UNIVERSITÉ DE GENÈVE

DIVISION DU SYSTÈME ET DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Standard de sécurité

Directive de gestion de la continuité d'activité pour les services numériques

Ce document présente les principes et activités de Gestion de la Continuité d'Activité pour les services numériques (GCA-ServicesNum) déployés au sein de l'UNIGE et opérés par la Division du Système et des Technologies de l'Information et de la Communication (DiSTIC).

Statut :	En cours de rédaction / En cours de validation / **Validé**
Auteur(s) :	Pierre L'Hostis – RSSI
Validé par/le :	DirSTIC / 23 janvier 2017
Liste de diffusion :	DiSTIC

Remarques :

- Pour faciliter la lecture de ce document, le masculin générique est utilisé pour désigner les deux sexes.
- Les termes suivis d'un astérisque sont expliqués dans le glossaire disponible à l'adresse suivante : https://plone.unige.ch/distic/documents-de-reference/continuite-dactivites

Historique des révisions

N° vers.	Modifié par / le	Validé par / le	Description
1.0	PLH / 18.01.17	DirSTIC / 23.01.17	Version initiale présentée en DirSTIC

Sommaire

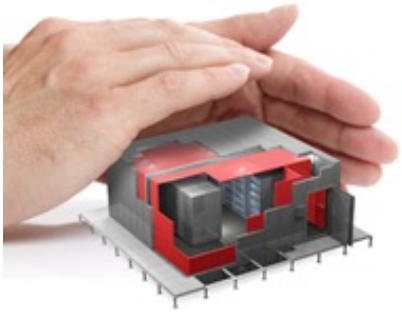
1 Introduction

1.1 Contexte

Les services numériques sont aujourd'hui incontournables à l'Université, aussi bien pour les activités académiques qu'administratives. On peut penser en particulier au portail web de l'institution, aux services d'enseignement et d'apprentissage en ligne, aux services de gestion des données de la recherche, à l'ensemble des applications administratives, aux différents réseaux filaires et Wi-Fi d'accès à l'information. Ils sont donc indispensables au bon fonctionnement de l'Université.
Il est à noter également qu'une grande partie du patrimoine informationnel de l'Université est aujourd'hui conservé sous un format électronique (fichiers informatiques, bases de données).

La disponibilité du système d'information (SI) qui permet de mettre en œuvre ces services numériques, et par voie de conséquence de soutenir les activités métiers, peut être compromise par des incidents ponctuels touchant une partie des infrastructures (panne d'un serveur informatique par exemple) ou des sinistres plus importants (dégât des eaux, incendie, etc.) affectant plus totalement et durablement les ressources d'un site informatique.

Il est donc indispensable de fournir en tout temps une protection adaptée des composants actifs et passifs tels que les applications, les serveurs, le réseau ou les sauvegardes afin de s'assurer de la continuité d'activité des services numériques reposant sur ces composants. Cette protection doit s'appuyer sur une organisation et des mesures de protection organisationnelles et techniques adaptées qui nécessitent un cadre de gestion spécifique.



1.2 Définitions

Les définitions suivantes sont à connaître pour une meilleure compréhension du document :

- Métier : ce terme désigne la maîtrise d'ouvrage d'un service numérique.
- Planification de la Continuité des Activités (PCA) : planification de toutes les tâches nécessaires pour assurer la continuité des services en cas de sinistre
- Plan de Reprise d'Activité (PRA) : plan documenté des actions à effectuer pour relancer un service ou un ensemble de services

