MAI 2020

PCA 2.0, résultat du Covid-19

Article élaboré par :

Didier SPELLA

Mohamed AMRI

Mohamed SAAD

Sommaire :

1. Introduction :

La propagation du Coronavirus Covid-19 provoque une crise sanitaire, sociale et économique sans précédent, qui touche tous les secteurs d'activité et toutes les sociétés.

Notre génération a connu de nombreuses crises économiques et financières. Avec l'épidémie du virus Covid-19, elle traverse sa première crise sanitaire de grande ampleur, à laquelle elle semblait bien mal préparée.

Depuis plusieurs mois, de nombreuses communautés d'expertise alertent sur d'autres types de risques auxquels nous sommes sans nul doute aussi mal ou peu préparés : les risques liés aux changements climatiques, les risques liés au développement du numérique, pour ne citer qu'eux.

Si ces crises sont inévitables, soyons réalistes : l'objectif de l'ensemble des dirigeants de la planète doit être d'en minimiser les impacts afin que la société puisse continuer à fonctionner, même en mode dégradé. Une activité normale devra bien pouvoir reprendre au bout d'un certain temps. On parle alors de Résilience.

Cette situation inédite a des impacts sur la charge et la nature du travail des entités chargées des systèmes d'information et de la transformation digitale, qui ont dû prendre dans l'urgence des actions pour assurer la continuité des activités vitales des entreprises par la mise en œuvre du plan de continuité d'activité (PCA).

Par ailleurs, la pandémie actuelle devra inciter les organisations à repenser leur transformation digitale dans une perspective de digitalisation par défaut des processus opérationnels et des services assurés aux clients, quand l'activité s'y prête.

Cette digitalisation nécessite le renforcement des capacités des infrastructures et de la cybersécurité pour supporter les processus et les services précisés ci-dessus dans des conditions de performance et de sécurité acceptables.

Elle permettra également, grâce au télétravail, de garantir la santé et la sécurité des collaborateurs et des clients et d'améliorer leurs conditions de travail. En effet, les réunions en présentiel devront être organisées à titre exceptionnel et remplacées par des réunions effectuées en ligne à chaque fois que c'est possible.

Mais cette nouvelle situation comporte des risques pour les entreprises, notamment pour celles qui n'ont pas pris les mesures nécessaires en matière de cybersécurité.

Dans le cadre de la préparation de la phase de déconfinement, avec ses incertitudes quant aux délais nécessaires pour revenir à une situation « normale », cet article vise à recenser les principales recommandations opérationnelles d'ordre informatique à suivre pour, d'une part, assurer la protection des équipements et des collaborateurs et, d'autre part, accompagner l'entreprise dans cette période.

L'article aborde les thèmes suivants :

- Cybersécurité
- Plan de Continuité d'Activité
- Télétravail
- Situation Post-Confinement
- Nouveaux enjeux

2. Cyber sécurité :

La propagation des cyberattaques (vol de données, ransomware, vol d'identifiants, etc.) et l'augmentation des menaces qui profitent de la situation actuelle d'inquiétude et d'incertitude nécessitent des actions de renforcement de la protection en repensant l'architecture de sécurité et en appliquant les correctifs pour se prémunir des vulnérabilités découvertes par les éditeurs ou les constructeurs.

Le développement de services digitaux (egov, etc.) nécessite de prendre des mesures de sécurité car cela augmente le nombre d'entrées d'attaques potentielles (API, third party service, etc.).

Les principales recommandations concernant la cybersécurité sont :

