Gouvernance de la protection des données au sein du CIRB

Norme stratégique

Ce document traite de la gouvernance de la protection des données qui est d'application au sein du CIRB. Ce document interagit avec plusieurs autres directives et procédures dont il fait partie intégrante. Notamment, la politique de sécurité de l'information du CIRB

Pour rappel, l'autorité de contrôle attache beaucoup d'importance à cet objectif dans le cadre de la sécurité des données à caractère personnel.

Implication stratégique

L'information est une ressource qui, à l'instar d'autres moyens de production importants, représente une valeur considérable devant être protégée de manière appropriée. L'information peut exister sous diverses formes. Quelle que soit la forme que prend l'information et quel que soit le moyen de partage, de stockage ou de communication, elle doit toujours être protégée de manière adéquate.

Vu la dépendance croissante des organismes du service public à leur système d'information, l'information a acquis une valeur prépondérante pour ceux-ci. De plus, la protection des données à caractère personnel est un droit primordial, il convient donc de veiller à ce que le nouveau règlement européen sur la protection des données[1] soit rigoureusement respecté. Dans ce cadre, le CIRB, intervenant en tant que sous-traitant des administrations régionales traite (stocke, transmet, collecte, adapte, etc. …) des données à caractère personnel de ses clients et se doit de disposer d'une stratégie de sécurité de l'information et de protection de la vie privée.

En effet, le CIRB, soucieux de maîtriser les risques liés à ses systèmes d'information et conscient des enjeux associés, a décidé :

- De mettre en œuvre une approche globale et cohérente de protection de son patrimoine informationnel ;
- D'assurer une sécurité efficace et continuellement améliorée des informations stockées, traitées et produites par le CIRB dans le cadre de ses activités ainsi que

[1] Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

celles de ses clients, partenaires, employés, etc...

Contexte

La stratégie de la sécurité de l'information est référencée dans la politique de sécurité de l'information du CIRB. Cette politique tient donc lieu de cadre de référence pour l'accomplissement d'une gestion de la sécurité comme un processus à part entière au sein du CIRB. Elle constitue le socle visant à assurer la protection des informations sous la responsabilité du CIRB, ainsi que le respect de la législation en vigueur à l'égard des traitements et des échanges d'informations.

Les objectifs visés par la politique de sécurité du CIRB sont les suivants :

1. Le respect de la vie privée et des obligations légales se rapportant au traitement des données à caractère personnel,
2. La conformité à un ensemble de mesures de sécurité d'application dans le cadre du traitement des données précitées,
3. L'intégration de la sécurité de l'information au sein de la culture de l'organisation,
4. L'intégration des exigences sécuritaires requises dans les conventions liant l'organisation à des sous-traitants ou à des entités externes impliquées dans le traitement de données à caractère personnel,
5. La disponibilité, l'intégrité et la confidentialité des informations,
6. L'amélioration continue de la sécurité de l'information jusqu'à un niveau de maturité désiré.

Il en découle la présente gouvernance de la protection des données au sein du CIRB

cirb.brussels
IT is for you

Mesures organisationnelles et techniques

Le référentiel de mesures organisationnelles et techniques est basé sur le standard « ISO 27002 : 2013 - Code de bonnes pratiques pour le management de la sécurité de l'information ». Celui-ci a été constitué sur base d'analyses de risques et toutes les mesures reprises ci-dessous sont d'application au sein du CIRB :

Politique de la sécurité de l'information (ISO 27002 Sect.5)

1. Le CIRB a une politique de sécurité de l'information approuvée par la direction
2. Cette politique est revue périodiquement et interagit avec des politiques spécifiques (subordonnées) et des directives afin de préciser les obligations qui en découlent.

