I. Objectif et champs d'application

Cette procédure a pour objet de définir les règles et les modalités de détection, de signalement, d'analyse, de traitement et de suivi des incidents de sécurité affectant le système d'information de la Banque de l'Union – Côte d'Ivoire (BDU-CI).

Cette procédure s'applique à l'ensemble des collaborateurs (employés, prestataires, sous-traitants) de la BDU-CI, ainsi qu'à toute personne ou entité disposant d'un accès aux ressources du système d'information, dans les cas suivants :

- Détection ou suspicion d'un incident de sécurité (intrusion, fuite de données, malware) ;
- Signalement d'un comportement anormal sur un poste ou une application ;
- Compromission avérée ou potentielle d'un compte utilisateur ou d'un équipement ;
- Tout événement pouvant affecter la sécurité des informations ou des services critiques.

II. Objectifs de la procédure

L'objectif de cette procédure est de définir les rôles, responsabilités et mécanismes opérationnels pour permettre la détection, la qualification, le traitement, la traçabilité et le retour d'expérience liés aux incidents de sécurité des systèmes d'information de la BDU-CI.

III. Rôles et responsabilités

Le comité sécurité

- Défini les orientations stratégiques et les décisions majeures liées à la gestion des incidents de sécurité de l'information ;
- Examine régulièrement les rapports d'incidents significatifs, les indicateurs de performance du dispositif de gestion des incidents liés à la sécurité de l'information, ainsi que les tendances et menaces émergentes ;
- Statue sur les mesures correctives à engager suite aux incidents majeurs ou récurrents, notamment lorsque ceux-ci présentent un impact opérationnel, réglementaire ou réputationnel ;

- S'assure que les ressources humaines, techniques et financières nécessaires au bon fonctionnement du dispositif de réponse aux incidents sont disponibles ;
- Contribue à l'amélioration continue de la politique de gestion des incidents et valide les propositions de mise à jour formulées par le RSSI ou le DSI ;
- Assure le lien avec les autres comités de gouvernance (comité des risques, comité de conformité, comité de continuité d'activité) pour garantir une gestion cohérente et transversale des incidents.

Le Responsable de la Sécurité des Systèmes d'Information (RSSI)

- Supervise le dispositif global de gestion des incidents liés à la sécurité de l'information ;
- Valide les procédures d'escalade, de communication, de réponse et de retour d'expérience en cas d'incident ;
- Coordonne les analyses de risques liées aux incidents détectés ou potentiels ;
- Assure la relation avec les équipes de réponse aux incidents (internes ou prestataires spécialisés – CERT /CSIRT/SOC) ;
- Participe à l'amélioration continue des dispositifs de réponse aux incidents liés à la sécurité de l'information à travers des tests réguliers et des exercices.
- Met à jour la présente procédure.

La Direction des Systèmes d'Information

- Déploie les outils techniques nécessaires à la détection, l'analyse, le traitement et la traçabilité des incidents de sécurité ;
- Veille à la disponibilité des ressources techniques pour assurer la continuité des opérations en cas d'incident ;
- Contribue aux revues post-incidents pour identifier les causes racines et proposer des mesures correctives.

Les Responsables Métiers

- Déclarent sans délai tout incident ou suspicion d'incident impactant leurs activités, leurs applications ou leurs données ;
- Participent à l'évaluation de l'impact métier d'un incident et à la priorisation des réponses à apporter ;

- Coopèrent avec les équipes techniques et sécurité lors de la gestion d'un incident affectant leur périmètre ;
- Contribuent aux retours d'expérience et à la mise en œuvre des actions correctives.

Equipe en charge de la réponse aux incidents

- ✓ **Les Equipes de supervision (N1) (Equipe de supervision N1 du CERT/SOC)**
- ✓ Elle est chargée de **surveiller en continu l'état du réseau, des applications, des systèmes et des dispositifs de sécurité**, de **détecter rapidement les anomalies ou incidents**, d'en **assurer le traitement initial** et, si nécessaire, de les **escalader** vers les niveaux techniques supérieurs (N2/N3) ou les équipes spécialisées (sécurité, infrastructure, applicatif, etc.). **Les analystes en sécurité (N2)**

Les **analystes en sécurité (N2)** sont des **spécialistes techniques** chargés d'**examiner en profondeur les alertes de sécurité** détectées par les outils de supervision (SIEM, EDR, IDS/IPS, firewalls, etc.), d'en **évaluer la gravité**, et de **coordonner la réponse appropriée.**

- ✓ **Les experts techniques spécialisés (N3)**

Les **experts techniques spécialisés (N3)** sont des **ingénieurs ou architectes de haut niveau**, responsables du **diagnostic avancé**, de la **remédiation définitive** et de l'**amélioration continue** des infrastructures techniques et de sécurité.

