Federal Information Security Policy Guideline

Glossaire

21/11/2019

FISPDOC10 V1.0

Remarque importante : Le présent document est un guide qui résulte d'une collaboration entre des experts en sécurité de l'information des différents services fédéraux (SPF, OIP, IPSS). Les mesures présentées sont considérées comme des mesures minimales applicables raisonnablement de manière commune à tous les services fédéraux. Elles se basent sur des normes internationales et des bonnes pratiques en matière de sécurité de l'information ainsi que sur les expériences des participants au groupe de travail FISP.

Si des mesures plus strictes sont nécessaires à un service fédéral pour des raisons réglementaires ou pour d'autres raisons formelles et contraignantes, il va de soi que ces mesures prévalent sur celles décrites dans le présent guide.

Groupe de travail

.be

Contenu du document

Orientation du document

Ce document fait partie intégrante de la méthodologie relative à la sécurité de l'information au sein de l'administration fédérale (projet FISP).

Objectif de sécurité du document

Le but du document est de garantir une cohérence dans la terminologie et les notions utilisées dans tous les documents stratégiques de FISP.

Champ d'application

Afin de garantir la cohérence dans la terminologie et les notions utilisées dans tous les documents stratégiques, toutes les définitions pertinentes sont centralisées dans c document.

Sauvegarde

Ces informations ne peuvent pas être utilisées individuellement comme documentation de référence. Ce document ne peut pas servir de substitut à la législation ou à des normes, mais vise à guider le lecteur dans la prise de mesures de sécurité appropriées.

Responsabilités

Le présent document est destiné au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution publique de l'administration fédérale, aux responsables du traitement de l'information (y compris les sous-traitants des systèmes d'informations) et aux autres intervenants dans des domaines connexes (exemple : le gestionnaire de documents).

Propriétaire

Le groupe de travail FISP est propriétaire du présent document.

Définitions

A

Action préventive : mesure prise pour prévenir un incident (notamment les mesures pare-feu et antivirus).

Address spoofing **(usurpation d'adresse)** : technique permettant d'usurper des adresses IP afin de contourner les pare-feux.

Analyse d'impact relative à la protection des données : analyse de parties de processus et de l'impact que peut y entraîner une interruption des activités.

Appareils mobiles : terme général employé pour désigner les smartphones, tablettes, notebooks et autres ordinateurs portables.

Applications critiques : sans les applications critiques, une organisation n'est pas en mesure d'exécuter les activités quotidiennes.

Appréciation des risques : processus par lequel le risque estimé est confronté à des critères de risques établis afin de déterminer dans quelle mesure le risque et/ou l'ampleur de ce risque est acceptable ou supportable.

Attaque : tentative d'obtenir un accès non autorisé à l'information de l'entreprise. Lire, voler, modifier, rendre inutilisable ou utiliser illicitement cette information.

Authentification à deux facteurs (TOTP) : méthode d'authentification utilisant une combinaison de deux moyens différents pour confirmer l'identité de l'utilisateur (exemple : retirer de l'argent par le biais d'une carte bancaire et d'un code PIN).

Authentifier : rendre authentique, valable, reconnaître comme authentique. Dans le contexte IT, on entend généralement par authentifier : déterminer l'identité correcte d'une personne ou d'un système qui se connecte auprès d'un autre système pour avoir accès à l'information. Garantir qu'un trait de caractère présumé d'une identité est correct.

Authentique : lorsqu'une entité est ce qu'elle prétend être.

Autorisation : détermination des actions que l'utilisateur peut exécuter dans une application ou un système.

Autorité de protection des données : chaque État membre de l'UE doit mettre sur pied une ou plusieurs autorité(s) de surveillance afin de surveiller l'application du règlement et faire office de point de contact pour chaque action de l'intéressé.

C

CISO : CISO signifie *Chief Information Security Officer*. Celui-ci fait partie du top management. Il définit au nom du top management la politique de sécurité de l'information et organise et dirige la sécurité de l'information de l'organisation en fonction des besoins et de la prise de risques de l'organisation.

Clé compromise : clé dont il est impossible de garantir qu'elle est utilisable exclusivement par des personnes autorisées.

Cloud Backup Service Provider : un tiers qui gère pour des clients des services et des solutions de back-up de données basés sur le cloud et en assure la distribution depuis un *data center* central.