- Allouer les ressources nécessaires pour mettre à jour les postes de travail, les serveurs, etc. avec les derniers patchs des logiciels anti-virus ou de la protection des points d'accès.
- Renforcer la cybersécurité pour permettre aux collaborateurs de faire du télétravail d'une manière productive.
- Acquérir des outils ou faire appel à des entreprises spécialisées pour détecter les menaces qui pèsent sur les postes de travail à distance, les serveurs etc., et les neutraliser.
- Lancer des campagnes de sensibilisation des collaborateurs autour du développement de la culture de la sécurité, afin d'accroitre la vigilance et mieux protéger les ordinateurs des cyberattaques, en donnant des exemples concrets :
    - Méthodes de traitement des courriers d'apparence officielle
    - Organisation de fraudes massives concernant la vente de biens recherchés.
- Identifier les risques et les contraintes dus à l'utilisation d'équipement professionnel dans un cadre personnel et/ou familial et apprendre à séparer les usages professionnels et personnels. L'environnement réseau à la maison n'est pas aussi bien sécurisé que celui de l'entreprise.
- Créer une cellule chargée de collecter les incidents et les suspicions d'incident de sécurité.
- Face à l'absence de sauvegarde dans certaines situations, mettre en œuvre une stratégie cohérente correspondant aux besoins de l'entreprise.
- Mettre en place une administration et une supervision des postes de travail connectés à distance.
- Elaborer un guide et une charte de télétravail.
- Elaborer un tableau de bord de suivi de la cybersécurité.
- Diagnostiquer et mettre à jour les postes qui étaient dédiés au télétravail et planifier leur accès au réseau local de l'entreprise pour éviter les phénomènes de saturation des serveurs et du réseau.
- Alerter sur la recrudescence de fausses applications sur mobile : par exemple de fausses cartographies de la propagation du coronavirus qui permettent d'accéder au système d'information de l'entreprise.

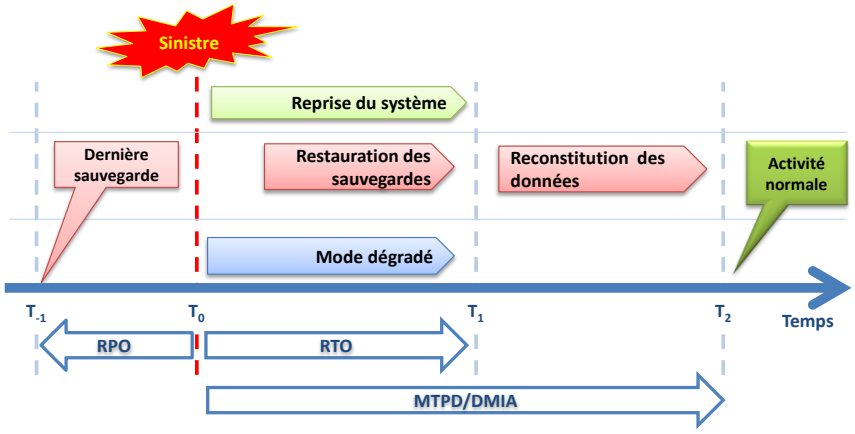
3. Plan de Continuité d'Activité :

1. La norme ISO 22301 :

Une norme nous aide pour bien prendre en compte ces problématiques de reprise d'activité. Cette norme est la norme ISO 22301. Celle-ci spécifie les exigences nécessaires pour planifier, déployer, mettre en œuvre, exploiter, surveiller, revoir, maintenir et améliorer en permanence un système de gestion documenté. Elle permettra ainsi de réduire la probabilité d'occurrence d'un événement désastreux, de s'y préparer, d'intervenir et de récupérer après la survenance d'incidents perturbateurs quels qu'ils soient.

Les exigences spécifiées dans la norme ISO 22301 sont génériques et prévues pour s'appliquer à toutes les organisations (ou parties de celles-ci), indépendamment du type, de la taille et de la nature de l'organisation. La portée d'application de ces impératifs dépend de l'environnement opérationnel de l'organisation et de sa complexité, et c'est à la charge de toute institution de les mettre en place , tout en les adaptant à son contexte. La liste des exigences ci-dessous n'est pas exhaustive :

- INS.MCA.02 : SMCA - Politique SMCA
- ENR.MCA.03 : SMCA - Domaine d'application
- INS.MCA.09 : SMCA - Guide méthodologique
- PRO.PS.06 : Procédure Management des Risques
- Démarche d'appréciation des risques
- Analyse d'impact sur l'activité (Business Impact Analysis)
- Priorités et délais de reprise des activités :



La démarche ISO 22301 va au-delà de la mise en place d'un PCA, s'apparentant plus à un Système de Management de la Continuité d'Activité (SMCA), appelé aussi BCMS (Business Continuity Management System), qui vise à faire vivre un système avec les audits adéquats, les revues nécessaires, sous le leadership du Top Management et, enfin, vers un système qui suit le processus d'amélioration continue tel que défini par W.E. Deming, dont toutes les normes ISO se sont inspirées.