- ✓ **Le Comité de sécurité et/ou cellule de crise (N4)**

Lorsqu'un incident a un impact majeur ou systémique — par exemple, une propagation virale, une compromission massive, une interruption de services critiques, une perte financière importante, une atteinte à la réputation, ou une fuite de données réglementées ou sensibles — une escalade formelle est déclenchée vers le comité de sécurité. Ce dernier décide alors de la mise en place, ou non, d'une cellule de crise ainsi que de sa composition.

Le comité de sécurité, ou le cas échéant la cellule de crise, décide des actions stratégiques à mener, telles que la déconnexion d'équipements, l'activation du PCA/PRA, la déclaration aux autorités

compétentes (régulateur, autorités de protection des données), ainsi que la communication interne et externe.

IV. Sigles et Définitions

➢ Définitions

Incident de sécurité de l'information: Un incident lié à la sécurité de l'information est tout événement avéré ou suspecté susceptible de compromettre la confidentialité, l'intégrité ou la disponibilité des informations, qu'elles soient numériques ou physiques, ainsi que des systèmes et services informatiques

Revue post-morterm

Une revue post-mortem (ou retour d'expérience) est l'analyse réalisée après la résolution d'un incident de sécurité. Elle vise à comprendre les causes, évaluer la réponse, identifier les défaillances et proposer des améliorations pour éviter que l'incident ne se reproduise.

Playbooks

Un playbook est un guide opérationnel structuré, décrivant étape par étape comment réagir face à un type d'incident spécifique (phishing, ransomware, fuite de données, etc.). Il contient les procédures, outils, responsabilités, modèles de communication, etc.

Actifs critiques : Systèmes, données ou services dont la compromission aurait un impact significatif sur les opérations de la banque.

Analyse post-incident : Une analyse post-incident est l'étape qui suit la gestion d'un incident de sécurité (cybersécurité, sécurité physique).
Elle consiste à étudier en détail ce qui s'est passé, pour comprendre les causes, mesurer les impacts et surtout éviter que cela ne se reproduise.

➢ **Sigles**

SSSI : Service Sécurité des Systèmes d'Information

SI : Systèmes d'Information

DSI : Direction du Système d'Information

SI : Système d'Information ;

RSSI : Responsable de la Sécurité des Systèmes d'Information ;

DGGR : Direction Gestion Globale des Risques

Sommaire de la procédure

Table des matières

V. Références / Règles de gestion

❖ Documents de références

- Norme ISO/IEC 27001 : 2022 ;
- Politique de sécurité des systèmes d'information de la BDU-CI ;
- Politique de gestion des incidents de sécurité de l'information de la BDU-CI.

❖ Règles de gestion

➢ Classification des incidents

- **Les incidents simples, courants ou déjà documentés**

Ce sont des **événements de sécurité connus, maîtrisés et dont les procédures de réponse sont déjà établies**. Ils concernent la **sécurité des systèmes d'information** (SI), mais **n'impliquent pas une menace grave ou une compromission majeure**.

- **Incident inhabituel, impact potentiel non maîtrisé, informations insuffisantes**

Un **incident inhabituel** est un événement **non récurrent**, **non documenté** ou **peu fréquent**, pour lequel les équipes ne disposent pas encore de suffisamment d'informations pour déterminer :

- l'origine du problème,
- son impact réel ou potentiel sur les systèmes d'information,
- ou son niveau de gravité (mineur / majeur / critique).

- **Incident à forte technicité**

Un **incident de sécurité à forte technicité** désigne un **événement de sécurité complexe**, souvent **critique pour la continuité des activités**, qui **nécessite l'intervention d'experts hautement qualifiés** (sécurité, réseau, infrastructure, base de données, forensique, etc.) pour être analysé, contenu et résolu.

