordonnées téléphoniques ou mails;
- Un contact direct d'un escroc se faisant passer pour un membre de la société ou un responsable qui va faire usage de flatterie ou de menace dans le but de manipuler son interlocuteur;
- Pour asseoir sa crédibilité et usurper une fonction, l'escroc apportera une abondance de détails sur l'entreprise et son environnement : données personnelles concernant le chef d'entreprise, ses collaborateurs, ...

Que devons-nous faire?

Afin d'avoir un système de messagerie électronique sécurisé, les organisations devraient:

- Utiliser une authentification multi-facteur pour la messagerie électronique;
- Chiffrer les messages de bout à bout afin qu'en cas d'interception par un hacker, le message ne soit pas lisible;
- Savoir où sont stockées les données personnelles et avoir la possibilité de les supprimer soit même en cas de besoin;
- Renforcer la sensibilisation des utilisateurs pour qu'ils ne divulguent pas leurs mots de passe et soient vigilants en cas d'emails piégés / Spams.

Pour ce qui est du FOVI, les mesures suivantes devraient être prises:

- Rappeler à l'ensemble des collaborateurs la nécessité d'avoir un usage prudent des réseaux sociaux privés et professionnels. Les alerter sur l'importance de ne pas y divulguer d'informations concernant le fonctionnement de votre organisation;
- Sensibiliser régulièrement l'ensemble des employés des services comptables, trésorerie, secrétariats, standards, de ce type d'escroquerie. Prendre l'habitude d'en informer systématiquement les remplaçants sur ces postes;
- Instaurer des procédures de vérifications et de signatures multiples pour les paiements et les changements de coordonnées bancaires;
- Rompre la chaîne des mails pour les courriers se rapportant à des virements en saisissant soi-même l'adresse habituelle du donneur d'ordre;
- Maintenir à jour le système de cyber sécurité.

Que faire en cas d'attaque FOVI ?

1) Demander immédiatement à la banque le retour des fonds;
2) Déposer une plainte auprès des services de police et de gendarmerie, en apportant un maximum d'éléments.

Sensibilisation des utilisateurs

L'être humain est le maillon faible de tout système de cyber sécurité. A cet effet, un hacker pourrait profiter de l'inattention d'un collaborateur pour introduire un code malveillant sur son poste, puis sur le réseau, voler des identifiants, des données personnelles ou stratégiques et éventuellement extorquer de l'argent. A titre d'exemple, les utilisateurs étant particulièrement craintifs en cette période de pandémie, certains escrocs se font passer pour des représentants de l'OMS (Organisation Mondiale de la Santé) pour obtenir des renseignements confidentiels via le phishing.

Que devons-nous faire?

Afin de réduire le risque d'être victime d'attaques de type phishing, les organisations devraient tenir compte des recommandations suivantes:

- Disposer d'une charte d'utilisation des systèmes informatiques afin que les collaborateurs soient au courant de leur responsabilité en matière de cyber sécurité au sein de l'organisation. Cette charte doit être signée par tout nouveau collaborateur à l'embauche, ainsi que par les prestataires;
- En fonction de la nature des prestations, les prestataires doivent signer un accord de confidentialité;
- Effectuer la sensibilisation continue: produire et partager 1 à 2 communications cyber-sécurité par semaine vers les collaborateurs afin de leur rappeler les bonnes pratiques (éviter d'utiliser les adresses personnelles pour des échanges professionnels, ne pas cliquer sur des liens contenus dans des mails provenant d'une adresse suspecte, avoir des mots de passe robustes, privilégier les sites officiels pour avoir des informations sur la pandémie, téléchargements uniquement sur les sites officiels des éditeurs, remonter systématiquement tout cas suspect, …);
- Prévoir des quizz pour tester les connaissances des utilisateurs. Récompenser les utilisateurs ayant de bons scores aux quizz de cyber sécurité, ceci va encourager les autres à d'intéresser à cette importante problématique;
- Concevoir des e-learning de formations pour les nouveaux collaborateurs, ainsi qu'au moins une par an pour tous les collaborateurs;
- Etudier la possibilité d'utiliser des *serious games de cyber sécurité*. Les serious games sont des jeux qui captent l'attention du joueur et déclenchent la prise de conscience en matière de cyber sécurité. Ils peuvent avoir un impact fort sur les utilisateurs en matière de sensibilisation.

Projets de digitalisation

La **digitalisation** est le procédé qui vise à transformer un objet, un outil, un processus ou un métier en un code informatique afin de le rendre plus performant.
L'efficacité opérationnelle, l'amélioration de la connaissance et de la satisfaction des usagers, l'amélioration de la relation fournisseurs, la réduction des couts sont tous des objectifs atteignables par une digitalisation des pratiques.
Compte tenu de ces opportunités offertes par la digitalisation, le Cameroun a lancé un « Projet d'accélération de la transformation numérique du Cameroun », répondant ainsi aux orientations du Président de la République qui à travers son adresse à la jeunesse le 10 février 2015 a déclaré à ce propos : « l'évolution technologique a changé le cours des choses. La nouvelle économie est dominée par l'informatique ».

Cette pandémie a permis plus que jamais de se rendre compte de la nécessité d'accélérer ce processus de digitalisations de nos organisations. En effet, la mise en place du télétravail est beaucoup plus aisée pour les organisations ayant un bon niveau de digitalisation.