Cloud Backup : le *cloud backup*, ou *cloud computer backup*, désigne la réalisation de back-ups de données vers un serveur externe, basé sur le cloud. Pour cette forme de stockage cloud, des back-ups cloud sont stockés et rendus accessibles via plusieurs ressources dispersées et reliées, formant ensemble un cloud.

Cloud Broker (intermédiaire) : une entité qui crée et entretient des relations avec plusieurs fournisseurs de services cloud. Fonctionne comme intermédiaire pour les clients et fournisseurs de services cloud, en sélectionnant pour chaque client le meilleur fournisseur et en assurant le monitoring des services.

Cloudburst : le *cloud bursting* est une technique utilisée par des clouds hybrides pour fournir au besoin des ressources complémentaires pour les clouds privés. Si le cloud privé a la capacité de supporter ses charges de travail, le cloud hybride n'est pas utilisé. Le *cloudburst* intervient lorsque votre cloud connaît une perturbation ou une faille de sécurité et que vos données ne sont pas disponibles. Le terme *cloudburst* est utilisé de deux manières, dans un sens positif et dans un sens négatif :

- *Cloudburst* (négatif) : l'échec d'un environnement de *cloud computing* en raison de l'incapacité à réagir à un pic de sollicitations.
- *Cloudburst* (positif) : la mise en œuvre dynamique d'une application logicielle, qui travaille normalement sur des ressources informatiques internes, dans un cloud public pour réagir à un pic de sollicitations.

Cloud Center : un *data center* dans le cloud qui utilise des composantes virtualisées basées sur des standards comme une infrastructure de type *data center* qui loue son infrastructure.

Cloud computing : le *cloud computing* est la mise à disposition via internet de hardware, software, informations, fichiers et données. Voir le document "FISP - Sécurité du Cloud".

Cloud Database : une base de données qui est accessible aux clients via le cloud et qui est fournie à des utilisateurs sur demande via internet par des serveurs d'un fournisseur de base de données cloud. Aussi appelée *Database-as-a-Service* (DBaaS). Les bases de données cloud peuvent utiliser le *cloud computing* pour permettre une évolutivité optimisée, une grande disponibilité, le *multitenancy* et une affectation effective des ressources.

Cloud externe : services cloud publics ou privés qui sont fournis par un tiers en dehors de l'organisation. Un environnement de *cloud computing* qui se trouve hors des limites de l'organisation.

Cloud Management : logiciels et technologies développés pour l'exécution et le monitoring d'applications, de données et de services qui se trouvent dans le cloud. Les outils de *cloud management* permettent de veiller à ce que les ressources de *cloud computing* d'une entreprise fonctionnent de manière optimale et communiquent bien avec les utilisateurs et les autres services.

Cloud Migration (migration du cloud) : processus de déménagement de tout ou partie des données, applications et services d'une entreprise, d'emplacements sur site derrière un pare-feu vers le cloud, où les informations peuvent être fournies sur demande via internet.

Cloud-Oriented Architecture (COA) (architecture orientée cloud) : terme créé par Jeff Barr d'Amazon Web Services. Décrit une architecture dans laquelle des applications fonctionnent comme des services dans le cloud et servent d'autres applications dans l'environnement cloud. Une architecture pour infrastructure IT et applications logicielles qui sont optimisées pour une utilisation dans des environnements de *cloud computing*. Ce terme n'est

pas encore très répandu et, comme c'est le cas pour le terme '*cloud computing*', il n'existe pas de définition générale ou généralement admise ou de description spécifique d'une architecture orientée cloud.

Cloud Platform : la couche du milieu de la Pyramide du Cloud qui fournit une plateforme ou un cadre informatique (exemple : .NET, Ruby on Rails ou Python) comme *stack service*. Le contrôle n'est possible que sur la plateforme ou le cadre, mais pas à un niveau inférieur (infrastructure serveur). Exemples : Google AppEngine ou Microsoft Azure.

Cloud Portability (portabilité) : dans la terminologie du cloud (*computing*), le terme '*cloud portability*' signifie la possibilité de déplacer des applications et des données correspondantes d'un fournisseur de cloud vers l'autre – ou d'un environnement cloud public vers un privé. Voir aussi *Vendor-lock-in*.

Cloud Provider (fournisseur de cloud) : fournisseur de services qui offre aux clients un espace de stockage ou des solutions logicielles via un réseau privé ou public.