Organisation de la sécurité (ISO 27002 Sect. 6)

Organisation

1. Le CIRB dispose d'un comité de sécurité de l'information assurant le pilotage stratégique de la sécurité. En tant que comité décisionnel, sa mission est la mise en œuvre et le suivi du plan d'actions. Ce comité fixe les échéances et les responsabilités de la mise en pratique des différentes mesures considérées comme nécessaires pour atteindre le niveau de sécurité adéquat et valide la feuille de route de trois ans.
2. UN CISO et un DPO ont été désigné par le CIRB.
3. Le CISO et son équipe ont un rôle de coordination pour la mise en œuvre et l'application de la gouvernance sur la protection des données. Il intervient en tant que conseiller en sécurité de l'information dans tout nouveau projet, participe à l'homogénéisation du niveau de sécurité et se tient informé de l'état de l'art en matière de TIC, et contrôle le respect des exigences légales, dont la protection des données à caractère personnel.

1. Le télétravail est soumis à un contrôle d'accès à distance sécurisé via le VPN .
2. Une directive de sécurité « Télétravail et informatique nomade » est d'application

Sécurité des ressources humaines (ISO 27002 Sect. 7)

1. Tout collaborateur (interne et externe) du CIRB signe au travers de leur contrat de travail un engagement de confidentialité lors de son entrée en fonction.
2. Un rappel sur les obligations en matière de respect du secret professionnel et sur les clauses de confidentialité est effectué régulièrement au personnel (interne ou externe).
3. Une charte utilisateur présentant les limitations générales à l'utilisation des Systèmes d'Information du CIRB, des droits et obligations des utilisateurs, les contrôles réalisés par le conseiller en sécurité et les conséquences en cas de non -respect des règles, est transmise à chaque utilisateur lors de son arrivée. Ce document est porté à la connaissance de tout nouvel employé, qu'il soit embauché à titre temporaire, à titre définitif ou en tant qu'externe.
4. Des séances de sensibilisation à la sécurité et à la nouvelle réglementation européenne sur la protection des données sont menées régulièrement, les utilisateurs sont sensibilisés à leurs responsabilités et aux bonnes pratiques sécuritaires concernant la protection des données.

Gestion des actifs (ISO 27002 Sect. 8)

1. Tous les logiciels et serveurs utilisés sont repris dans des inventaires spécifiques.
2. Un registre d'activité de tous les traitements de données à caractère personnel que CIRB exécute est constitué et tenu à jour.
3. Des procédures relatives à la manipulation des actifs , notamment sur la mise en œuvre, l'utilisation, la restitution des actifs sont documentés et appliquées.

Contrôle d'accès logique (ISO 27002 Sect. 9)

1. Une directive « Contrôle d'accès » est d'application :

    1.1. L'identification de la personne se connectant au réseau est effectuée de façon formelle et non ambiguë. L'ensemble des utilisateurs (interne, tiers, etc.) possède un compte nominatif ; exception faite dans le cadre cité au 1.5 où des utilisateurs peuvent avoir recours à des comptes génériques.

    1.2. Les accès aux applications sont donnés après requête et validation, ou sur base du rôle, ou sur base de l'appartenance à une équipe. Seuls les accès nécessaires à la réalisation des tâches sont octroyés.

1.3. Une directive de mots de passe complexes d'accès ciblant l'ensemble des utilisateurs des SI (interne, tiers) est établie, respectant les préconisations relatives à la sécurité : complexité, longueur minimale, limite de tentatives d'accès, etc.

1.4. La procédure des mouvements (arrivée, départ ou mutation interne), est formalisée et inclut la mise à jour du référentiel et des droits d'accès associés. Elle prend en compte le profil et la durée de la mission du nouvel utilisateur (interne ou tiers). Cela inclus dans le processus d'entrée d'un nouvel employé, la création des comptes et des accès aux applications / au réseau et dans le processus de fin d'emploi, la désactivation des comptes de l'utilisateur.

1.5. Les utilisateurs avec des privilèges élevés sont limités et utilisés dans des cadres bien spécifiques d'utilisation (comptes génériques et comptes de service).

Chiffrement (ISO 27002 Sect.10)

1. Les bonnes pratiques concernant l'utilisation des clés de chiffrement et des certificats sont communiqués et disponibles sur le réseau.

