Continuité d’activité

**1. Objet**

**1.1 Finalité**

**1.2 Domaine d'application**

**1.3 Glossaire**

**2. Responsabilité**

**3. Documents**

**4. Exigences de la norme ISO 27001 : 2022**

**5. Déroulement**

**5.1 Préparation**

**5.2 Mise en place**

**5.3 Vérification**

Historique

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Toutes | Création | 01/01/2022 |
| **Page** | **Changement** | **Date** |

**1. Objet**

**1.1 Finalité**

La présente procédure a pour finalité pendant une perturbation :

* de protéger l’information et les autres actifs associés
* d’assurer la disponibilité de l’information de l’organisation et des autres actifs associés

**1.2 Domaine d'application**

Le domaine d’application de la procédure « Continuité d’activité » s’applique à tous les systèmes informatiques, applications et données entrant dans le plan de continuité d’activité de notre organisation.

**1.3 Glossaire**

PCA – plan de continuité d’activité

TIC – technologie de l’information et de la communniation

RSI – responsable sécurité de l’information

**2. Responsabilité**

Le responsable sécurité de l’information (RSI) a l’autorité de l’écriture et de la mise à jour de cette procédure. Il est garant de son application. Il a l’appui du directeur.

**3. Documents**

Plan de continuité d’activité

Gérer la continuité d’activité

Sauvegarde de l’information

Classification de l’information

Redondance des moyens

**4. Exigences de la norme ISO 27001 : 2022**

A.5.29 Sécurité de l’information pendant une perturbation

L’organisation doit planifier comment maintenir la sécurité de l’information au niveau approprié pendant une perturbation.

A.5.30 Préparation des TIC pour la continuité d’activité

La préparation des TIC doit être planifiée, appliquée, maintenue et testée selon les objectifs et les exigences de continuité d'activité.

**5. Déroulement**

**5.1 Préparation**

Le Plan de continuité d'activité - PCA (*BCP* – *Business Continuity Plan*) de la sécurité de l’information définit comment maintenir les activités critiques informatiques de l'organisation pendant et après un désastre.

Les objectifs de sécurité de l’information applicables aux situations défavorables sont déterminés conformément aux résultats de l’analyse de l’impact sur nos activités en cas de crise ou de sinistre. Ces objectifs sont validés par la direction et enregistrés dans le Plan de continuité d’activité (PCA).

Exemples de risques identifiés :

* défaillances techniques des serveurs, de la communication critique ou de l'équipement réseau
* actions humaines (erreurs involontaires, manque de préparation, abus de ressources, vol, actes terroristes)
* catastrophes naturelles (tremblements de terre, inondations, incendies)

L'appréciation et le traitement des risques de sécurité de l’information contribuent à l'élaboration du PCA, notamment en définissant activités et systèmes critiques. Plus de détails dans la procédure Classification de l’information.

La continuité de la sécurité de l’information est intégrée dans le processus Gérer la continuité d’activité.

La politique de Sauvegarde de l’information permet de restaurer les données essentielles de nos systèmes et applications.

La planification des actions pour garantir la continuité de la sécurité de l’information et des processus en cas d'urgence est basée sur :

* utiliser des mesures de sécurité de l’information
* assurer des systèmes et des outils de support
* maintenir les mesures de sécurité de l’information pendant des perturbations
* compenser des mesures pour les mesures de sécurité de l'information qui ne peuvent pas être maintenus pendant l'interruption
* comprendre les risques, leur vraisemblance d’apparition et leur impact
* définir les processus critiques de l'activité et déterminer les priorités
* identifier les actifs impliqués dans les processus critiques
* clarifier les conséquences sur les activités causées par des incidents de sécurité de l'information
* former et sensibiliser le personnel sur les processus de continuité de l’activité de l'information
* sélectionner les solutions pour faire face aux incidents à impact plus limité, ainsi qu'aux incidents graves pouvant menacer la viabilité de l'organisation
* assurer la sécurité du personnel et la protection des équipements
* fournir les ressources financières, organisationnelles et techniques nécessaires
* documenter les plans de continuité de la sécurité de l'information

**5.2 Mise en place**

L’équipe adéquate pour se préparer et réagir à une situation défavorable inclut des personnes possédant l’autorité, l’expérience et les compétences nécessaires. Cette équipe est nommée par la direction dans le but d’apporter à temps une réponse aux incidents et de maintenir la sécurité de l’information.

Des réponses aux questions suivantes sont déterminées :

* qui doit évaluer la situation lors de l'activation du PCA ?
* qui contacter ?
* quand ?
* comment ?
* qui est responsable de la communication ?
* quelles actions immédiates entreprendre ?
* quels sont les systèmes critiques ?
* quels sont les services critiques ?
* quelles actions spécifiques prendre pour des circonstances extraordinaires ?
* quel site temporaire alternatif mettre en place pour les activités ou services critiques ?
* quelles sont les étapes de récupération dans les plus brefs délais ?
* quelles sont les actions de restauration des sauvegardes ?
* quels sont les équipements à remplacer ?

Le Plan de continuité d’activité (PCA) inclut les mesures nécessaires afin de fournir le niveau requis de continuité de la sécurité de l’information pour toutes les activités critiques, sensibles et confidentielles.

Exemples de mesures :

* 30 minutes – réunion des équipes d’urgence
* 120 minutes – bilan de la situation et des dégâts
* 8 heures – mise en place des systèmes de secours
* une semaine – restauration de tous les systèmes

L'organisation s'assure que :

* une structure organisationnelle adéquate est en place pour se préparer, atténuer et répondre à une perturbation soutenue par du personnel ayant la responsabilité, l'autorité et la compétence nécessaires
* le plan de continuité d’activité, y compris les procédures d'intervention et de récupération détaillant la manière dont l'organisation prévoit de gérer une interruption des services TIC, est :
  + évalué régulièrement au moyen d'exercices et de tests
  + approuvé par la direction
* le plan de continuité d’activité comprend les informations suivantes :
  + spécifications de performance et de capacité pour répondre aux exigences et aux objectifs de continuité d’activité
  + objectif de récupération temps de chaque service TIC prioritaire et les procédures de restauration de ces composants
  + objectif de point de récupération des ressources TIC prioritaires définies comme information et les procédures de restauration de l’information

La gestion de la continuité des TIC est un élément clé des exigences de continuité d'activité concernant la disponibilité pour pouvoir :

* réagir et se remettre d'une interruption des services TIC, quelle qu'en soit la cause
* s'assurer que la continuité des activités prioritaires est soutenue par les services TIC requis
* réagir :
  + avant qu'une interruption des services TIC ne se produise
  + lors de la détection d'au moins un incident pouvant entraîner une interruption des services TIC

La procédure Redondance des moyens établit les moyens à dupliquer pour faire face à des défaillances, surtout si des temps de récupération courts sont nécessaires.

**5.3 Vérification**

Le PCA est mis à jour et testé au minimum une fois par an (calendrier et ressources). Les résultats des tests sont analysés et évalués par la direction. Les mises à jour font suite à des changements intervenus dans les processus, politiques, procédures des systèmes d’information.