2. Cas COVID-19 :

Après la phase de gestion du confinement, qui a nécessité l'activation du Plan de Continuité d'Activité, les enjeux aujourd'hui pour les entreprises sont, d'une part, de définir les modalités de gestion de la phase transitoire entre la période de déconfinement progressif et un semblant de retour à la normale et, d'autre part, de mener une réflexion sur la stratégie post Covid-19. Cette réflexion devra être basée sur différents scénarios possibles, compte tenu des :

- Incertitudes actuelles au niveau sanitaire, social et économique.
- Incertitudes relatives aux conditions de reprise progressive d'activité qui seront décidées par les pouvoirs publics.

La phase transitoire nécessitera l'activation du plan de reprise d'activité alors que la période post Covid-19 déclenchera le plan de retour à la normale :

- Revue du Plan actuel de Continuité d'Activité (PCA) en tenant compte de la nature de la pandémie : propagation du virus, impacts sur les secteurs d'activité, etc.
- Etablissement d'un nouveau PCA basé sur différents scénarios possibles tenant compte des incertitudes citées ci-dessus :
    - Evaluation de la phase de confinement et les leçons apprises.
    - Revue de la capacité des fournisseurs de service (télécoms, hardware, maintenance…).
    - Disponibilité des dispositifs nécessaires aux mesures sanitaires (masques, gels hydroalcooliques, thermomètres distants, gants…)
    - …
- Etude de l'opportunité de renforcer l'utilisation du Cloud pour bénéficier de ses avantages, notamment le dimensionnement des ressources en fonction des besoins et de l'évolution de la situation.

4. Télétravail :

Le recours massif au télétravail dû au confinement généralisé a été adopté et à la grande satisfaction des collaborateurs et des entreprises qui n'étaient pas nécessairement favorables à ce type d'activité à grande échelle. Cela a nécessité la mise en place dans l'urgence d'un aménagement du temps de travail et l'adoption de nouveaux modes de travail, ainsi que des pratiques et des outils de collaboration à distance.

Il est également important de souligner que le télétravail est un changement majeur pour les collaborateurs et nécessite un accompagnement spécifique en termes de coaching, de support et d'assistance. Cet accompagnement fait partie des clés de la réussite du télétravail.

En cette période, le digital a été vital pour faciliter la continuité des activités des entreprises et la vie des clients et des collaborateurs.

Compte tenu des incertitudes citées ci-dessus, il faudra mener des actions pour assurer le télétravail à grande échelle entre les collaborateurs mais également privilégier les interactions à distance avec les clients, quand l'activité s'y prête, et renforcer les services en ligne :

- Acquérir et fournir aux collaborateurs des outils digitaux pour une mobilité et une connectivité sécurisée.
- Renforcer le développement des services digitaux afin d'assurer la continuité des activités et répondre aux besoins et aux attentes des clients.
- Décontaminer régulièrement les locaux, les sols et les surfaces.
- Généraliser le télétravail et prendre en compte les cas de vulnérabilité liée à la santé.

- Limiter les réunions au strict nécessaire dans le respect des règles de distanciation et des gestes barrières.
- Identifier les travaux éligibles à être effectués à distance.
- Mettre à niveau l'infrastructure technique pour permettre le télétravail dans des conditions de performance et de sécurité acceptables et pour refléter les exigences opérationnelles actuelles ou d'autres évènements similaires.
- Mettre à niveau les infrastructures matérielles et logicielles pour supporter le télétravail des collaborateurs à grande échelle et anticiper ainsi une éventuelle deuxième vague de la pandémie ou d'autres évènements similaires.
- Organiser le télétravail en tenant compte de l'expérience acquise s'il est amené à se poursuivre.
- Maintenir l'engagement des collaborateurs en établissant avec eux une relation de confiance.
- Maintenir une dynamique et une solidarité de groupe grâce à des communautés virtuelles.
- Faciliter la collaboration entre collègues en télétravail et dans les bureaux.
- Faciliter le partage des connaissances entre les collaborateurs et les équipes.
- Informer régulièrement les collaborateurs sur les orientations de l'entreprise et les projets à venir.

