Ligne directrice sécurité de l'information & vie privée :

Gestion de la continuité

(BLD BCM)

TABLE DES MATIÈRES

1. INTRODUCTION 3
2. GESTION DE LA CONTINUITÉ 3
ANNEXE A: GESTION DOCUMENTAIRE 4
ANNEXE B: RÉFÉRENCES 4
ANNEXE C: DIRECTIVES RELATIVES À LA CONTINUITÉ DE LA SÉCURITÉ DE L'INFORMATION ET DE LA VIE PRIVÉE 5
ANNEXE D: LIEN AVEC LA NORME ISO 27002:2013 8

1. Introduction

Le présent document fait intégralement partie de la méthodologie relative à la sécurité de l'information et à la vie privée au sein de la sécurité sociale. Le présent document est destiné aux responsables, aux sous-traitants de données, au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution publique de sécurité sociale (IPSS).

Les principaux objectifs de la gestion de la continuité sont :

- protéger les processus critiques contre les effets d'incidents ou sinistres majeurs
- appliquer une approche commune et cohérente pour la réalisation d'un plan de continuité
- veiller à ce que tous les composants nécessaires soient présents de sorte que l'organisation puisse réagir, de manière appropriée, aux incidents et sinistres majeurs et ainsi réaliser une restauration dans les meilleurs délais

La gestion de la continuité est plus large que les TIC: l'absence de collaborateurs (maladie, licenciement, décès) ou la disparition d'un fournisseur critique peut constituer une réelle menace. Lors de l'organisation de la gestion de la continuité, il y a lieu de prendre en compte tous les aspects pertinents qui sont susceptibles de compromettre la continuité.

Le présent document traite les aspects relatifs à la sécurité de l'information et à la vie privée au niveau du traitement d'informations lors de la gestion de la continuité d'une organisation: une approche pragmatique afin de protéger des processus (critiques) contre l'impact de perturbations ou sinistres majeurs et afin de rétablir la situation dans les meilleurs délais conformément aux attentes de l'organisation.

2. Gestion de la continuité

Toute organisation souscrit les directives suivantes relatives à la sécurité de l'information et à la vie privée pour l'ensemble des informations et systèmes d'information relevant de la responsabilité de l'organisation:

a. Pour tous les processus critiques et systèmes d'information essentiels, il y a lieu d'établir un plan de continuité. Ce plan décrit les activités, mesures et données essentielles des processus de l'organisation, ayant pour but de limiter le délai d'interruption à un niveau acceptable.

b. La sécurité de l'information et la vie privée doivent intégralement faire partie de la gestion de la continuité.

c. Chaque organisation doit disposer d'un plan de continuité propre qui accorde au moins une attention aux aspects suivants:
    1) L'identification et la documentation des processus essentiels et des systèmes d'information y afférents de l'organisation;
    2) L'évaluation des risques dans laquelle le risque, l'impact et les mesures de contrôle actuelles sont définies;
    3) Les connaissances et compétences des collaborateurs leur permettant de faire tourner les processus essentiels et systèmes d'information y afférents ou de les redémarrer;
    4) En cas d'incident grave ou de sinistre, qui peut activer le plan de continuité, quand et comment?
    5) Informations (acceptabilité de la perte d'information);
    6) Priorités et ordre de restauration;
    7) Communication pendant et après un incident grave ou un sinistre;
    8) Comment le plan de continuité exécuté est-il formellement clôturé après un incident grave ou un sinistre, par qui et à quel moment?

d. En organisant une gestion de la continuité adéquate, l'organisation doit garantir que l'impact d'un incident ou sinistre majeur et sa restauration sont limités à un niveau acceptable, et ce conformément aux attentes de l'organisation.

e. Le plan de continuité doit régulièrement être testé et adapté. Les résultats des tests doivent être communiqués à la direction de l'organisation en vue de la validation et de l'approbation d'actions futures.