Cloud Provisioning (provisionnement cloud) : implémentation de la stratégie du *cloud computing* d'une entreprise, où l'on détermine d'abord quelles applications et quels services sont conservés dans le cloud et lesquels restent sur site derrière un pare-feu ou dans un cloud privé. Le provisionnement cloud comprend aussi le développement de processus pour des interfaces avec les applications et services cloud, de même que des audits et le monitoring de qui a accès aux ressources et les utilise.

Cloud public : voir le document "FISP - Sécurité du cloud".

Cloud Security (sécurité du cloud) : les principes de sécurité qui s'appliquent au *computing* sur site s'appliquent également à la sécurité du *cloud computing*.

Cloud Serverhosting : le *cloud serverhosting* est une forme d'hébergement où les services d'hébergement sont disponibles pour les clients sur demande via internet. Au lieu d'être proposés par un seul serveur ou serveur virtuel, les services d'hébergement de serveurs cloud sont fournis par plusieurs serveurs formant ensemble un cloud.

Cloud Servers (serveurs cloud) : serveurs virtualisés avec des systèmes d'exploitation Windows ou Linux qui sont activés via une interface web ou API. Les serveurs cloud se comportent de la même manière que les serveurs physiques et peuvent être gérés au niveau administrateur ou '*root*', selon le type de serveurs et le fournisseur d'hébergement cloud.

Cloud Service Architecture **(CSA)** : terme imaginé par Jeff Barr d'Amazon Web Services. Ce terme décrit une architecture où les applications et les composantes des applications fonctionnent comme des services dans le cloud, servant d'autres applications dans le même environnement cloud.

Cloud Sourcing : *outsourcing* de stockage ou d'exploitation d'un autre type de service cloud. L'*outsourcing* de certaines activités IT vers des services cloud meilleur marché. Exemple : *data backup*.

Cloud Testing **(test)** : exécution de tests de charge et de performance sur les applications et services proposés via le *cloud computing* – à savoir l'accessibilité de ces services – afin de garantir des performances et une évolutivité optimales dans diverses circonstances.

Conseiller en sécurité : responsable de la tenue à jour et du développement de la stratégie de sécurisation de l'organisation conformément à la législation en vigueur et aux normes minimales sur lesquelles se base l'organisation. Il rend formellement compte à la direction une fois par an.

Contrôle (mesure de) : moyen pour gérer un risque. Généralement, il s'agit d'une mesure de sécurité technique ou organisationnelle. Sont également comprises la politique de sécurité, les procédures, les directives et les bonnes pratiques.

Contrôle d'accès : moyens visant à garantir que l'accès aux biens est autorisé et limité sur la base des exigences de l'entreprise et en termes de sécurité.

Convention : accord écrit entre les organisations et un tiers sur des travaux, des livraisons et des services fournis par des tiers à l'organisation et/ou inversement.

Cryptage : la protection de vos supports d'information grâce à la transformation de l'information (texte non édité) de manière à la rendre illisible pour chacun (texte crypté), sauf pour ceux qui disposent d'une clé.

D

***Data at rest* (DAR) ou données inactives** : données stockées numériquement sur un support physique ou virtuel : supports de stockage, supports de données externes, bandes et supports de stockage virtuels. Les formes de stockage peuvent être : fichiers, bases de données, archives, back-ups off-site. Les lieux de stockage peuvent être : serveurs physiques et virtuels, stations de travail (mobiles), appareils mobiles, appareils.

***Data in motion* (DIM)** : données transférées via un réseau privé, public ou d'entreprise, indépendamment du support, câblé et sans fil.

***Data in use* (DIU) ou données actives** : Données présentes dans la mémoire, traitées activement ou stockées temporairement (*caching* technique) durant le traitement par un processus ou une application.

Déclassification : suppression de la classification précédemment accordée à l'information, de sorte que l'information est librement accessible.

Déni de service (*Denial of Service*) : situation dans laquelle un système informatique est malencontreusement indisponible pour la prestation de services attendue.

Destruction : s'assurer que toute trace de données ou d'informations a été éliminée d'un support de données ou que le support de données même est suffisamment détruit et que les données ou informations de la même source ne peuvent pas à nouveau être rendues visibles ou lisibles. La destruction de documents, par exemple, peut se faire au moyen d'une déchiqueteuse ou en rassemblant les données dans des containers spéciaux. Le contenu de ces containers est détruit par une firme spécialisée. La destruction de données originales n'est possible qu'après en avoir averti le propriétaire et compte tenu des dispositions légales y afférentes. L'acte de destruction doit faire l'objet d'une autorisation.