2 Principes fondamentaux

2.1 Vue d'ensemble

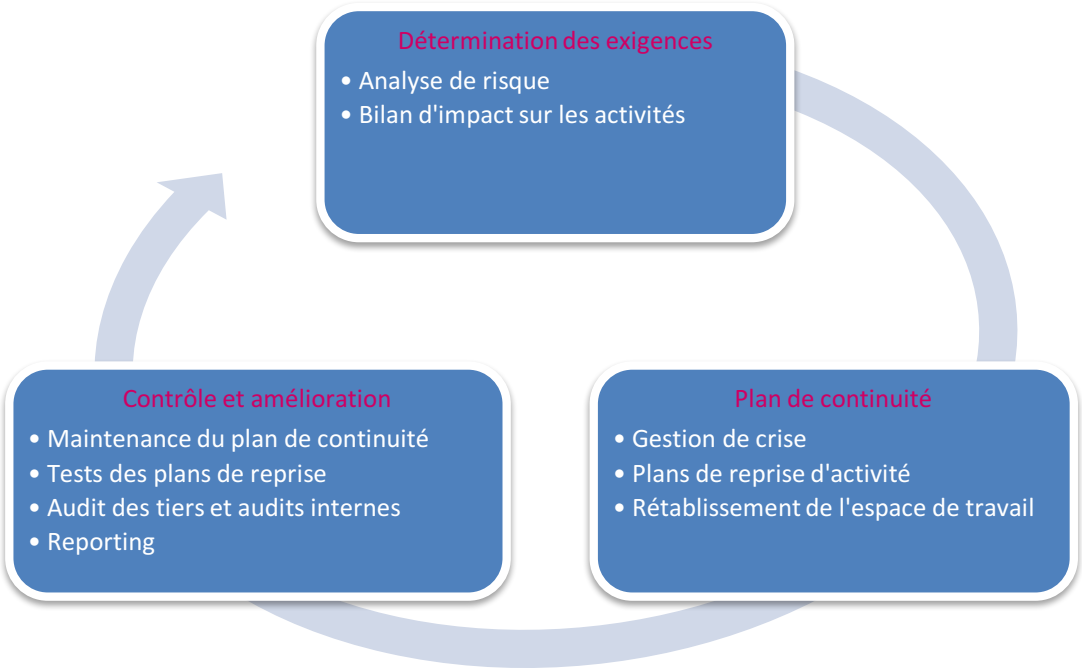
La Gestion de la Continuité d'Activité* (GCA) est le processus de pilotage global de toutes les activités traitant de continuité d'activité au sein de l'Université.

La Planification de la Continuité d'Activité* (PCA) est l'élaboration, par anticipation, de plans et procédures pour s'assurer que les services et les composants techniques essentiels pour les Métiers* continuent à fonctionner en cas de panne ou de sinistre majeur.

La GCA / PCA comprend plusieurs activités-clés :

- L'analyse de risques* – permet d'évaluer le contexte des menaces pesant sur les activités Métier ;
- Le bilan d'impact sur les activités* – comprend l'identification, l'évaluation et la priorisation des exigences des Métiers en termes de continuité de leurs activités ;
- La gestion de crise* – la gestion des incidents d'étendue ou de gravité exceptionnelle menaçant la continuité d'activité ;
- La reprise d'activité* après sinistre – le rétablissement* des activités après sinistre, et des systèmes et services de réseau ou informatiques sous-jacents, dans un délai et à un niveau de service convenus ;
- Le rétablissement d'un espace de travail* après sinistre – la fourniture de capacités de travail alternatives pour les fonctions de l'Université (y compris, collaborateurs, équipements et installations et/ou bureaux) dans un délai et à un niveau de service convenus ;
- Des activités de contrôle et d'amélioration notamment concernant la maintenance du plan de continuité, les tests planifiés des plans de reprise, les audits et le reporting.

Ces activités-clés se répartissent ainsi :



2.2 Périmètre

La GCA-ServicesNum concerne les services numériques sous la responsabilité de la DiSTIC, c'est-à-dire soit opérés par la DiSTIC dans ses locaux, soit opérés par des fournisseurs de services externalisés pour lesquels des contrats de prestation ont été établis au préalable avec la DiSTIC. La maîtrise d'ouvrage de ces services numériques est soit la DiSTIC elle-même, pour les services transverses tels que le Réseau, soit une autre entité métier de l'Université (divisions, services communs ou facultés).

Par la mise en œuvre de la GCA-ServicesNum, la DiSTIC a pour objectif d'assurer :

- La continuité du service pour tous les utilisateurs du SI (étudiants, enseignants, chercheurs, personnel administratif et technique, externes, grand public) ;
- Le respect de ses obligations (contrats de services implicites ou explicites, légales) ;
- La limitation des pertes financières directes ou indirectes suite à une panne ou un sinistre majeur ;
- Le renforcement de la confiance et le maintien de l'image de marque de l'Université.