Annexe A: Gestion documentaire

Gestion des versions

Date	Auteur	Version	Description du changement	Date approbation	Date entrée en vigueur
2014		V2014	Première version	20/09/2014	01/10/2014
2017		V2017	Intégration UE GDPR	07/03/2017	07/03/2017

Erreurs et omissions

Si à la lecture du présent document, vous constatez des erreurs ou des problèmes, vous êtes invité, en tant que lecteur, à transmettre une brève description de l'erreur ou du problème et de sa localisation dans le document ainsi que vos données de contact au conseiller en sécurité de l'information (CISO) / délégué à la protection des données (DPO) de l'organisation.

Définitions

Pour garantir la cohérence en ce qui concerne la terminologie et les notions utilisées à travers les divers documents de politique, toutes les définitions relatives à la sécurité de l'information et à la protection de la vie privée sont regroupées dans un document spécifique : "Définitions sécurité de l'information et protection de la vie privée".

Annexe B: Références

Ci-dessous figurent les documents qui ont servi de source d'inspiration pour le présent document:

- ISO, “ISO/IEC 27001:2013 Information Security Management System Requirements”, september 2013, 23 p.
- ISO, “ISO/IEC 27002:2013 Code of Practice for Information Security Management”, september 2013, 80 p.
- ISO, “ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity”, juni 2016, 36 p.
- ISO, “ISO/IEC 22301:2012 Societal security. Business continuity management systems. Requirements”, mei 2012, 24 p.
- ISACA, “COBIT 5 for Information Security”, Mei 2012, 220 p.
- FOD Binnenlandse Zaken, “BUSINESS CONTINUITY MANAGEMENT, handleiding voor implementatie”, juni 2009, 132 p.

Ci-dessous figurent les références aux sites web qui ont service de source d'inspiration pour le présent document:

- https://www.iso.org/isoiec-27001-information-security.html
- http://www.iso.org/iso/catalogue_detail?csnumber=54534
- http://www.iso.org/iso/catalogue_detail?csnumber=54533
- https://www.iso.org/standard/44374.html
- https://www.iso.org/standard/50038.html
- http://www.isaca.org/cobit
- http://crisiscentrum.be/nl/publication/business-continuity-management-een-handleiding-bij-de-implementatie
- http://www.ccb.belgium.be/nl/work
- http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Annexe C: Directives relatives à la continuité de la sécurité de l'information et de la vie privée

Le processus de gestion de la continuité

Le processus de gestion de la continuité (business continuity management ou BCM) identifie les menaces pour une organisation de sorte que celle-ci puisse continuer à remplir sa mission en cas d'événement majeur ou de sinistre. La gestion de la continuité a pour résultat la rédaction, l'actualisation et, en cas de dommages, l'activation du plan de continuité jusqu'à ce que la situation normale soit rétablie.
Les activités comprennent:

1. Le programme de continuité: cette phase fixe la structure de l'organisation ainsi que les objectifs du projet.
2. La notion de l'organisation: au cours de cette phase, une évaluation de l'impact et des risques permet d'évaluer l'impact d'une interruption du processus pour l'organisation et de définir les critères de disponibilité pour chaque processus de l'organisation.
   Objectif de sécurité: cette analyse tient compte de la sécurité de l'information
3. Stratégie du plan de continuité (Business Continuity Plan ou BCP): Élaboration d'une stratégie de la continuité en fonction des objectifs à atteindre
   Objectif de sécurité: définition des normes minimales de sécurité
4. Mise en œuvre du plan de continuité: rédaction du plan de continuité
   Objectif de sécurité: veiller à ce qu'il soit tenu compte des exigences de sécurité
5. Test du plan de sécurité: le test des plans permet de vérifier que les activités critiques sont susceptibles d'être rétablies dans le délai fixé.
   Objectif de sécurité: vérifier que les exigences de sécurité sont opérationnelles
6. Maintenance et révision du plan de continuité et formation des collaborateurs dans le cadre du plan de continuité:
   Objectif de sécurité: mettre à jour les documents relatifs au plan de continuité

Directives concernant l'aspect sécurité de l'information et vie privée dans le plan de continuité

Stratégie en matière de continuité de la sécurité de l'information et de la vie privée

