

TELECOMMUNICATIONS

CATEGORIE: Dépendance technologique

 En collaboration avec :

# Telecom

La transition numérique que viet actuellement notre société reposent sur les télécommunications et présent de très nombreuses *opportunités* pour les entreprises qui sont de plus en plus nombreuses à élaborer une stratégie digitale pour se positionner sur un marché ouvert au monde.

Toutefois, lors de l’élaboration de telles stratégies, il importe de ne pas sous-estimer les *risques*. La digitalisation envisagée se fait-elle de manière cyber-sécurisée ? Les aspects relatifs à la protection de la vie privée et des données à caractère personnel ont-ils été correctement évalués (GDPR,...) ? Les obligations légales en matière d’informations devant figurer sur les sites web ont-elles été respectées ? Le personnel est-il suffisamment formé et sensibilisé ?...

A ces risques inhérents à toute activité en ligne, s’ajoute le risque de la dépendance technologique : l’entreprise dépend de plus en plus des télécommunications (internet, téléphonie mobile, téléphonie fixe) pour son bon fonctionnement que ce soit pour ses moyens de paiement, sa gestion de la chaîne logistique, sa relation à la clientèle, sa gestion des ressources humaines, ses contacts avec ses fournisseurs, le traitement de ses dossiers, la gestion de sa réputation en ligne,…

Il est donc important d’évaluer le risque que pourrait représenter pour votre entreprise une interruption de vos moyens de télécommunications. Comment l’entreprise pourrait-elle gérer une interruption ou une dégradation significative de ses moyens de télécommunications ?

**Avertissement**

Les informations fournies par le présent document sont destinées à fournir des éléments de réflexion à l’employeur dans le cadre d’une gestion des incidents afin d'assurer la continuité des activités de l'entreprise. L’objectif n’est donc pas de se substituer aux autorités chargées de surveiller la sécurité du travail. Ces informations ne dispensent pas l’employeur de respecter les dispositions réglementaires qui sont susceptibles de s’appliquer pour chaque situation de travail spécifique.

Cela signifie que l’utilisation du présent document par l’employeur est toujours tributaire de son jugement pragmatique et qu’il lui appartient d’apprécier les éléments et les circonstances, en fait et en droit, auxquels l’employeur doit faire face dans les cas bien définis et concrets sur les lieux de travail.

Pour des interprétations lors de cas ou de situations concrètes, l'avis des fonctionnaires chargés de surveiller la réglementation relative à la sécurité du travail peut toujours être sollicité.

*Pour en savoir plus sur les différentes étapes, voir template “Gestion des incidents”, chapitre III.*

TELECOMMUNICATIONS

[I. Etape 1: Préparation (AVANT INCIDENT) 4](#_Toc57970225)

[1.1 : Placez un pilote dans l’avion 4](#_Toc57970226)

[1.2 : Connaissez vos risques 4](#_Toc57970227)

[1.3 : Mesures préventives 5](#_Toc57970228)

[II. Etape 2 : Notification et identification 7](#_Toc57970229)

[2.1 : Notification 7](#_Toc57970230)

[2.2 : Identification 7](#_Toc57970231)

[III. Etape 3 : Activation et traitement (INCIDENT) 8](#_Toc57970232)

[3.1 : Identifiez vos outils et moyens 8](#_Toc57970233)

[3.2 : **MESURES DE GESTION** 9](#_Toc57970234)

[IV. Etape 4 : Eradication 10](#_Toc57970235)

[V. Etape 5 : Desactivation 10](#_Toc57970236)

[VI. Etape 6 : Leçons acquises (post incident review) (APRES INCIDENT) 11](#_Toc57970237)

[6.1 : Contexte : informations relatives a l’incident 11](#_Toc57970238)

[6.2 : Evaluation de l’incident et leçons acquises 11](#_Toc57970239)

[VII. Annexes 15](#_Toc57970240)

[7.1 : Liste des contacts 15](#_Toc57970241)

[7.2 : Tableau 17](#_Toc57970242)

## Etape 1: Préparation (AVANT INCIDENT)

Voir également Risk Assessment et Risk Treatment.

### 1.1 : Placez un pilote dans l’avion

|  |
| --- |
| Qui peut dresser ce plan de gestion des incidents ?  Qui peut élaborer et gérer cette fiche ? |

*Voir Annexe VII, 7.2 : Tableau*

Dans les grandes structures, un groupe (idéalement pluridisciplinaire et inclusif) peut être constitué.