Exclusions

La GCA-ServiceNum ne traite pas de la GCA globale de l'Université qui concerne l'ensemble des fonctions et pas seulement le volet numérique.

La GCA-ServiceNum ne traite pas des services numériques qui sont sous la responsabilité d'une entité autre que la DiSTIC. Dans ce cas, c'est cette entité qui doit s'assurer de l'adéquation entre les attentes des Métiers et utilisateurs de ces services numériques, et la qualité de service proposée par ces services.

La GCA-ServiceNum ne traite pas du rétablissement de l'espace de travail* après sinistre pour les collaborateurs de l'Université, à l'exception des collaborateurs de la DiSTIC nécessaires à la continuité d'activité convenue des services numériques.

Exceptions

La Direction du Système et des Technologies de l'Information et de la Communication (DirSTIC*) et/ou le Rectorat peuvent autoriser des exceptions à la présente Directive lorsque sa mise en œuvre serait difficile, voire impossible ou ne se justifie pas. Les exceptions à la présente politique doivent être consignées dans la cartographie des risques* associée au bilan d'impact sur les activités.

2.3 Organisation, rôles et responsabilités

Au niveau de la Division STIC

La Division STIC doit mettre en œuvre une organisation et identifier les rôles-clés, afin de mettre en place la GCA-ServicesNum. La DirSTIC s'assurera que ces ressources disposent de l'autorité requise et sont correctement dimensionnées pour assurer leurs missions.

En particulier, la Direction de la Division STIC peut nommer un (voire plusieurs) référent(s) en tant que Responsable(s) de Gestion de la Continuité d'Activité (Responsables GCA* ou RGCA), étant établi que la coordination globale de la GCA-ServiceNum est de la responsabilité du RSSI. Un RGCA est responsable, dans son périmètre, de la bonne exécution des tâches comprises dans la GCA-

ServicesNum et de son maintien opérationnel. Un RGCA peut également être nommé Responsable d'un processus de Prévention / Gestion de Crise.

Le Responsable GCA est chargé de gérer tous les aspects de la GCA, en étroite relation avec toutes les parties prenantes concernées internes ou externes à la Division STIC, et en particulier les suivants :

- Evaluation des risques sur les activités,
- Bilan d'impact sur les activités,
- Gestion de crise, reprise après sinistre et rétablissement d'un espace de travail,
- Développement, tests et maintenance des plans de reprise d'activité,
- Conformité aux exigences internes et aux obligations légales et réglementaires,
- Communication interne et externe.

Une obligation légale, une réglementation ou un contrat conclu avec un partenaire – notamment dans le domaine scientifique – peut imposer que les systèmes ou services disposent d'éléments de GCA. La DirSTIC doit prendre en compte ces contraintes.

Au niveau des Métiers et des facultés

Les Métiers doivent participer activement à la GCA-ServicesNum en fournissant, de manière régulière, une évaluation de leurs exigences en termes de disponibilité de service et d'intégrité des données pour les services numériques dont ils assument la maîtrise d'ouvrage.

D'un point de vue pratique, la revue et la validation de ces exigences doit être effectuée par les Directions Métier concernées.

Au niveau des Tiers

S'il est fait appel à des fournisseurs/prestataires, à de la sous-traitance, à de la délocalisation, à de l'externalisation ou à un partenariat avec une entité tierce, la DirSTIC doit s'assurer que la GCA est bien prise en compte dans les engagements contractuels liant l'Université avec ces fournisseurs/prestataires/partenaires. La DirSTIC doit ainsi veiller aux exigences en termes de gestion de la continuité d'activité selon des conditions définies à l'avance concernant notamment les ressources mises à disposition, les stocks et les délais, ainsi que les moyens mis en œuvre pour prévenir les interruptions de service et réagir le cas échéant.