- La direction doit offrir un cadre pour la fixation des objectifs de continuité, en ce compris l'engagement de satisfaire à toutes les conditions applicables, d'attribuer des responsabilités inhérentes et de contribuer à une amélioration permanente du plan de continuité.
- La continuité est un processus interactif qui doit être géré de manière active. Pour commencer, le plan de continuité peut être géré sur la base d'une approche pour la gestion de projets. Ce plan doit être actualisé au moins une fois par an.
- Pour tous les actifs qui sont considérés comme critiques par l'organisation, il y a lieu de décrire et de documenter les critères de disponibilité relatifs à la reprise des activités. Les critères de disponibilité minimums sont les suivants: RTO–RPO.
- Il est aussi nécessaire de mentionner dès le début d'un nouveau projet applicatif ou d'un projet relatif à un service les exigences relatives à la sécurité de l'information et à la vie privée dans l'analyse préalable, en particulier les critères de disponibilité.
- L'appréciation et le traitement des risques relatifs à la sécurité de l'information et à la vie privée des systèmes d'information contribuent à l'exécution de ces plans, notamment en décrivant le caractère critique des activités et des systèmes d'information, les risques résiduels et les mesures de sécurité à intégrer. Le conseiller en sécurité de l'information (CISO) et le délégué à la protection des données (DPO) qui font intégralement partie du processus de gestion des risques, doivent collaborer avec le responsable de l'élaboration du plan de continuité désigné dans ce plan.
- Lors de l'évaluation des risques, l'organisation doit également identifier toute activité critique et déterminer dans quelle mesure elle est dépendante de fournisseurs ou d'autres tiers. Elle doit par ailleurs veiller à ce que les aspects relatifs à la sécurité de l'information et à la vie privée soient repris dans le plan de continuité.

Développement de la continuité de la sécurité de l'information et de la vie privée

- L'organisation s'engage à mettre en œuvre un processus formel et permanent pour la gestion de la continuité de la sécurité de l'information et de la vie privée, ainsi que la structure adéquate pour se préparer à un incident imprévu, limiter cet incident et y réagir.
- Dans ce cadre, une gestion des incidents est opérationnelle dans l'organisation (où il est tenu compte des incidents relatifs à la sécurité de l'information et à la vie privée).
- Sur la base d'un plan de continuité ou d'une évaluation des risques existant, l'organisation doit déterminer le niveau admissible en cas d'une diminution de la prestation de service lorsque les activités reprennent suite à un incident ou sinistre majeur.
- Le niveau de sécurité de l'information et de vie privée minimal requis en cas d'une diminution de la prestation de service est documenté dans le plan de continuité.
- Il y a lieu de veiller à ce que les conditions relatives à la sécurité de l'information et à la vie privée soient opérationnelles dans les procédures de sauvegarde et de restauration.

Contrôle, révision et évaluation de la continuité de la sécurité de l'information et de la vie privée

- Un plan de test annuel est déterminé et approuvé par la direction.
- Le conseiller en sécurité de l'information (CISO) et le délégué à la protection des données (DPO) doivent vérifier que les tests proposés tiennent compte de la continuité de la sécurité de l'information et de la vie privée.
- L'organisation réalise régulièrement des évaluations de ses procédures et capacités en matière de continuité et veille à ce que le niveau fixé soit respecté en cas d'une diminution de la prestation de service.
- Etant donné que le plan est régulièrement revu, ceci doit être planifié en début d'année, de sorte que les plans soient consolidés pour une date déterminée.
- L'organisation doit veiller à ce que le plan de continuité soit publié et distribué aux intéressés, de sorte que ces plans soient disponibles en cas d'incident ou sinistre majeur; leur exécution étant requise dans ces cas.
- Lors de chaque révision du plan de continuité, l'organisation prévoit une session de sensibilisation relative aux adaptations pour tous les acteurs intéressés.
- Le conseiller en sécurité de l'information et le délégué à la protection des données vérifient régulièrement le plan de continuité. Ils analysent les résultats de test afin de détecter des lacunes et des incohérences. Si nécessaire, ils proposent des améliorations pertinentes.