Dans les plus petites structures, il est possible qu’une seule et même personne soit désignée par la direction ou que la direction assume ce rôle elle-même. Dans ce cas, il est néanmoins conseillé de désigner un back up (une personne qui pourra le remplacer en cas d’absence, de maladie ou de départ).

Pensez à inclure votre service informatique (interne ou externe) si vous en disposez.

Assurez-vous de faire valider les procédures/le plan de gestion des incidents ainsi que la présente fiche?

### 1.2 : Connaissez vos risques

|  |
| --- |
| Avez-vous réalisé un Risk Assessment ?  Avez-vous réalisé un Risk Treatment ? |

*Voir Annexe VII, 7.2 : Tableau*

Pour que le plan de gestion des incidents puisse être efficace, l’entreprise doit avoir identifié, analysé et évalué ses risques. C’est l’objet du Risk Assessment (voir template). Il faut également que les mesures de traitement des risques soient connues, c’est l’objet du Risk Treatment (voir template).

Vu la forte dépendance de notre société aux télécommunications, chacun peut ressentir rapidement les conséquences d'une dégradation significative ou d’une interruption des services de télécommunication sur la continuité des activités de l’entreprise.

En fonction des activités de l’entreprise, vous pourriez notamment éprouver des perturbations comme :

* difficultés à contacter fournisseurs et clients,
* bases de données inaccessibles,
* (forte) dégradation ou interruption des services en ligne à la clientèle,
* impact sur la chaine logistique, dégradation ou interruption des activités en ligne,
* atteinte à la réputation,
* non-respect des délais,
* chaine de commandement perturbée,
* ...

La forte perturbation des lignes téléphoniques peut avoir diverses origines : une tempête, une coupure électrique, un flux anormal d’appel (suite à un attentat dans la localité par exemple),...

N’oubliez pas que le Risk Assessment (voir template) est un processus itératif et non pas une opération unique. Les réseaux télécoms, vos besoins et vos risques évoluent constamment.

Il vous faut également identifier les scenarios spécifiques. Par exemple :

##### Scenario 1. Téléphonie mobile ou fixe

L’entreprise n’a plus accès aux services de téléphonie fixe ou de téléphonie mobile. Ce scenario peut s’accompagner ou non d’une perte de connexion à internet. En cas de rupture de courant électrique, il est également possible que la téléphonie fixe tombe d’abord puis, au bout de quelques heures, que votre appareil ou les antennes qui vous desservent n’aient plus de batterie.

##### Scenario 2. Connexion à internet

L’entreprise éprouve une forte dégradation de sa connexion à internet ou n’a plus accès à internet. Il est possible que les moyens d’accès à internet via smartphone persistent mais les accès aux outils de l’entreprise (base de données, logiciels spécifiques etc.) peuvent être malaisés voire impossibles par ce biais.

### 1.3 : Mesures préventives

##### Scenario 1 : Téléphonie mobile ou fixe

**Redondance**

Si l’impact pour l’entreprise d’une interruption de la téléphonie fixe et/ou mobile peut être important, n’oubliez pas d’envisager des dispositifs de redondance efficaces (back up). Vous pourriez par exemple disposer de deux lignes téléphoniques fixes concurrentes (redondantes) ou de deux cartes SIM différentes. Cette redondance peut notamment être assurée par plusieurs opérateurs concurrents (au moins 2).

S’il s’agit de téléphonie fixe, pensez à demander à vos opérateurs si l’un d’eux loue son infrastructure auprès d’un autre opérateur pour vous servir : il est possible que votre bâtiment soit desservi par un seul et même “câble”. Si tel est le cas, vous paieriez deux fois mais sans disposer de redondance effective.

**Plan “B”**

Interne

Pensez à identifier toutes les procédures internes mais également toutes les chaînes de commandement (techniciens, IT, direction, etc.) qui reposent sur l’accès aux moyens de télécommunication (téléphonie fixe, mobile et internet) pour leur bon fonctionnement. Pensez à identifier des moyens alternatifs pour ces procédures et chaînes de commandement en cas de perte des moyens de télécommunication. Multipliez les canaux de communication possibles et si plus aucun de ces canaux de communication n’est accessible, pensez à indiquer vos instructions (télétravail,....).

Externe

N’oubliez pas également de donner à vos clients et fournisseurs différentes options pour vous contacter.