Disaster Recovery (DR) (reprise après sinistre) : possibilité de restaurer l'accès aux archives, données, hardware et software, de manière à pouvoir reprendre les activités importantes de l'entreprises après un sinistre. Pensons par exemple aux sinistres dans vos facilités (incendie dans le bâtiment, alerte à la bombe), catastrophes locales (coupure de courant, inondation, tremblement de terre), catastrophes régionales (ouragans [l'ouragan Katrina faisait 800 km de long], perturbations sur le réseau électrique). Les coûts pour garantir la reprise des activités augmentent généralement avec la distance et le nombre de centres de reprise de sinistre. C'est souvent lié à la *Business Continuity*.

Disponibilité de l'information : fait que l'information est accessible et utilisable à la demande d'une entité compétente. En d'autres termes, la disponibilité garantit le fait que les systèmes informatiques sont disponibles au moment où ils sont nécessaires pour exécuter les processus de travail.

Données à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée 'personne concernée') ; est réputée être une personne physique identifiable une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Données dans le cloud : la gestion de données dans le cloud requiert une sécurisation des données et la protection des données à caractère personnel, ainsi que le contrôle du déplacement des données d'un point A à un point B. Cela comprend également la gestion du stockage des données et des ressources pour un traitement de données à grande échelle.

Données internes : toutes les données qui ne peuvent être utilisées qu'au sein de l'organisation. Ces données ne peuvent être rendues publiques sans l'accord préalable d'un membre du personnel compétent de l'organisation.

Données sensibles : données classifiées comme telles par leur propriétaire. De manière générale, les données sensibles ne peuvent pas être communiquées au public, mais exclusivement à la personne ou à l'entreprise concernée. En fonction de la classification, ces données sensibles sont clairement définies, soumises à des règles d'utilisation et utilisées par un groupe relativement restreint de collaborateurs.

Données : information électronique traitée ou stockée sur des systèmes d'information.

DPIA : signifie *Data Protection Impact Assessment*, aussi appelée analyse d'impact relative à la protection des données.

DPO : signifie *Data Protection Officer*, aussi appelé délégué à la protection des données.

Droits d'accès privilégiés : droits d'accès nécessaires pour introduire des modifications dans le modèle RBAC ou pour exécuter des modifications sur le système (administration système).

Droits de la personne concernée (RGPD) : toute personne concernée a de nouveaux droits et peut demander à chaque organisation de modifier ses droits. Cela comprend le droit à l'information et l'accès aux données à caractère personnel ; correction et échange de données ; opposition à des pratiques de marketing direct ; opposition à une prise de décision et un profilage automatisés ; transférabilité des données.

E

Environnement à haut risque : environnement exposé à un grand risque sur le plan de la sécurité de l'information. Exemple : environnement qui génère un trafic de données sur un réseau public (comme une connexion VPN).

Espaces sécurisés : espaces physiquement protégés (exemple : *data centers*).

Évaluation des risques : ensemble de procédures visant à identifier, analyser et évaluer des risques.

Événement de sécurité de l'information : changement observé dans le fonctionnement normal d'un système, d'un environnement, d'un processus ou d'une personne, en relation avec une violation potentielle de la sécurité

de l'information, l'échec des mesures de contrôle, une situation inédite qui peut être pertinente dans le cadre de la sécurité de l'information.

Event logging (enregistrement d'événements) : il s'agit de la collecte des activités du système et des utilisateurs, des événements du système, des erreurs et des événements qui concernent la sécurité de l'information.

F

Facilités pour l'utilisation de l'information : toute forme de système d'information, service ou infrastructure qui est utilisé pour enregistrer, traiter et gérer l'information et les moyens physiques et les lieux qui doivent être présents à cet effet.

FISP : *Federal Information Security Policy*.

Forensics : Concernant des procès, des enquêtes judiciaires.

G

Gestion de la continuité business (*Business Continuity Management* – BCM) : la gestion de la continuité business a pour but de protéger les processus business (activités business) contre les interruptions et, en cas d'interruption, de veiller à une réaction positive et efficace.

Gestion de la continuité ICT : la gestion de la continuité ICT garantit que les technologies de l'information et de la communication ainsi que les services sont protégés et peuvent être restaurés à la fois à des niveaux prédéfinis et dans des délais exigés par le business. La gestion de la continuité ICT soutient le processus général de gestion de la continuité business (*Business Continuity Management* (BCM)) d'une organisation.