- **Incident a un impact majeur ou systémique**

Un **incident de sécurité à impact majeur ou systémique** est un **événement critique** qui compromet gravement la **sécurité, la disponibilité ou l'intégrité** des systèmes bancaires et qui **affecte directement la continuité des opérations**, **plusieurs services** ou **plusieurs entités** du groupe bancaire.

➢ Catégorisation des incidents

- **Les incidents simples, courants ou déjà documentés**

- Détection d'un fichier malveillant déjà connu et automatiquement mis en quarantaine par l'EDR (FortiEDR, Checkpoint, Defender) ;
- Réception d'un e-mail suspect signalé par un employé, mais déjà recensé dans la base de menaces ;
- Blocage automatique d'un compte après 3 tentatives de mot de passe incorrect ;
- Alerte de connexion SSH non réussie depuis IP interne connue (activité interne légitime) ;
- Poste non mis à jour détecté, mais procédure de mise à jour planifiée ;
- Employé signale une alerte antivirus déjà documentée (faux positif) ;
- Etc....

- **Incident inhabituel, impact potentiel non maîtrisé, informations insuffisantes**

  - Connexions anormales sur le serveur Core Banking ;
  - Processus applicatif qui s'arrête sans raison ;
  - Alerte SIEM sur comportement utilisateur anormal ;
  - Fuite d'information suspectée ;
  - E-mail de phishing non détecté par le filtre ;
  - Etc....

- **Incident à forte technicité**

  - Intrusion détectée sur un serveur Windows Core Banking avec élévation de privilèges ;
  - Trafic sortant anormal détecté via un pare-feu FortiGate vers une IP externe non répertoriée ;
  - Injection SQL ou exploitation d'une faille zero-day sur l'application de paiement SWIFT ;
  - Propagation d'un malware ciblé (phishing sophistiqué) via Outlook/Exchange ;
  - Corrélation d'alertes multiples indiquant une activité de type ransomware dans un environnement virtualisé ;
  - Attaque sur la console d'administration VMware ou Azure AD ;
  - Etc...

- **Incident a un impact majeur ou systémique**

Type d'incident	Description	Impact
Attaque par Ransomware sur le Datacenter bancaire	Chiffrement de serveurs Core Banking, systèmes de paiement et fichiers clients.	Interruption totale des services, perte d'accès aux données, risque de fuite d'informations.
Intrusion sur le réseau central	Compromission d'un compte administrateur et exfiltration de données clients.	Atteinte à la confidentialité et risque de sanctions réglementaires.
Panne prolongée du système Core Banking	Défaillance critique du cluster de base de données sans basculement possible.	Interruption des opérations de guichet et des transactions.
Attaque DDoS massive	Saturation des serveurs de banque en ligne et mobile banking.	Indisponibilité des canaux digitaux pour tous les clients.

Erreur de configuration de sécurité sur le réseau SWIFT	Transactions non sécurisées ou détournement potentiel.	Risque financier systémique et atteinte à la crédibilité institutionnelle.
Fuite de données massives (exfiltration)	Données personnelles et financières de milliers de clients divulguées.	Risque juridique, financier et réputationnel majeur.

❖ **Contrôles permanents et périodiques**

- Un contrôle de premier niveau est réalisé **mensuellement** par la Direction des Systèmes d'Information (DSI), en collaboration avec le Responsable du SOC, afin de veiller au respect opérationnel des principes et exigences définis par la présente politique, notamment en matière de détection, de traitement et de communication des incidents de sécurité.

- Des contrôles de second niveau sont effectués **trimestriellement** par le Responsable de la Sécurité des Systèmes d'Information (RSSI). Ils visent à évaluer la cohérence, l'efficacité et la conformité de l'application des dispositions de cette politique sur l'ensemble des périmètres concernés.

- Un contrôle de troisième niveau est conduit **annuellement** par la Direction de l'Audit Interne, en vue d'apprécier l'adéquation, la fiabilité et la conformité du dispositif global de gestion des incidents de sécurité, ainsi que de formuler, le cas échéant, des recommandations d'amélioration continue.