N.B. : Selon une étude Gartner du 30 mars 2020, 74% des directeurs financiers interrogés s'attendent à faire travailler au moins 20% de leurs salariés de façon permanente après la crise.

5. Situation Post-Confinement :

Une préparation au jour « J » s'avère être un facteur clé de succès pour la réussite d'un retour en toute confiance, mais surtout dans l'efficacité et l'efficience.

Nous présentons ci-dessous un benchmark des mesures de déconfinement de différents pays :

Critère	Belgique	France	Suisse	UAE
Date de début	04/05/2020	11/05/2020	27/04/2020	04/04/2020
Par étapes	Oui	Oui	Oui, (27/4, 11/5, 8/6)	Oui
Distance sociale	Oui	Oui	Oui	Oui (1,2m)
Port du masque	Oui	Oui	Oui	Oui
Télétravail	Reste la norme	3 semaines au min	Recommandé	Recommandé
Aller au travail	Oui. Protection et distanciation	Oui. Avec horaires décalés	Autorisation progressive	Oui, (30% effectif) masque, test °C
Rassemblements	Non	Non	08/06/2020	Oui (<6p)
Transports en commun	Oui, sous conditions	Oui, sous conditions	Oui	Non
Voyage domestique	Oui, (avec masque si +12 ans)	Oui (<100 Km)	Oui	Oui, avec masque (<4 p / véhicule)
Rester chez soi	Oui, si possible	Oui, si possible	Personnes vulnérables	Personnes vulnérables
Tests généralisés	Oui, via médecin généraliste	Oui, 700 000 par semaine	Oui, +autotests	Oui, +autotests
Activités sportives	Oui, cafétérias & vestiaires fermés	Oui, individuelles et en plein air	Oui, activités sans contact physique	Oui, près du domicile -3h, -4p, 2m
Ouverture des écoles	18/05 partielle et progressive.	Partielle et progressive	11/05 primaire, 08/06 le reste	Non
Autorisation déplacement	Non	Non	Non	Non (6h-22h)
Commerces ouverts	Ceux ouverts + Alimentation et fournitures pour masques	Tous, sauf cafés, restaurants et marchés (après accord des autorités locales)	Oui. Masque obligatoire	Oui, le 28/04, 30% capacité, masque (+12,-60 ans), test température
Café & restaurants	Non	Non	Non	Oui, sous conditions
Voyage international	Non	Non	Non	Non

Benchmark préparé par M. Yahya ARROUBAT, RSSI, RPCA, Bourse de Casablanca

Il est important de noter que le déconfinement progressif énoncé par différents gouvernements doit également être accompagné de mesures mises en place par les institutions, mais aussi par les ménages. Nous citons quelques dispositions à mettre en place par les entreprises :

- Réduction du taux d'occupation des locaux :
    - Etablissement de listes du personnel avec 3 priorités :
        - P1 : Personnel obligatoire en présentiel.
          Ces collaborateurs peuvent opérer un système de roulement ou d'astreinte avec d'autres personnes de même compétence.
        - P2 : Personnes continuant à faire du télétravail qui seront amenées à regagner leurs bureaux dans un délai minimum de 3 à 4 semaines.
        - P3 : Personnes vulnérables dont la présence sur site n'est pas indispensable et qui peuvent continuer à faire du télétravail.
- Veiller à la mise en place des mesures sanitaires nécessaires dans les locaux.
- Eviter les cantines et tous les lieux de rassemblement.
- Limiter les réunions : privilégier les outils de eMeetings. Le cas échéant, respecter la distanciation.
- Préparer les scénarios nécessaires à déclencher devant tout risque de contamination d'un collègue, ou d'un membre de la famille d'un collègue.
- Garder le Log des mesures de températures.
- Veiller au respect de l'anonymisation des données de santé et de la protection des données personnelles.
- Alerter les autorités au cas où des cas sont avérés, ou même en cas de doutes de contamination.
- Garder le contact avec le personnel non concerné par le télétravail afin qu'il ne se sente pas marginalisé.
- …

Cette liste non exhaustive se veut être une bonne base pour observer les bonnes pratiques et les facteurs clés de succès en vue d'éradiquer ce fléau et retrouver une vie normale.