Gestion de la sécurité de l'information : toutes les activités coordonnées qui orientent la politique d'une organisation à l'égard des risques. La gestion des risques comprend normalement des analyses de risques, la prise de mesures de sécurité, l'acceptation de risques jusqu'à un certain niveau et la communication des risques au sein de l'organisation.

Gestion de l'identité : la gestion des données d'identité personnelles, afin de contrôler l'accès aux ressources informatiques, applications, données et services de manière correcte.

Gestion des incidents de sécurité de l'information : processus destinés à détecter, rapporter, évaluer, répondre, traiter et tirer un enseignement des incidents de sécurité de l'information.

Gestion des risques : activités coordonnées pour orienter et surveiller une organisation en ce qui concerne les risques.

Gestion relationnelle : gestion de la relation avec un tiers qui a (ou aura) accès à l'information et/ou aux ressources d'information de l'organisation et/ou livre (livrera) des informations et/ou des ressources d'information à l'organisation.

Gestionnaire opérationnel de l'information : un gestionnaire opérationnel de l'information est un individu ou un département, désigné soit par l'organisation, soit par le propriétaire des processus, qui est responsable de l'implémentation et de la gestion opérationnelle des mesures de sécurité nécessaires en fonction du niveau de classification défini par le propriétaire des processus. Dans la pratique, un gestionnaire opérationnel de

l'information peut être un administrateur système, un développeur d'applications, un responsable de la gestion des bâtiments, etc.

Guide : on désigne ici les directives à considérer comme étant conseillées. Celles-ci ne doivent pas être absolument suivies en tant que telles. Elles constituent des outils qui orientent la méthode de travail.

H

Hybride cloud (cloud hybride) : voir le document "FISP - Sécurité du cloud".

I

IAAS : *Infrastructure As A Service* - Voir le document "FISP - Sécurité du cloud".

IAM : *Identified Access Management* - Voir le document "IAM & PAM".

Incident de sécurité de l'information : un ou plusieurs événements non désirés liés à la sécurité de l'information présentant un risque significatif de perturber la prestation de services de l'organisation et de compromettre la sécurité de l'information.

Information : l'information est une ressource qui, comme toute autre ressource importante, doit être protégée/sécurisée adéquatement. L'information peut prendre différentes formes, notamment écrite, imprimée, électronique ou orale. Lorsque l'information est stockée sur un système informatique, on parle généralement de données (*data*).

Informations confidentielles : caractéristique d'une information qui n'est pas rendue disponible ou accessible à des personnes, entités ou processus non autorisés.

Intégrité de l'information : l'intégrité porte sur l'exactitude et l'exhaustivité. Il s'agit de garantir que l'information est fiable et qu'il n'y a pas de modification non autorisée de l'information.

Interfaces standardisées : les services cloud devraient avoir des API standardisés, qui donnent des instructions sur la manière dont deux sources d'applications ou de données peuvent communiquer entre elles.

Intrusion Detection System **(IDS)** (système de détection d'intrusion) : système automatisé qui détecte les tentatives ou les cas d'accès non autorisé à un système d'information ou un réseau.

Intrusion Prevention System **(IPS)** (système de prévention d'intrusion**)** : système automatisé qui bloque les tentatives ou les cas d'accès non autorisé à un réseau.

IP / ***Internet Protocol*** : l'IP définit la manière dont les paquets de données, aussi appelés datagrammes, sont déplacés entre une source et une destination. Techniquement parlant, on peut définir l'IP comme le protocole de la couche réseau dans la suite de protocoles de communication TCP/IP.

ITIL : acronyme de '*Information Technology Infrastructure Library*'. Il s'agit d'une série de solutions et de concepts de meilleures pratiques qui servent de cadre de référence pour la mise en place de processus de gestion au sein d'une organisation TIC.

L

LAN : un groupe d'ordinateurs et d'appareils connexes qui partagent une ligne de communication commune ou une connexion sans fil et partagent généralement les ressources d'un seul processus ou serveur dans un petit espace géographique (exemple : dans un immeuble de bureaux).

Liste de distribution : une liste de distribution est une liste des personnes auxquelles un document peut être envoyé ou communiqué en tout ou en partie. Il peut s'agir de personnes individuelles physiques ou de groupes de personnes qui se distinguent par une caractéristique vérifiable particulière.