Liens utiles

* [SPF Economie](https://economie.fgov.be/fr/themes/energie/securite-dapprovisionnement/penurie-delectricite/questions-frequemment-posees/questions-frequemment-posees-0)
* [BE-Alert](https://be-alert.be/fr)

##### Scenario 2 : Connexion à internet

**Redondance**

Si l’impact pour l’entreprise d’une interruption de la connexion à internet peut être important, n’oubliez pas d’envisager des dispositifs de redondance efficaces (back up). Vous pourriez par exemple disposer de deux connexions concurrentes (redondantes). Cette redondance peut notamment être assurée par plusieurs opérateurs concurrents (au moins 2).

N’oubliez pas de demander à votre opérateur télécom, service de paiement,… :

* Si, pour vous servir, il loue tout ou partie de l’infrastructure auprès d’un autre opérateur...A défaut, vous pourriez avoir deux contrats auprès de deux opérateurs différents mais...pour la “même” connexion. Si celle-ci tombe, vous ne disposez pas de vrai back up. Une redondance effective implique de pouvoir disposer de plusieurs connexions distinctes qui ne dépendent pas l’une de l’autre.
* Si votre opérateur peut vous indiquer quel est le pourcentage d’accessibilité pendant vos heures d’ouverture et quel est le temps maximal d’interruption ou de perturbation enregistré durant les 12 derniers mois.
* Si l’infrastructure que votre opérateur vous propose présente des “Single Points of Failure” (SPoF) c’est à dire des points qui ne disposent pas de redondance.
* Si vous perdiez l’accès à l’électricité, au bout de combien de temps n’auriez-vous plus accès à internet? Votre opérateur télécom vous propose-t-il des solutions ? Renseignez-vous sur le fonctionnement du réseau de l’opérateur dans les “last miles”, la possibilité de prévoir des onduleurs,...
* Si vous pouvez bénéficier d’une assistance (helpdesk) 24/7.

**Résilience des réseaux (contrats)**

Vos contrats devraient contenir des “service level agreement” (SLA) qui identifient au moins certains aspects en rapport avec la résilience des réseaux. Pensez notamment à exiger :

* Garantie de disponibilité (%)
* Délais de dépannage en rapport avec les objectifs de temps que vous avez définis (voir 2.2.3)
* Mise en œuvre de solutions de backup (voir commentaire concernant l’effectivité réelle de cette mesure)
* Vous pourriez également transformer certaines obligations de moyen (votre opérateur fait “ce qu’il peut”) en obligation de résultat (si le résultat n’est pas atteint, des sanctions pécuniaires sont prévues).
* …

1. Etape 2 : Notification et Identification

### 2.1 : Notification

Il est essentiel de pouvoir détecter, identifier et qualifier/classer rapidement un incident afin d’en limiter l’impact sur la continuité des activités en activant la procédure adéquate. La personne qui reçoit la notification de l’incident qualifie l’incident sur base de critères prédéterminés.

Chaque employé doit signaler tout incident ou événement susceptible d’entraîner un incident, et ce dès que possible. Les clients et fournisseurs peuvent également signaler un incident.

Les moyens de signaler les incidents sont décrits dans le processus de gestion des incidents.

* Voir Etape 3. Activation et Traitement, Mesures de gestion

### 2.2 : Identification

2.2.1 : Identifiez les activites concernées

|  |
| --- |
| Quelles sont les tâches de l’entreprise qui doivent être maintenues pour assurer sa survie économique ?  Voir également le plan de gestion des activités (Business Continuity plan- BCP) et les objectifs de temps fixes (RTO,...) |
|  |

Pour vous aider identifier les processus et activités prioritaires, posez-vous les questions suivantes :

1. quelles sont les activités qui peuvent mettre en danger le personnel (ou les clients) ?
2. quelles sont les activités qui après quelques heures auraient un impact économique signifi-catif pour votre entreprise ? Après 24h ? 45h ? Une semaine ?