Sécurité physique et environnementale (ISO 27002 Sect.11)

Zones sécurisées

1. Les périmètres de sécurité ont été clairement établis. Les zones sécurisées sont protégées contre toute tentative d'accès par effraction et munies d'un dispositif de sécurité d'accès physique progressif (niveaux et cloisonnement), adapté à la nature des risques liés à la circulation de personnes « non habilitées ».
2. Les bâtiments et salles informatiques sont protégées par des systèmes de détection d'incendie et d'intrusion.
3. L'accès aux locaux techniques et sensibles (salles informatiques) est nominatif et n'est autorisé qu'aux personnes habilitées. Les personnes habilitées sont enregistrées et les accès journalisés.
4. Les parkings sont isolés des autres zones du bâtiment par une porte équipée d'un contrôle d'accès (badge).
5. Seules les personnes enregistrées ou inscrites dans un registre des visites peuvent accéder au site. Les intervenants tiers non habilités par contrat et les visiteurs sont accompagnés par une personne habilitée.
6. La liste des personnels autorisés est régulièrement vérifiée.

1. Les éléments non dématérialisés, comme les archives, les produits finis sont stockés dans des locaux adéquats, afin de les protéger contre le vol et des dangers environnementaux.
2. Tous les équipements informatiques qui sont répertoriés comme importants ou vitaux sont installés dans des locaux sécurisés, appelés salle informatique ou locaux techniques
3. La protection des équipements sensibles est réalisée par des mesures de prévention et/ou de protection en fonction de leur sensibilité (protection incendie, climatisation, unités de secours électrique (UPS)).
4. Le matériel sensible (serveurs, équipements réseaux) est protégé contre les perturbations de l'alimentation électrique (surtension par exemple) et disposent d'une alimentation électrique de secours lui permettant de garantir la disponibilité du service attendu.
5. La mise au rebut ou la réaffectation de matériel informatique de bureau suit une procédure qui assure l'effacement des données confidentielles.
6. Pour les actifs classifiés sensibles, un contrat de maintenance est conclu avec un délai d'intervention ou de remplacement garanti, compatible avec les exigences de disponibilité et d'intégrité de l'actif.
7. La politique du bureau propre et de l'écran vide est connue par le personnel et d'application au sein de CIRB afin de ne laisser aucune information sensible sans surveillance.

Sécurité liée à l'exploitation (ISO 27002 Sect.12)

1. Les procédures opérationnelles sont décrites et disponibles et tout changement de systèmes se fait par un processus de gestion de changement. Les changements pouvant affecter la disponibilité des systèmes sont testés au préalable.
2. Les environnements de test, d'acceptation et de production sont séparés logiquement.
3. Des dispositifs contre des logiciels malveillants sont mis en place au niveau des postes clients et au niveau de l'infrastructure afin de se protéger contre les risques d'infection. Les mails entrant ou sortant de l'infrastructure sont scannés pour détecter et bloquer les virus. Les spams sont dans la mesure du possible automatiquement détectés et bloqués. Le personnel est informé régulièrement au sujet des malwares.
4. Une politique de sauvegarde est formalisée. Elle prend en compte : le

responsable de la sauvegarde, la fréquence, type (complète, incrémentale, différentielle), le support, la durée de rétention, des test réguliers de restauration et le contrôle de l'intégrité des données sauvegardées. De plus, une redondance suffisante est assurée afin de garantir une disponibilité adéquate.

5. La prise de traces est assurée au sein de l'infrastructure des Systèmes d'information du CIRB afin de répondre à :
    - La « conformité à la législation relative à la vie privée » ;
    - Aux requêtes judiciaires ;
    - Aux suivis des opérations ;

6. Les collaborateurs du CIRB ne sont pas autorisés à installer des logiciels sur les systèmes gérés entièrement par le CIRB dans les environnements d'acceptation et de production. L'installation ou la mise à jour de logiciels en exploitation est réalisée uniquement par des administrateurs qualifiés.

7. La standardisation de la configuration des systèmes d'exploitation garantit le niveau de sécurité adéquat.

8. Un processus formel de gestion des vulnérabilités techniques est défini et mis en place. Les systèmes exposés (internet / réseau IRISNet) sont scannés à intervalle régulier pour détecter les failles. Les failles rapportées sont traitées via le système de change management.