6. Nouveaux enjeux :

Afin de comprendre ce qui se passe, nous pensons qu'il est nécessaire de modéliser ces crises afin de mieux en appréhender les enjeux. Nous serons ainsi plus en mesure de nous en protéger et de les gérer au mieux.

Ces crises comportent plusieurs caractéristiques communes :

- Absence de frontières géographiques ;
- Propagation rapide ;
- Propagation aléatoire ;
- Impact global ;
- Multi-activités ;
- Multi-secteurs ;

Ces différentes caractéristiques nous amènent à identifier des limites au BCP et DRP. En effet, les BIA ne couvrent pas de telles caractéristiques. Les prérequis sont généralement les suivants :

- Les risques couverts sont en général assez co-localisés (glissement de terrain, incendie, inondation, etc.) ;
- Les prestataires ne sont pas inclus dans la crise (pas dans le même lieu, pas la même activité, pas les mêmes ressources, etc. ;
- Les personnels ou une partie peuvent se déplacer ;
- Les organisations étatiques sont en fonctionnement nominal ;
- …

En fait, nous avons pris le mot crise pour parler de mode dégradé. Nos procédures de secours ne permettent d'aborder les problèmes qu'au travers de ce prisme réducteur.

Il faut travailler sur un spectre plus large et global.

Nos analyses doivent prendre en compte les notions suivantes :

- Entreprise étendue ;
- Crise étendue pour ne pas dire globale ;
- Degré d'autonomie.

Nos plans doivent :

- Avoir une approche globale stratégiquement, tactiquement et opérationnellement parlant ;
- Prendre en compte les spécificités complètes de la structure ;
- Faire développer une conscience collective auprès des collaborateurs.

Les crises nous ont aussi amenés à revoir la dynamique de l'approche, qui se fait en 3 phases :

- Déclenchement de la crise ;
- Fonctionnement en mode crise ;
- Reprise d'activité en mode normal, ou sensé l'être.

Il est bon à ce niveau de considérer chacun de ces passages d'une étape à la suivante comme une augmentation du risque car nous nous retrouvons dans un état instable, propice aux criminels.

Ces transitions doivent être donc traitées avec le plus grand sérieux possible. Elles doivent être aussi élaborées en même temps pour permettre une amélioration continue. L'approche pourra donc s'appuyer sur la norme ISO 9001.

Il s'agit aussi de repenser nos approches de numérisation. Là aussi, il est nécessaire d'identifier les différentes phases de maturité de cette numérisation et de réfléchir à ce que pourraient être les prochaines étapes.

Nous en voyons trois principales :

Etape 1 : la numérisation des supports

Il s'agit de la toute première étape qui consiste à transformer tout type de support analogique en support numérique : les documents, les musiques ; en bref, tous les types possibles. L'humain a un usage plus pratique de ces supports.

Etape 2 : la numérisation des outils simples

Il s'agit de transformer, d'adapter les outils analogiques en outils numériques. La machine à écrire devient traitement de texte, la calculatrice, tableur, etc. Les machines-outils sont numérisées. L'humain devient un utilisateur.

Etape 3 : l'intégration des outils

Cette troisième évolution consiste à intégrer ces outils simples pour en faire des outils plus complexes en combinant différentes technologies : plate-forme numérique, communication, énergie. On y ajoute aussi les supports numérisés.

Nous voyons alors apparaître des outils complexes, utilisant plus ou moins bien les caractéristiques techniques de chacun de ces composants technologiques. Les concepteurs de ces outils proposent du confort par le biais de paramétrages mais nous ne pouvons parler de réel progrès. L'humain doit s'adapter à l'outil numérique.

Nous voyons bien la limite qu'offre ce modèle et beaucoup de ses contraintes sont apparues lors de cette crise, qui pourrait se doubler d'une cyber-crise, devenant alors une catastrophe pour les entreprises et les administrations.

Nous avons élaboré une 4ème étape qui ne suit plus cette évolution technologique mais va plutôt vers une évolution sociologique :

Etape 4 : l'intégration numérique

Par « intégration numérique », nous amenons le concept de concevoir des systèmes numériques totalement intégrés qui offrent notamment la personnalisation de tous ces outils et non pas uniquement un seul paramétrage. L'humain devient l'élément central de cette numérisation. Il peut choisir les outils qui lui sont nécessaires et utiles. Ces outils évolueront avec ses besoins. La personnalisation est effective.