**LISTE DES ACTIVITES ESSENTIELLES**

| **Activité essentielle 1** |
| --- |
| Liste des éléments nécessaires pour la continuité de l’activité essentielle |
| Personnel clef |
| Information ou données clefs |
| Service informatique (hardware, software) nécessaire |
| Bâtiments |
| Personnes externes de contact (ressources) |
| Interdépendance avec d’autres activités (si oui, lesquelles) |

2.2.2 : Classez

La personne qui reçoit les renseignements (p. ex. Helpdesk) doit les classer, par exemple de la manière suivante:

1. **Faible** – aucun incident ne s’est produit, mais l’événement lié à un système, à un processus ou à une organisation peut déclencher la survenance d’un incident dans un avenir proche ou ultérieur;

2. Mineu**r** – incident qui n’a pas d’impact significatif sur la continuité des activités;

3. **Majeur** – incident qui peut avoir un impact significatif sur l’organisation, mais qui n’est pas encore considéré comme une crise;

4**. Crise** – incident qui peut avoir un impact significatif sur l’organisation et la continuité des activités.

2.2.3 : Identifiez les priorités

|  |
| --- |
| En cas d’interruption ou de dégradation de vos activités, quel est l’ordre de priorité des activités ?  Quels sont vos objectifs de temps ?  Voir également les Risk Assessment, Risk Treatment et plan de continuité des activités |

Lors de l’analyse relative à l’impact sur la continuité des activités, gardez à l’esprit qu’il est possible que toutes les activités ne fonctionnement pas forcément à 100% et que cela puisse être acceptable.

Vous avez défini vos activités essentielles impactées ? Il s’agit maintenant d’identifier l’ordre dans lequel ces activités devraient reprendre (certains services sont interdépendants des autres) et d’identifier les objectifs de temps estimé en les comparant aux objectifs fixés (voir Risk Assessment et Business Continuity Plan).

En fonction de ce qui précède, identifiez l’ordre dans lequel les actions doivent être entreprises afin d’assurer la continuité des activités essentielles. N’oubliez pas d’envisager l’interdépendance possible de certaines activités et de maintenir un dialogue constant avec le gestionnaire du plan de continuité des activités.

1. Etape 3 : Activation et Traitement (INCIDENT)

L’objectif principal est de réduire aussi rapidement que possible l’impact de l’incident pour la protection de la vie humaine puis pour la continuité des activités de l’entreprise.

### 3.1 : Identifiez vos outils et moyens

*Voir annexe VII, point 7.2 : Tableau*

En particulier, vos procédures (identification...), vos moyens de communication...

### 3.2 : Mesures de gestion

##### Scenario 1 : Téléphonie mobile ou fixe

##### Scenario 2 : Connexion à internet

La majorité des mesures que vous pouvez prendre sont des mesures préventives. Quand l’incident est là, il ne vous reste plus qu’une petite marge de manœuvre...

Dans les deux scenarii, les réflexes suivants peuvent vous aider :

**Pensez à l’évident**

* Vérifiez si les câbles, routeurs et modems sont tous bien branchés et l’alimentation électrique est bien assurée.
* Vérifiez si vous n’avez pas coupé le réseau Wi-Fi (bouton, touche...).
* Vérifiez si d’autres sites web sont toujours accessibles (le problème ne vient peut-être pas de votre connexion mais du site que vous souhaitez consulter).

**Pensez à vos outils**

* Vérifiez si votre pare-feu fonctionne et ne bloque pas tout le trafic.
* Renouvelez votre adresse IP (pensez à imprimer les [informations](https://www.tp-link.com/fr-be/support/faq/840/) nécessaires si vous ne savez pas comment faire).
* Faites un reset de vos appareils (modems....) : si vous ne trouvez pas le bouton “reset”, débranchez le modem 30 secondes au moins avant de rebrancher.

**Vérifiez avec les voisins** s’il s’agit d’un problème qui les concerne également ou si vous êtes le seul touché.

Si possible, **contactez votre fournisseur d’accès (opérateur télécom)**

Si au bout de quelques minutes cela ne fonctionne toujours pas, contactez votre service clientèle professionnel (et non “résidentiel”).

**Passer au plan B**

Si possible, utilisez temporairement d’autres moyens de communication et pensez à en informer le personnel.

**Pensez à votre communication externe**

Des clients, des fournisseurs s’énervent peut-être ? Voir Fiche Communication.

1. Etape 4 : Eradication

Il n’est pas toujours possible de déterminer pendant l’incident les causes de celui-ci. Dans ce cas, il s‘agira d’abord d’agir sur les conséquences (impact sur la continuité des activités) avant de pouvoir en déterminer la cause. Toutefois, des efforts raisonnables doivent être déployés pour pouvoir identifier la cause et limiter les risques qu’un tel incident se reproduise à nouveau...