Sécurité des communications (ISO 27002 Sect.13)

1. L'architecture du réseau garantit le cloisonnement logique entre les différents domaines de confiance. Les équipements sont placés en fonction de leur sensibilité et du niveau de risque de la zone.
2. Des dispositifs de filtrage, de commutation et de routage sont configurés pour garantir uniquement la communication des flux autorisés.
3. Les flux sont rigoureusement sélectionnés sur base d'une liste standard de protocoles autorisés.
4. Toutes anomalies détectées par les dispositifs réseaux (Pare feux) et les caractéristiques des sessions établies sont enregistrées et archivées à des fins d'audit.
5. Les accès aux réseaux externes sont dupliqués. Les applications disponibles via des réseaux publics (internet, wifi ouverts, etc…) utilisent des protocoles sécurisés.

6. Des procédures de maintenance des équipements réseaux sont définies et mises en œuvre.
7. Les transferts d'information sensible sont effectués au moyen de protocoles sécurisés (contre l'altération ou la divulgation).

Acquisition, développement et maintenance des système d'information (ISO 27002 Section 14)

1. Les exigences de sécurité sont inclues dans les spécifications d'évolution d'infrastructure.
2. Un processus relatif au cycle de vie du développement est en place et les conseillers en sécurité sont inclus dès le début de tout nouveau projet.
3. Les concepts "Privacy by design or by default" sont maintenant intégrés dans le processus de développement.

La sous-traitance (ISO 27002 Section 15)

1. Les accords conclus avec les fournisseurs de services incluent une clause de confidentialité.
2. Les accords conclus avec les fournisseurs stipulent qu'ils prennent les dispositions nécessaires afin de veiller au respect des règles de protection des données à caractère personnel.
3. Suivant l'étendue du service demandé, les exigences de sécurité suivantes sont intégrées dans le cadre d'appel d'offres :
    3.1. Les responsabilités en matière de sécurité pour le CIRB et pour le sous-traitant.
    3.2. La vérification du respect des exigences de confidentialité et d'intégrité des informations.
    3.3. Les mesures de contrôle d'accès physique et logique à mettre en place et à respecter,
    3.4. Les mesures de continuité de service en cas de survenance d'un sinistre,
    3.5. Le niveau de protection physique des matériels confiés à des tiers,
    3.6. Le droit d'audit de l'application, des procédures et des installations de sécurité.

La gestion d'incident de sécurité (ISO 27002 Sect.16)

1. Une gestion d'incident et une gestion de crise est en place. Un log d'incident est constitué tenu à jour permettant de recenser les incidents, l'origine, la cause, l'impact sur la disponibilité, l'intégrité ou la confidentialité et les actions entreprises.
2. La documentation sur la gestion d'incident a été modifiée afin de remonter toute faille de sécurité et violation de données constatées. La procédure d'évaluation et de notification de l'incident relative à la vie privée est en place.
3. En cas d'infection (vers, virus, cheval de Troyes), faille de sécurité ou toute violation de données constatées ou soupçonnée sur un poste de travail, une procédure de réaction connue des utilisateurs est mise en place

La gestion de la continuité (ISO 27002 Sect.17)

1. Différentes procédures de secours informatiques existent et sont mises en œuvre afin de garantir la disponibilité des applications et services.
2. La plupart des composants critiques de l'infrastructure sont redondants. Les procédures de continuité de service sont régulièrement testées par l'équipe informatique.

La conformité (ISO 27002 Sect.18)

1. Les services juridique et sécurité s'assurent d'identifier les législations applicables et de mettre le CIRB en conformité.
2. Une directive de sécurité est d'application en ce qui concerne l'installation de logiciel sous licence et le stockage de médias avec droit d'auteur.
3. Des audits internes indépendants sont réalisés régulièrement sur la sécurité de l'information et les mesures d'amélioration sont proposées à la direction.
4. Une revue de sécurité technique du système d'information est réalisée périodiquement afin d'assurer que les contrôles de sécurité matériels et logiciels ont correctement été mis en œuvre.