Que devons-nous faire?

Les organisations doivent saisir l'opportunité de la pandémie du COVID-19 pour élaborer un plan de digitalisation et se lancer dans des projets de digitalisation afin de tirer entre autres les bénéfices suivants:

- Briser les barrières géographiques: l'usager peut accéder aux services peu importe sa position géographique et un employé peut traiter des dossiers à distance.
- Fiabilité: La digitalisation permet de réduire considérablement les erreurs humaines, les fraudes et les couts.
- Cible: L'information et les contenus dématérialisés peuvent toucher un plus grand nombre de personnes et sans réelle limite;
- La collaboration entre personnes, les contenus partageables et modifiables en temps réel par tous permettent de travailler sur un même projet bien plus facilement;
- L'automatisation de tâches répétitives permet une meilleure optimisation du temps de travail pour se focaliser sur les travaux à réelle valeur ajoutée.

Pour les projets de digitalisation, les organisations devraient tenir compte des points suivants:

- Définir en amont une stratégie de transformation digitale;
- S'assurer de l'implication forte du top management et non pas seulement des informaticiens;
- Sensibiliser les parties prenantes avant la digitalisation et leur expliquer les bénéfices pour eux;
- Mettre en œuvre une démarche de gestion des projets efficace et ne pas hésiter à passer par l'étape de prototypage qui permettra de mieux comprendre le besoin e les spécifications et contraintes du livrable final.
- Anticiper dès à présent la réponse aux risques inhérents:
  - Risque de résistance au changement: mettre en place un processus de **conduite du changement** avant, pendant et après le projet de digitalisation;
  - Risque de dysfonctionnements techniques : mettre en place une équipe de maintenance et résolution des incidents et une procédure de gestion des changements;
  - Risque de cyber attaques: les processus étant digitaux, il existe désormais un risque de cyber attaques et des mesures doivent être prises pour y faire face.

Conclusion

Dans le domaine des systèmes d'informations, la pandémie du COVID-19 apporte avec elle de nombreuses menaces et opportunités pour lesquelles les organisations doivent être sensibilisées afin d'en tenir compte et mettre en place des mesures pour y faire face.

Dans ce document, nous avons abordé les problématiques suivantes et proposé des pistes de solutions:

- L'importance du **Plan de Continuité des Activités** et surtout de tests périodiques de ce dernier : il y va de la survie de l'organisation face à un sinistre majeur;
- La vulgarisation des **outils de téléconférence et de partage de fichiers** pour faciliter le télétravail: il est impératif de tenir compte de mesures de sécurité telles que le chiffrement de bout en bout et la protection des données personnelles;
- La poursuite de la sécurisation des **réseaux de l'organisation**: utiliser des solutions VPN sécurisées, mettre à jour les patchs de sécurité et les antivirus et mettre en place un mécanisme d'authentification multi-facteur pour les appareils mobiles;
- La mise à disposition de **plateformes web** d'accès distant pour les collaborateurs, clients et partenaires: pour assurer la disponibilité, effectuer des sauvegardes régulières et avoir une source d'énergie de secours; Pour assurer la sécurité, utiliser l'authentification à double facteur et imposer des mots de passe forts;
- L'importance de sécurisation des plateformes de **messagerie électronique**: utiliser le chiffrement de bout en bout, utiliser l'authentification à double facteur;
- La **sensibilisation** continue des utilisateurs sur la cyber sécurité: mettre en place un programme de sensibilisation des utilisateurs à la cyber sécurité (communication régulière, e-learning, quizz, serious games de cyber sécurité, …);
- Les **attaques FOVI** (Faux Ordres de VIrement): sensibiliser régulièrement les employés des services comptables, trésorerie, secrétariats, standards à ce sujet, maintenir à jour le système de cyber sécurité;
- La mise en évidence de l'importance de la **digitalisation** des processus des organisations: les organisations devraient saisir cette opportunité pour mettre en place un plan de digitalisation porté par le top management et des pratiques de gestion des projets aux normes internationales.

La mise en œuvre des différentes recommandations que nous avons portées à votre attention peut s'avérer être couteuse en temps et en budget, toutefois nous pensons que pour la plupart, des solutions intermédiaires peu couteuses peuvent être mises sur pied en attendant de disposer des ressources suffisantes.

Le CENADI se tient prêt à vous accompagner et à vous conseiller dans la mise en œuvre de ces différentes recommandations.

Contacts

Le Centre national de développement de l'informatique (**CENADI**) est l'organe de l'Etat du Cameroun rattaché au Ministère des Finances chargé de la mise en œuvre de la politique informatique du gouvernement et du conseil du gouvernement et des entreprises publiques et parapubliques, voire privées, en matière d'informatique et de téléinformatique.

De ce fait, il offre les prestations suivantes :

- Accompagnement des administrations publiques ;
- Maîtrise d'ouvrage déléguée pour les grands projets informatiques ;
- Promotion du développement de l'économie numérique ;
- Hébergement des données et applications stratégiques de l'Etat ;
- Recherche, Développement et coopération multiforme ;
- Conduite des audits des systèmes informatiques de l'Administration ;
- Certification de la qualité des prestations, des produits et fournitures informatiques.

Dr Chantal Marguerite MVEH

Directeur du Centre National de Développement de l'Informatique (CENADI)

Email: chantal.mvehz@minfi.cm
Téléphone: +237 222 220 766