3 Activités clés

La mise en œuvre de la GCA-ServicesNum se base sur les principes présentés dans la section 2.1 « Vue d'ensemble » afin de garantir que la GCA est régie, mise en œuvre et mise à jour conformément aux pratiques de référence. Les activités-clés de ce modèle sont présentées dans ce chapitre.

3.1 Evaluation des risques

L'Analyse de Risque consiste à :

- identifier les actifs participant aux activités de l'Université,
- identifier les menaces qui pèsent sur ces actifs
- évaluer leur probabilité et leur impact afin de s'en protéger

L'Analyse de Risque est un élément sur lequel s'appuie le Plan de Reprise d'Activité. L'Analyse de Risque documente les mesures permettant de limiter l'apparition et la fréquence des risques.

L'Analyse de Risque doit être menée régulièrement, idéalement une fois par an.

3.2 Bilan d'impact sur les activités

Le Bilan d'impact sur les activités (BIA) doit être mené régulièrement, idéalement une fois par an, avec les maîtrises d'ouvrage des services numériques pour identifier et valider les exigences en matière de continuité des activités Métiers.

Ces activités reposent sur des services numériques et des éléments techniques. Le BIA examine l'impact sur l'Université de la défaillance de ces services numériques ou éléments techniques. Cet impact est utilisé pour en déduire les exigences en matière de continuité.

Les exigences sont définies par la maîtrise d'ouvrage (Métiers), à partir des critères de base suivants :

- Durée maximale d'indisponibilité admissible*,
- Perte de données maximale admissible*,
- Détérioration acceptable du niveau de service*, et conditions d'intégrité et de confidentialité des données.

Illustration :

Service de paiement par cartes de crédit

✓ Durée maximale d'indisponibilité admissible < 4 heures

✓ Perte de données maximale admissible < 1 jour

✓ Détérioration acceptable du niveau de service : disponibilité de 95% sur l'année. Les conditions d'intégrité doivent être les mêmes en fonctionnement nominal ou de secours

✓ Application sensible avec stockage et/ou traitement d'informations sensibles

Le BIA établit également une correspondance entre les exigences en matière de continuité et les solutions techniques à mettre en œuvre : sauvegarde distante, redondance de système, réplication des services numériques sur plusieurs sites physiques, etc.

Illustration :

Service	Technologies recommandées
Service de paiement par cartes de crédit	Réplication sur 2 sites physiques avec cluster actif-actif et réplication synchrone.

Les services ou éléments techniques essentiels qui ne disposeraient pas de plans de reprise cibles tels que définis dans le BIA sont un risque pour l'Université. Toute lacune en matière de GCA-ServicesNum doit être consignée dans un répertoire ou une cartographie des risques, et actée au niveau de la DirSTIC et des Métiers concernés.

3.3 Gestion de crise

La planification de la gestion de crise se base sur une organisation traitant de la réponse stratégique, tactique et opérationnelle à apporter en cas de crise touchant certaines fonctions ou éléments techniques essentiels pour l'Université. La DiSTIC doit disposer d'un plan de gestion de crise étroitement lié au PCA existant.

3.4 Reprise après sinistre

Le processus de planification de reprise après sinistre consiste à préparer à l'avance des plans de reprise d'activité destinés à restaurer le fonctionnement des services dans un délai et à un niveau de service convenus avec les Métiers.

Ces plans s'appuient sur des mécanismes techniques et des procédures de reprise. Le périmètre des plans peut être local (sur le site informatique principal) ou externe (mise en œuvre de sites informatiques de secours).

3.5 Rétablissement d'un espace de travail

Le processus de planification de rétablissement d'un espace de travail après sinistre consiste à préparer à l'avance des capacités de travail alternatives afin de rétablir les fonctions de l'Université (y compris collaborateurs, équipements, postes de travail et installations et/ou bureaux) dans un délai et à des niveaux de service convenus avec les maîtres d'ouvrage (Métiers).

3.6 Maintenance du plan de continuité

Le plan de continuité (constitué des plans de reprise des activités essentielles) doit être examiné et actualisé régulièrement selon une fréquence définie par la DirSTIC. Pour assurer son maintien en conditions opérationnelles, il est recommandé d'actualiser le plan de continuité au moins une fois par an ou après toute évolution majeure dans l'organisation.