Redondances

Sur la base d'une évaluation des risques, l'organisation a identifié les exigences en matière de disponibilité des systèmes d'information:

- Si l'infrastructure existante ne permet pas de garantir la disponibilité des systèmes d'information, il y a lieu d'envisager la redondance des composants ou de l'architecture.
- Le cas échéant, il y a lieu de tester régulièrement la redondance des systèmes d'information afin de veiller à ce que la transition d'un composant vers un autre fonctionne correctement.
- La mise en œuvre de la redondance peut entraîner de nouveaux risques sur le plan de l'intégrité et de la confidentialité des systèmes d'information; il y a lieu d'en tenir compte lors de la conception de la redondance.

Mesures de gestion

1. Cadre du plan de continuité

L'organisation doit développer/adopter un cadre pour un plan de continuité. Ceci afin de garantir que tous les plans sont cohérents, pour traiter les conditions relatives à la sécurité de l'information et à la vie privée de manière cohérente et pour fixer des priorités pour les tests et la maintenance.

2. Intégrer la sécurité de l'information et la vie privée dans le processus de gestion de la continuité

L'organisation doit développer et maintenir un processus de continuité, de sorte à garantir le respect des conditions relatives à la sécurité de l'information et à la vie privée qui sont nécessaires pour la continuité du fonctionnement de l'organisation.

3. Continuité et évaluation des risques

Les événements susceptibles de donner lieu à une interruption des processus, doivent être identifiés au moyen de la réalisation d'une évaluation des risques. Une analyse des risques permet d'inventorier la probabilité/le risque et les effets/l'impact d'une interruption en termes de délais, de dommages et de période de restauration. Il est opportun et efficace d'intégrer les aspects relatifs à la sécurité de l'information dans l'analyse des risques normale de la gestion de la continuité. Ceci implique que les conditions de continuité en matière de sécurité de l'information et de vie privée doivent être formulées explicitement dans les procédures de gestion de la continuité. L'idée sous-jacente est d'épargner du temps et des efforts étant donné qu'il ne faut pas réaliser d'analyse des risques supplémentaire pour la sécurité de l'information et la vie privée.

4. Développer, valider, mettre en œuvre et communiquer le plan de continuité

Il y a lieu de développer et de mettre en œuvre des plans afin de maintenir ou de rétablir les activités et afin de garantir la disponibilité des informations au niveau convenu à l'avance et dans les délais requis après une interruption ou une cessation de processus critiques. A cet égard, il est explicitement tenu compte des aspects relatifs à la sécurité de l'information et à la vie privée.

Les plans de continuité développés peuvent être utilisés pendant les activités de sensibilisation, de formation et de test.

5. Tester, évaluer et adapter le plan de continuité

Le plan de continuité doit être régulièrement testé afin de garantir qu'il reste actuel et efficace. Le plan de continuité doit être adapté sur la base des résultats et doit être communiqué aux parties concernées.

Priorités

Au cours d'un incident ou sinistre majeur, tous les processus ne peuvent avoir lieu. Trop peu de moyens et de collaborateurs sont en général disponibles à cet effet. Il y a donc lieu d'opérer des choix: comment l'organisation utilise-t-elle les collaborateurs et moyens rares? Quelles sont les priorités de l'organisation?

Les processus peuvent par exemple être répartis en groupes (priorités):

- processus qui ne peuvent pas être postposés;
- processus qui peuvent être postposés d'1 jour au maximum;
- processus qui peuvent être postposés d'1 semaine au maximum;
- processus qui peuvent être postposés d'1 mois au maximum;
- processus qui peuvent être postposés de 3-6 mois au maximum;

Pour les organisations, le catalogue de produits et de services constitue un moyen pratique.

Annexe D: Lien avec la norme ISO 27002:2013

Nous vous renvoyons ici aux principales clauses de la norme ISO 27002:2013 en rapport avec le sujet du présent document.

Norme ISO 27002:2013	
Politique de sécurité	
Organisation de la sécurité de l'information	
Sécurité des ressources humaines	
Gestion des actifs	
Protection de l'accès	
Cryptographie	
Sécurité physique et environnementale	
Protection des processus	
Sécurité de la communication	
Maintenance et développement de systèmes d'information	
Relations avec les fournisseurs	
Gestion des incidents de sécurité	
Aspects de la sécurité de l'information dans la gestion de la continuité	**Oui**
Respect	

***** FIN DU DOCUMENT *****