Banque de la République d'Haïti

CIRCULAIRE

No. 126

AUX INSTITUTIONS FINANCIÈRES

La présente circulaire détermine les règles en matière de sécurité informatique auxquelles sont assujetties les institutions financières ce conformément aux articles 83 et 161 de la loi du 14 mai 2012 portant sur les banques et autres institutions financières.

1. Définitions

Les définitions suivantes s'appliquent à la présente circulaire :

a) **Sécurité informatique :** ensemble des moyens techniques et non techniques (organisationnels, juridiques, humains…) mis en place pour établir, conserver, rétablir et garantir la sécurité des systèmes informatiques.

b) **Système d'information :** ensemble organisé de ressources (matérielles, humaines, organisationnelles…) permettant d'acquérir, de traiter, de stocker, de diffuser des informations (sous forme de données, textes, images, sons, etc.) dans et entre les organisations.

c) **Système informatique :** ensemble composé de matériels, logiciels, réseaux et procédures d'utilisation. Ces derniers ont pour finalité d'élaborer, de traiter, de stocker, d'acheminer, de présenter ou de détruire des données numériques.

2. Dispositions générales

Les normes minimales de sécurité exposées ci-après s'appliquent au fonctionnement du système informatique des institutions financières. Ces normes doivent permettre la disponibilité, l'intégrité, la confidentialité et la traçabilité de toutes les données et informations gérées à travers le système informatique.

Il appartient aux institutions financières de mettre en œuvre les mesures de sécurité les plus appropriées compte tenu de leur situation spécifique et de l'importance des moyens de fonctionnement à protéger.

La mise en œuvre des normes minimales de sécurité par des tiers qui traitent des données pour le compte d'une institution financière doit être contrôlée par l'institution qui confie les travaux à ces tiers, ce conformément à la circulaire sur le contrôle interne.

3. Normes et standards

Les institutions financières sont tenues de mettre en œuvre les normes et standards suivants :

a) **Politique de sécurité informatique :** toute institution financière doit disposer d'une politique de sécurité informatique écrite et actualisée sur une base annuelle. Elle doit être approuvée par le conseil d'administration de ladite institution.

b) **Comité de sécurité informatique :** toute banque doit disposer d'un comité de sécurité informatique devant valider et approuver les mesures de sécurité informatique adoptées dans le cadre de la mise en œuvre de la politique de sécurité informatique. Cette fonction est dévolue au conseil d'administration pour les autres catégories d'institutions financières.

c) **Organisation de la sécurité informatique :** toute institution financière doit :
   - organiser, en son sein, un service ou département de sécurité informatique ou confier cette tâche à un prestataire spécialisé en sécurité informatique ;
   - disposer d'un plan de sécurité approuvé par le comité de sécurité informatique de l'institution concernée ou par la Direction Générale ;
   - disposer des moyens de fonctionnement nécessaires, approuvés par le comité de sécurité informatique de l'institution concernée et par le conseil d'administration, en vue de l'exécution de son plan de sécurité ;
   - installer un système et mettre en place des procédures permettant la détection, le suivi et la réparation d'infractions au niveau de la sécurité et proportionnées aux risques technique et opérationnel encourus ;
   - désigner un responsable de la sécurité informatique et veiller à ce qu'il dispose des données et accès nécessaires à l'exécution de sa mission. Ce responsable doit être indépendant du service informatique et rattaché soit au responsable de la gestion des risques soit directement à la Direction Générale ;
   - sensibiliser son personnel sur l'importance de la sécurité informatique.

d) **Inventaire :** toute institution financière doit disposer d'un inventaire du matériel informatique et des logiciels. Cet inventaire doit être tenu à jour de manière régulière en fonction des procédures mises en place.

e) **Classification de l'information :** toute institution financière doit classer les informations qu'elle détient selon leur niveau de confidentialité déterminé suivant des règles qu'elle aura préalablement définies.

f) **Protection des systèmes et données :** toute institution financière doit s'assurer que les données informatiques sont conservées dans des conditions appropriées à leur classification. Elle doit également disposer de systèmes actualisés pour se protéger (prévention, détection et rétablissement) contre des codes nocifs. L'institution financière doit implémenter un système de gestion sécurisé de l'accès pour les données nécessaires à l'application et à l'exécution de ses opérations.