7. Conclusion :

Malgré les circonstances actuelles, l'amélioration de l'expérience collaborateur et de l'expérience client (symétrie des attentions), facilitée par la transformation des organisations à l'ère digitale, devra rester au centre des préoccupations des entreprises pendant cette période et celle post covid-19.

A cet effet, il est recommandé d'organiser, pendant la période transitoire citée ci-dessus et celle post covid-19, des ateliers pour écouter les clients et les collaborateurs afin de recenser leurs besoins, leurs attentes et leurs contraintes en vue d'élaborer la feuille de route digitale pour le court, moyen et long terme :

- Informer en temps opportun les clients et les partenaires de l'écosystème sur la l'évolution de la situation des services assurés par l'entreprise.
- S'assurer que les collaborateurs disposent des ressources et du soutien nécessaire pour effectuer le télétravail et pour rester en bonne santé.
- Surveiller et mesurer l'efficacité des conditions de travail de l'entreprise.

A moyen terme, le télétravail et la poursuite de la transformation des organisations dans l'ère digitale ont des impacts, d'une part, sur la qualité de vie et l'expérience des collaborateurs, sur leur productivité et leur niveau de stress et, d'autre part, sur l'expérience des clients et des partenaires de l'écosystème et sur les processus opérationnels.

En effet, certaines pratiques expérimentées pendant cette période (télétravail, recours à des outils collaboratifs, etc.) peuvent se révéler pertinentes à conserver et à renforcer. Elles vont également contribuer, d'une part, à lever certains freins à la transformation digitale et à « disrupter » les approches traditionnelles du travail et du management et, d'autre part, à maintenir et développer l'innovation.

Compte tenu des incertitudes quant au délai nécessaire pour contenir le Covid-19, les entreprises devront, tout en gérant le court terme, développer de nouvelles approches humaines (empathie) du travail pour le long terme.

Par ailleurs, il est également opportun d'évaluer l'impact de la situation actuelle sur le business model des entreprises et/ou réinventer de nouveaux modèles.

Cela nécessite la mise en place des conditions nécessaires de cybersécurité et d'infrastructures résilientes.

Biographie des experts :

Mohamed SAAD est un acteur dans le monde des Technologies de l'Information depuis 1991, Digital Evangelist ; Président de l'AUSIM et Directeur du Pôle Ressources de la Bourse de Casablanca, il a opéré dans le secteur du service, de l'industrie et du bancaire. Sur le plan associatif, il est membre fondateur de Isaca-Casablanca, chapitre marocain de l'ISACA, Vice-Président de CCAM (Club de la Continuité d'Activité Marocain), membre du PMI. Il est diplômé de l'INSEA et détenteur d'un MBA, et des certifications CISA, PMP, CRISC, ISO 27001.Mohamed SAAD est l'auteur de plusieurs articles sur l'IT Gouvernance, les risques IT, le ROI IT, les standards et référentiels IT…

Mohamed AMRI - Directeur associé de l'institut Africain du Numérique

Docteur en Informatique de l'université de Clermont-Ferrand, il est expert en transformation digitale, en marketing digital et en systèmes d'information. Il a exercé la fonction de DSI dans les secteurs de la banque et de l'assurance. Il a également enseigné à l'IUT et au CNAM de Clermont-Ferrand.

Didier SPELLA - Dirigeant de MIRAT DI NERIDE - Expert en stratégie des entreprises et en cybercriminalité.

Co-fondateur de CMCS (Charente-Maritime Cyber Sécurité) dont la deuxième édition en 2019 a réuni près de 450 participants et plus de 60 intervenants pendant 3 jours à La Rochelle.

Responsable Bureau CLUSIR - Nouvelle Aquitaine Ouest (La Rochelle – Niort – Cognac). Référent Cyber Malveillance.

Ancien Officier Supérieur de l'Armée de l'Air, expert en réseau et continuité des Affaires dans une multinationale américaine, j'ai toujours été passionné par la problématique de la cyber sécurité et notamment le conflit qui peut exister entre le cybermonde et la sécurité. Comment pouvons-nous positionner l'être humain confronté au dilemme liberté-sécurité.