3.7 Tests des plans de reprise

Tous les plans de reprise doivent être testés régulièrement selon une fréquence et un calendrier de test définis par la DirSTIC, en accord avec les Métiers concernés. Pour assurer leur maintien en conditions opérationnelles, il est recommandé de tester chaque plan de reprise au moins une fois par an. La totalité de chaque plan doit être testée. Différents types de test peuvent être utilisés :

- Simulation sur table – Revue virtuelle des plans, sur papier, en se basant sur des scénarios ;
- Simulation active – Tests en réel des plans, individuels ou multiples.

Les résultats des tests des plans associés à la GCA-ServicesNum doivent être transmis à la DirSTIC et aux Métiers concernés.

3.8 Audits

Il est nécessaire d'auditer régulièrement les capacités des tiers fournisseurs en matière de GCA afin de s'assurer du respect des exigences de l'Université en la matière.

Des audits internes ou externes peuvent être mandatés pour évaluer la conformité du dispositif de GCA-ServicesNum tel que défini dans la présente directive.

3.9 Reporting

Le Responsable GCA assurant la coordination globale de la GCA-ServiceNum, soit le RSSI, est chargé du reporting des capacités et activités en matière de GCA-ServicesNum auprès de la DirSTIC.

Ce reporting s'intéressera en particulier :

- aux résultats du BIA,
- à l'état d'avancement de la GCA,
- aux tests des éléments de la GCA et à la prise en compte des résultats de ces tests dans des boucles d'amélioration continue,
- aux risques en matière d'absence de GCA.

4 Intégration dans la Gouvernance du SI

La démarche de mise en œuvre de la GCA-ServicesNum décrite précédemment est prise en compte dans le cadre de la Gouvernance du SI institutionnel, en particulier dans le cycle de vie des projets de SI, ainsi que par la formation et la sensibilisation des acteurs concernés.

4.1 Projets de SI

La méthodologie de gestion des projets de SI doit permettre d'identifier et de prendre en compte au plus tôt les besoins des Métiers en termes de continuité d'activité. Les éléments principaux à prendre en compte sont :

- L'établissement des exigences en termes de continuité des activités Métiers (cf. BIA §3.2),
- La création d'un plan de reprise d'activité (cf. §3.4) et d'un plan de test de ce plan,
- La mise en œuvre d'un test de reprise et la rédaction d'un rapport de test (cf. §3.7),

La gestion du changement technique (hors projet) doit également garantir la continuité de l'activité convenue.

4.2 Formation et sensibilisation

En complément des différentes tâches exposées dans la présente directive, la Division STIC, en charge de la GCA-ServicesNum, doit sensibiliser les parties prenantes respectives et leur faire connaître les pratiques et processus de GCA.

Les collaborateurs qui participent aux activités de GCA doivent être formés afin de s'assurer qu'ils sont aptes à remplir leurs fonctions. Les autres collaborateurs doivent être sensibilisés à la GCA afin de savoir quel comportement adopter en cas de panne ou sinistre majeur.

5 Annexes

5.1 Références documentaires

Référence	Intitulé
PSSI	Politique de sécurité du système d'information https://memento.unige.ch/doc/0174
RGS	Règles générales de sécurité https://plone.unige.ch/distic/documents-de-reference/secu/rgs
Méthode projet	https://plone.unige.ch/pmo/methodologie-et-formation
Glossaire	Glossaire des termes relatifs à la Continuité d'activité https://plone.unige.ch/distic/documents-de-reference/continuite-dactivites
PSMSI008	Procédure de classification et d'inventaire des actifs du SI
ISO 27001	Norme ISO/CEI 27001:2013 – Technologies de l'information – Techniques de sécurité - Systèmes de gestion de sécurité de l'information – Exigences
ISO 22301	Norme ISO/CEI 22301:2012 – Sécurité sociétale – Systèmes de management de la continuité d'activité – Exigences
ISO 27002	Norme ISO/IEC 27002:2013 – Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information
ISO 27005	Norme ISO/IEC 27005:2011 – Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information