1. Etape 5 : Désactivation

Lorsque les services touchés par un incident sont revenus à des opérations normales, l’incident peut être clos par l’équipe de gestion de l’incident (p.ex. helpdesk) en accord avec le gestionnaire du Business Continuity Plan.

Le plan de gestion des incidents est désactivé et un “post incident review” est effectué (voir étape 6).

Les mesures suivantes devraient être prises:

| **Action** | **Fonction** | **Liens vers d’autres documents**  ***Nom et référence*** |
| --- | --- | --- |
| Fermer le ticket d’incident | Helpdesk après accord du gestionnaire du plan de gestion des incidents | Ticket dans le cadre de l’Incident Management |
| Désactiver le plan de gestion des incidents | Gestionnaire du plan des incidents |  |
| Effectuer le Post Incident Review | Gestionnaire du plan des incidents | Post Incident Review (document) |
| … |  |  |

1. Etape 6 : Leçons acquises (Post Incident Review) (APRES INCIDENT)

*“I never lose. I either win or learn.”*

Nelson Mandela

Il s’agit d’apprendre de son expérience en réalisant un “post incident review” afin d’améliorer dans un processus continu la gestion des incidents.

Le Post Incident Review devrait comprendre au moins les éléments suivants :

### 6.1 : Contexte : Informations relatives a l’incident

| Élément | **Information** |
| --- | --- |
| Administration |  |
| Numéro de l’incident dans le registre des incidents : |  |
| Date et heure de la détection de l’incident : |  |
| Date et heure de la résolution de l’incident : |  |
| Type d’incident : |  |
| Gravité de l’incident : |  |
| Les clients ont-ils été touchés : |  |
| Gestionnaire de l’incident : |  |
| Description de l’incident : |  |
| ... |  |

### 6.2 : Evaluation de l’incident et leçons acquises

|  |  |
| --- | --- |
| **Détection** |  |
| Comment et par qui l’incident a-t-il été détecté : |  |
| L'incident a-t-il été détecté rapidement ou aurait-il pu l'être plus tôt : |  |
| Peut-on utiliser des procédures ou des outils pour détecter les incidents plus tôt ? |  |
| Les procédures de notification des incidents ont-elles été suivies : |  |
| **…** |  |

|  |  |
| --- | --- |
| **Evaluation et actions** |  |
| L'incident a-t-il été évalué correctement et correctement ?  L’information appropriée était-elle disponible pour ce faire : |  |
| Le BCP a-t-il été activé ? |  |
| Quelles autres mesures ont été prises pour résoudre l’incident : |  |
| Quelles ressources ont été utilisées pour gérer l’incident : |  |
| Le plan est-il suffisamment souple pour faire face à des événements imprévus : |  |
| Les mesures ont-elles été prises en temps opportun ? |  |
| **…** |  |

|  |  |
| --- | --- |
| **Communication** |  |
| Une communication interne a-t-elle été envoyée (en temps voulu): |  |
| La communication externe a-t-elle été envoyée (en temps voulu): |  |
| Quels médias ont été utilisés : |  |
| Quand la première communication a-t-elle été envoyée et quelle fréquence de mise à jour a-t-elle été utilisée ? |  |
| Les personnes concernées ont-elles été impliquées : |  |
| Quelles sont les communications utiles : |  |
| Quelles communications ont été employées et se sont révélées inefficaces : |  |
| **…** |  |

|  |  |
| --- | --- |
| **Prévention** |  |
| Que peut-on apprendre de ce qui s’est passé : |  |
| Comment éviter la répétition d’incidents, quelles mesures peuvent être prises pour le faire et qui est responsable de leur exécution : |  |
| **…** |  |

|  |  |
| --- | --- |
| **Analyse des causes profondes** |  |
| La cause de l’incident a-t-elle été détectée : |  |
| Incidents liés ou de nature similaire : |  |
| Y a-t-il un problème sous-jacent : |  |
| Le problème sous-jacent a-t-il été détecté (voir étape 4 Eradication) |  |
| **…** |  |

|  |  |
| --- | --- |
| **Adéquation de la réponse** |  |
| Temps réel de récupération (comparez avec le Recovery Time Objective RTO)  L’incident a été résolu dans le délai prédéterminé :  Pour aucune des activités  Seulement pour quelques activités  Pour toutes les activités |  |
| Faut-il ré-adapter les contrats ? |  |