Loi belge sur le traitement des données à caractère personnel : la loi du 30 juillet 2018, qui met en œuvre le RGPD et définit une série de caractéristiques spécifiques pour la Belgique.

M

Matrice de sécurité : modèle utilisé pour gérer les droits d'accès sur la base des autorisations, rôles et fonctions pour les applications.

Menace : cause potentielle d'incident, qui peut résulter en un dommage au système ou à l'organisation.

Mesures de gestion : les mesures prises pour maîtriser les risques peuvent consister en une politique, des procédures, des directives et des méthodes de travail ou des structures organisationnelles qui peuvent être de nature administrative, technique, de gestion ou juridique.

Mobile device management **(MDM)** : software permettant, à distance, d'éteindre des appareils, d'effacer ou de bloquer des données en cas de vol ou d'abus.

Moyen d'entreprise : tout ce qui a de la valeur pour l'organisation (bâtiments, information, logiciels, hardware, services mais aussi personnes, aptitudes, ...).

Moyen d'information : tout élément/moyen utile à l'organisation pour créer, recevoir, traiter, stocker, distribuer, envoyer, dupliquer et détruire de l'information ; information pouvant être stockée sur différents supports d'information et dans différents systèmes d'information.

Multitenancy : l'hébergement sur le même hardware physique de la propriété de plusieurs entreprises, composé de plusieurs systèmes, applications et/ou données. Le *multitenancy* se rencontre sur la plupart des systèmes basés sur le cloud.

Multi-tenant : terme utilisé dans le domaine du *cloud computing* pour désigner plusieurs clients qui utilisent le même cloud public.

P

PAAS : *Platform As A Service* – Voir le document "FISP – Sécurité du Cloud".

PAM : *Privileged Access Management* – Voir le document "FISP – IAM & PAM".

Patch : adaptation / mise à jour soit d'un logiciel existant sur la base d'un code de programme pour corriger et/ou améliorer des lacunes ou des erreurs, soit d'une machine réseau et/ou d'un câblage réseau.

Périmètre logique : barrière au niveau des systèmes d'information, qui empêche l'intrusion de personnes ou d'applications non autorisées. L'existence d'un périmètre logique exige donc la vérification de l'identité, le contrôle de l'autorisation et le filtrage des données.

Périmètre physique : barrière physique bloquant l'accès aux personnes non autorisées. L'existence d'un périmètre physique s'accompagne donc de l'octroi d'un accès à des personnes autorisées. Diverses formes sont possibles, telles qu'une clé ou un système de badge. Dans le cadre de cette politique, on part du principe que le périmètre physique est suffisamment sécurisé contre une intrusion par des personnes non autorisées.

Politique : la définition formelle de la sécurité de l'information et l'intention de la direction concernant la gestion des risques d'entreprise et la protection de l'organisation contre les risques en matière de sécurité de l'information.

Privacy by Design : le principe du *Privacy by Design*, mentionné dans le RGPD, demande à chaque organisation de prendre les mesures de sécurité adéquates dès le début de chaque projet ou processus afin de sauvegarder et protéger les données à caractère personnel.

Privacy Risk Assessment **(PRA)** : voir analyse d'impact relative à la protection des données.

Private cloud (cloud privé) : voir le document “FISP – Sécurité du Cloud".

Procédures : elles soutiennent les documents politiques spécifiques en traduisant les politiques concernées en tâches opérationnelles spécifiques (détermination de la sécurisation).

Profil de risque : dans l'analyse des risques, les risques sont déterminés sur la base de l'impact et de la probabilité de menaces à la sécurité de l'information. Tous les risques confondus constituent le profil de risque de l'organisation.

Propriétaire de l'information : l'information doit être attribuée à un ‘propriétaire’ qui connaît l'utilisation et la valeur de l'information pour l'organisation, nécessaire pour déterminer le niveau de classification de l'information.

Propriétaire de rôle : responsable d'un rôle dans le modèle RBAC, composé d'un lot spécifique d'autorisations et associé à une ou plusieurs fonctions.

Propriétaire système : responsable d'un ou plusieurs systèmes d'information placés sous la gestion de l'organisation.

R

Recovery Point Objective **(RPO)** (objectif de point de reprise) : délai maximal durant lequel la perte de données est acceptable.