Toute institution financière doit prendre les mesures adéquates pour protéger les données confidentielles enregistrées sur des périphériques mobiles, qui peuvent quitter le périmètre sécurisé de l'institution.

g) **Internet et messagerie électronique :** toute institution financière doit établir et appliquer un code de bonne conduite pour l'utilisation d'internet et de la messagerie électronique.

h) **Utilisation de données à caractère personnel :** toute institution financière doit informer les collaborateurs internes et les personnes externes associées au traitement de données à caractère personnel en ce qui concerne les obligations de confidentialité et de sécurité à l'égard de ces données.

i) **Protection de l'accès physique :** toute institution financière doit accorder l'accès aux bâtiments et locaux informatiques uniquement aux personnes autorisées et effectuer un contrôle à ce sujet tant pendant qu'en dehors des heures de travail.

j) **Incendie, intrusion, dégâts causés par un incident :** toute institution financière doit prendre des mesures pour la prévention, la protection, la détection et l'intervention en cas d'incendie, d'intrusion et de dégâts causés par l'eau.

k) **Alimentation en électricité :** toute institution financière doit disposer d'une alimentation en électricité alternative afin de garantir la continuité des activités.

l) **Accès aux systèmes informatiques par les gestionnaires informatiques :** l'accès aux espaces liés à la gestion et au développement du système informatique (département informatique, salle de serveurs, etc.) de toute institution financière doit être réservé aux gestionnaires informatiques identifiés, authentifiés et autorisés et aux prestataires externes le cas échéant, conformément aux politiques de sécurité informatique.

m) **Connexion externe :** toute institution financière doit utiliser des outils de sécurité adéquats pour protéger ses connexions externes.

n) **Respect des exigences de sécurité dans la conduite des projets informatiques :** toute institution financière doit disposer de procédures qui prennent en compte les exigences de sécurité de la présente circulaire dans le cadre du développement ou de l'évolution des systèmes informatiques.

Par ailleurs, l'institution financière doit veiller dans tout projet informatique à ce que les exigences de sécurité établies, au début de la phase de développement, avant toute mise en production de nouveaux systèmes ou d'évolutions importantes dans les systèmes existants soient respectées par le responsable du projet.

o) **Sécurité au niveau du réseau et accès à distance :** toute institution financière doit mettre en place les mesures techniques nécessaires, suffisantes et efficientes pour la protection adéquate de son réseau. Elle doit prendre les mesures adéquates afin de sécuriser l'accès à distance à ses systèmes et données.

p) **Documentation :** toute institution financière doit organiser la documentation appropriée de ses systèmes et applications informatiques acquis ou développés en interne et assurer sa mise à jour régulière par la consignation des évolutions ou correctifs dont ils font l'objet.

q) **Méthode de développement structurée :** toute institution financière doit adopter une approche structurée en vue d'un développement sécurisé des systèmes informatiques.

r) **Gestion d'incidents relatifs à la sécurité de l'information :** toute institution financière doit veiller à ce que le Comité de sécurité de l'information soit non seulement informé systématiquement des incidents susceptibles de compromettre la sécurité de l'information, mais aussi des mesures prises pour y faire face. Un recensement systématique des incidents doit être organisé et suivi par le Comité de sécurité de l'information et la direction générale.

s) **Gestion de la continuité :** toute institution financière doit :
- élaborer, tester et maintenir un plan de contingence basé sur une analyse des risques, afin d'assurer la continuité en toutes circonstances de ses activités ;
- prévoir et organiser un centre de migration informatique en cas de catastrophe totale ou partielle. Ce site de repli doit être éloigné du site principal, sécurisé et faire l'objet de tests réguliers ;
- s'assurer de la mise en place d'un système de sauvegarde (backup) faisant l'objet d'un contrôle régulier afin d'éviter la perte irréparable de données en cas de catastrophe totale ou partielle.

t) **Audit interne et externe :** toute institution financière doit faire procéder à un audit de la sécurité de son système informatique tous les trois (3) ans au plus. Une copie du rapport d'audit doit être annexée au rapport annuel sur le contrôle interne, conformément à la circulaire sur les normes minimales sur le contrôle interne.

4. Sanctions

A défaut par une institution financière de faire auditer son système informatique, selon la périodicité minimale prescrite de trois ans, la BRH peut, après avis donné à l'institution concernée, faire procéder à un audit informatique aux frais de l'institution financière. De plus, l'institution financière qui commet une telle violation est passible d'une pénalité de deux cent mille gourdes (HTG 200,000.00).

La BRH peut exiger d'une institution financière qu'elle redresse toute situation ayant trait à des violations relatives aux dispositions de la présente circulaire et à celles relevées dans le rapport d'audit informatique. A défaut de se conformer aux actions de redressement requises par la BRH, une institution financière est assujettie à une pénalité de cent mille gourdes (HTG 100,000.00) par jour d'infraction à partir de la date à laquelle l'infraction lui est notifiée par la BRH.

Toute amende sera déduite du solde de l'un des comptes de l'institution financière fautive à la BRH. Le paiement de toute amende par toute institution financière ne disposant pas de compte à

la BRH se fera par chèque de direction à l'ordre de la Banque de la République d'Haïti, au plus tard cinq (5) jours ouvrables, après réception de l'avis exigeant le paiement. En cas de non-paiement dans les délais, des pénalités de retard additionnelles de deux mille cinq cents gourdes (HTG 2,500.00) seront appliquées par jour de retard.

5. Mise en vigueur

Les dispositions de la présente circulaire entrent en vigueur le 1er février 2022.

Port-au-Prince le 13 janvier 2022

Jean Baden Dubois
Gouverneur