|  |  |
| --- | --- |
| **Pertinence de la réponse du management à l’incident** |  |
| Le management n'a pas répondu ou n'a pas répondu de manière satisfaisante. |  |
| Le management a répondu, mais n’a pas suivi complètement les plans. |  |
| Le management a répondu pleinement conformément aux plans. |  |
| **…** |  |

|  |  |
| --- | --- |
| **Niveau de préparation du personnel** |  |
| 1. Non préparé |  |
| 2. Partiellement préparé |  |
| 3. Entièrement préparé |  |

|  |  |
| --- | --- |
| **Améliorations souhaitées** |  |
| Quels éléments pourraient être ajustés : |  |
| … |  |

|  |  |
| --- | --- |
| **Dommages et intérêts** |  |
| Y a-t-il des demandes de dommages-intérêts : |  |
| Des demandes de dommages-intérêts ont été déposées auprès de tiers dans le cadre de cet incident: |  |
| **…** |  |

|  |  |
| --- | --- |
| **Divers** |  |
| ... |  |

1. Annexes

### 7.1 : Liste des contacts

**Internes**

| **Fonction** | **Prénom NOM**  ***Pensez à designer une autre personne en cas d’absence, maladie,... de la personne de référence.*** | **Actions** | **Coordonnées**  ***Téléphonie fixe***  ***Bureau***  ***Maison***  ***Mobile***  ***Email***  ***Préférences de contact (le + rapide)*** |
| --- | --- | --- | --- |
| Personne de référence (continuité des activités) |  |  |  |
| Suppléant |  |  |  |
| ... |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Externes**

| **Fonction** | **Prénom NOM**  ***Pensez à designer une autre personne en cas d’absence, maladie,... de la personne de référence.*** | **Contrats**  ***Référence*** | **Coordonnées**  ***Téléphonie fixe***  ***Bureau***  ***Maison***  ***Mobile***  ***Email***  ***Préférences de contact (le + rapide)*** |
| --- | --- | --- | --- |
| Assureur |  |  | Téléphone fixe  Bureau  1)  2)  Maison  1)  2)  Mobile  1)  2)  Email  1)  2) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| … |  |  |  |
| … |  |  |  |

### 7.2 : Tableau

|  |  |  |
| --- | --- | --- |
| **1.1 Placez un pilote dans l’avion** | **Qui accomplit la tâche** | **Quelles procédures faut-il suivre?** |
|
| [Scenario 1] |  |  |
| [Scenario 2] |  |  |
| **[…]** |  |  |

|  |  |  |
| --- | --- | --- |
| **1.2: Connaissez vos risques** | **Prendre le résultat de la colonne P de votre Risk Assessment (2 (vert) à 10 (rouge)** | **Groupe Focus ?** **(1 ou 2)** |
| Dans votre Risk Assessment, quel est votre niveau de risque pour le scénario 1? |  |  |
| Dans votre Risk Assessment, quel est votre niveau de risque pour le scénario 2 |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  | **2.2.3: Identifiez les priorités**   * **Quels sont vos objectifs de temps?** * **Quel est le délai maximum «acceptable» pour restaurer l’activité? (Recovery Time Objective, RTO)** * **Quel est l’âge maximum des données dont vous avez besoin pour récupérer (Recovery Point Objective, RPO)** * **Qu’avez-vous prévu avec vos fournisseurs (Recovery Consistency Objective, RCO)?** * **... en cas d’interruption ou de détérioration de vos activités, quel est l’ordre de priorité des activités (P)?** | | | |
| **2.2.1 Identifiez les activités concernées (Scenario 1)** |  | | **RTO** | **RPO** | **RCO** | **P** |
| Ressources humaines |  | |  |  |  |  |
| Infrastructures |  | |  |  |  |  |
| Technologie |  | |  |  |  |  |
| Information et documentation |  | |  |  |  |  |
| Tiers |  | |  |  |  |  |
| **…** |  | |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **3.1: Identifiez vos moyens et outils (Scenario 1)** | **Activité essentielle 1** | **Activité essentielle 2** |
| Personnel clef |  |  |
| Informations ou données importantes |  |  |
| Services informatiques nécessaires (matériel, logiciel) |  |  |
| Bâtiments |  |  |
| Contacts externes (ressources) |  |  |
| Interdépendance avec d'autres activités (si oui, qui) |  |  |
| **…** |  |  |