Recovery Time Objective **(RTO) (**objectif de temps de reprise) : délai durant lequel des systèmes et des données doivent être restaurés à un point antérieurement constaté à la suite de la panne d'un système.

Respect : le non-respect de ces politiques peut entraîner de graves risques à la sécurité concernant la disponibilité, l'intégrité et la confidentialité des données (sensibles), ainsi que l'image et la réputation de l'organisation. Le non-respect de la politique et des procédures y afférentes peut conduire à des sanctions, voire à des poursuites judiciaires.

Responsable des données : personne physique ou morale qui, seule ou avec d'autres, détermine le but et les moyens pour le traitement des données à caractère personnel.

Responsable du traitement : le responsable du traitement détermine les finalités et les moyens du traitement des données à caractère personnel. Si votre organisation décide donc 'pourquoi' et 'comment' les données à caractère personnel doivent être traitées, c'est donc elle le responsable du traitement (source RGPD).

RGPD (GDPR) : le règlement général relatif à la protection des données est un texte législatif de l'UE qui fixe un nouveau cadre juridique pour le traitement de données à caractère personnel.

RGPD UE : Règlement général européen sur la protection des données.

Risque inhérent : probabilité d'un impact négatif en l'absence de mesures de protection.

Risque résiduel (*residual risk*) : le risque qui subsiste en dépit des mesures de sécurité prises. Il est souvent impossible d'exclure totalement les risques, en revanche il est généralement possible de ramener les risques à un niveau acceptable. Le risque résiduel est ce petit risque accepté.

Risque : chance ('probabilité') qu'une certaine menace se produise avec un certain impact ('gravité') en conséquence.

***Role-based access control* (RBAC) :** méthode permettant d'organiser de façon efficace et efficiente un contrôle d'accès pour des systèmes d'information, où les utilisateurs sont associés à des fonctions business prédéfinies, qui consistent en divers rôles, dont chacun détient un lot spécifique d'autorisations.

S

SaaS : *Software As A Service* - Voir le document "FISP – Sécurité du Cloud".

Sécurité de l'information : protection de l'information contre un large éventail de menaces. L'intégrité, la confidentialité et la disponibilité de l'information sont trois aspects fondamentaux dans ce contexte.

Sécurité de l'information : protection de la confidentialité, l'intégrité et la disponibilité de l'information. D'autres caractéristiques peuvent également jouer un rôle comme l'authenticité, la justification, l'irréfutabilité et la fiabilité.

Sécurité du cloud privé : l'implémentation d'un cloud privé vise à éliminer bon nombre des inconvénients de la sécurité du *cloud computing*. Comme le setup d'un cloud privé est implémenté en toute sécurité dans le cadre du pare-feu de l'entreprise, il reste sous contrôle du département IT.

***Security Incident & Event management* (SIEM)** : terme employé pour désigner des produits et services logiciels qui centralisent des données sur des événements et des incidents pour ensuite les analyser.

***Security Incident Response Team* (SIRT) :** équipe de collaborateurs appelée à agir lorsque certains incidents de sécurité de l'information se produisent. En fonction du type d'incident de sécurité de l'information, cette équipe peut chaque fois être composée de différentes personnes.

***Service Level Agreement* (SLA)** : convention contractuelle dans laquelle un fournisseur de services définit le niveau de service, les responsabilités, les priorités et les garanties en termes de disponibilité, prestations et autres aspects du service.

Service provider (fournisseur de services) : entreprise ou organisation qui fournit un service cloud public ou privé.

Session active : environnement en ligne spécifique dans lequel un utilisateur travaille avec son application / sa transaction. Un utilisateur peut travailler simultanément dans plusieurs environnements (ou sessions) en ligne.

Sous-traitant des données : personne physique ou morale qui, exclusivement sur la base d'une convention écrite, traite des données à caractère personnel pour le compte du responsable du traitement.

Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement (source RGPD).

Stockage cloud privé : forme de stockage cloud où les données d'entreprise et les ressources de stockage cloud se trouvent à la fois dans le *data center* de l'entreprise et derrière le pare-feu.

Stockage cloud public : forme de stockage cloud où l'entreprise et le fournisseur de services cloud sont séparés et où les données sont stockées en dehors du *data center* de l'entreprise.

Stockage cloud : service avec lequel le client peut stocker des données en les amenant via internet ou un autre réseau vers un système de stockage externe géré par un tiers. Le stockage cloud signifie “stockage de données en ligne dans le cloud”, où les données d’entreprise sont stockées et rendues accessibles à l’aide de plusieurs ressources dispersées et reliées, formant ensemble un cloud.

Stockage : conservation de données sur un support (moyen de stockage). Un traitement peut être effectué à partir du stockage.

Support analogique : un support analogique permet de sauvegarder des données sous forme non numérique. Le support analogique le plus répandu est le papier.

Support numérique : lorsque des données sont sauvegardées de façon électronique (représentation des données sous forme binaire), on parle d'un support numérique.

Systèmes d'information : tous les réseaux et systèmes ICT, applications incluses, gérés par l'organisation.

Systèmes d'utilisateurs : tous les systèmes attribués à un utilisateur individuel et utilisés exclusivement par cette personne.

Systèmes informatiques ou d'information critiques : sur la base d'une analyse des risques, il faut déterminer si un système informatique ou d'information doit être considéré comme critique. Le caractère critique doit être considéré sur la base de l'importance d'un système informatique ou d'information dans la garantie de la confidentialité, de l'intégrité ou de la disponibilité des données et de la prestation de services IT.

T

Tiers : personne ou organisation étrangère à l'organisation, qui n'est pas concernée par un contrat comme partie contractuelle.

Token : moyen d'authentification utilisé pour contrôler l'identité de l'utilisateur. Un token comporte généralement des séries de chiffres qui font partie d'un mot de passe (exemple : token que peuvent demander des citoyens, token électronique délivré aux collaborateurs de l'organisation).

Traitement : toute opération ou ensemble d'opérations concernant des informations, effectué(e) ou non en recourant à des procédures automatisées, comme la collecte, l'enregistrement, l'ordonnancement, la conservation, la mise à jour, la modification, la demande, la consultation, l'utilisation, la fourniture via envoi ou diffusion ou la mise à disposition, la compilation ou la mise en relation d'une quelconque autre façon, de même que le verrouillage, l'effacement ou la destruction de données à caractère personnel.

Transaction : échange automatique de données entre systèmes IT sans intervention d'un utilisateur. Exemple : échange de données avec d'autres institutions publiques.

Transport : le transport physique de données désigne le déplacement du support (analogique ou numérique) ou le déplacement du matériel dans lequel serait intégré ce support. Implicitement, il est alors aussi automatiquement question de moyen de stockage mobile. Le transport électronique désigne la copie ou le traitement de données numériques. Le transport électronique concerne exclusivement des données numériques. Le transport électronique se caractérise par le fait que l'on ne déplace pas le moyen de stockage même, mais une copie des données.

U

UPS : UPS signifie *Uninterruptible Power Supply*. Il s'agit de l'alimentation électrique de secours qui entre en fonction lorsque l'alimentation électrique primaire habituelle tombe en panne.

Utilisateurs de systèmes d'information : tous les collaborateurs internes et externes, services et applications automatisés, parties externes (exemple : autres organisations) et clients (exemple : individus, entreprises, institutions).

V

Vendor lock-in : dépendance vis-à-vis d'un certain fournisseur cloud et problème pour passer d'un fournisseur à l'autre, en raison de l'absence de protocoles, API, structures de données (schéma) et modèles de service standardisés.

Virtual Private Cloud **(VPC)** : un cloud privé qui existe dans un cloud public ou partagé.

Z

Zone/espace/matériel critique : chaque organisation devra identifier les domaines les plus risqués et donc les plus critiques sur la base d'une analyse d'impact sur les activités (*business impact analyse*). On utilisera aussi à cet égard la classe DIC : Disponibilité, Intégrité et Confidentialité.

Gestion du document

Historique

Date	*Auteur*	*Version*	*Description des modifications*
28/10/2019	BOSA	v0.1	Draft
05/11/2019	BOSA	v0.2	Ajout de notions. Notamment CISO, data at rest, ... Suppression du lien avec autre politique
21/11/2019	FISP workgroup	V.1.1	Distribution publique

Approbations

Date	*Approbateur(s)*	*Version*
21/11/2019	FISP FISP workgroup	V1.0

Sources

Ce document a été rédigé à l'aide des sources suivantes :

- https://www.ksz-bcss.fgov.be/sites/default/files/assets/gegevensbescherming/mnm_minimale_normen_definities.pdf
- CEI 27000/2018
- “Basiskennis informatiebeveiliging op basis van ISO27001 en ISO27002”, Van Haren Publishing.