VI. Narratif de la procédure		
PRO-RSSI-SSI-09	Procédure de gestion des incidents de sécurité des systèmes d'information	RSSI, DSI, Comité Sécurité, users, Direction générale.

Acteurs	**Descriptions des tâches**	**Outils et interfaces**
I. <u>Supervision et détection des évènements pouvant conduire à un incident de sécurité de l'information</u>		
Tous les employés, sous-traitants et prestataires de services tiers	**Lorsqu'un incident de Cyber sécurité est détecté** – Signaler par mail l'incident détecté à l'équipe de supervision (N1) ou le centre de services (SOC ?) via l'adresse **alerte.incident@bduci.com**. En cas d'indisponibilité de la messagerie ou de situation d'urgence, le signalement téléphonique doit être privilégié. Dans tous les cas, l'envoi ultérieur d'un mail reste obligatoire afin d'assurer la traçabilité du signalement. – Renseigner une Fiche de déclaration d'incidents et de pertes opérationnelles avec les informations dont il dispose puis la transmettre par mail au RSSI avec en copie la DSI et la DGGR – Le RSSI se charge de compléter les éventuelles informations manquantes sur la fiche de déclaration d'incidents et de pertes opérationnelles.	Hotline sécurité / DSI (liste de numéros de téléphone de l'équipe en charge de la réponse aux incidents), Fiche de déclaration d'incidents et de pertes opérationnelles Outil de ticketing / SIEM avec alerte automatique Adresse mail
II. <u>Analyse des incidents après détection</u>		
Les équipes de supervision (N1)	- Réceptionner le mail ou l'appel téléphonique de déclaration d'incident. - **Attribuer un identifiant** unique pour le suivi.	Adresse mail Hotline sécurité / DSI

Acteurs	Descriptions des tâches	Outils et interfaces
	- Analyser et qualifier les incidents conformément à la politique de gestion des incidents de sécurité de l'information. - **Enregistrer l'incident** dans le registre des incidents de cyber sécurité **S'il s'agit d'un incident simple, courant ou déjà documenté,** traiter l'incident en s'appuyant sur les fiches réflexes ou les playbook correspondantes à chaque type d'incident. **Si l'incident** ne peut être résolu par l'équipe de supervision(N1), transférer par mail, le traitement aux analystes sécurité de niveau 2 - Informer par mail les parties prenantes internes (RSSI, DSI, direction générale ou le comité de crise si nécessaire, ...).	Outil de ticketing / SIEM avec alerte automatique Fiche de déclaration d'incidents et de pertes opérationnelles Outil de ticketing / SIEM avec alerte automatique Adresse mail liste de numéros de téléphone de l'équipe en charge de la réponse aux incidents Rapport détaillé d'incidents Base d'incidents fiches réflexes ou des playbook
III. <u>Traitement de l'incident</u>		
<u>Cas d'incidents de Cyber sécurité</u>		
Analystes en sécurité (N2) **/** **RSSI** **/** **DSI**	- Réceptionner le mail de traitement de l'incident - Analyser les incidents escaladés. Si incident inhabituel à impact potentiel non maîtrisé, informations insuffisantes :	Rapport d'analyse Plan d'action détaillé, décrivant les étapes à suivre pour gérer les

Acteurs	Descriptions des tâches	Outils et interfaces
	○ engager sans délai les actions de réponse adaptées à la criticité et à la nature de l'incident (attaque, compromission, indisponibilité, fuite de données, etc.) en collaboration avec l'équipe de réponse aux incidents. ○ limiter la propagation ou les effets de l'incident par des actions techniques rapides : isolement du système affecté, désactivation de comptes compromis, coupure réseau, etc. ○ identifier et corriger les vulnérabilités exploitées (patchs, reconfiguration, restauration depuis une sauvegarde saine), en veillant à éviter toute réapparition de l'incident. ○ Conserver de manière sécurisée les éléments de preuve (fichiers logs, images disques, captures d'écran, etc.) nécessaires à une analyse forensic, à une procédure judiciaire ou à un audit, conformément à la chaîne de conservation des preuves prévue par la législation applicable. ○ enregistrer systématiquement toutes les mesures prises (techniques, organisationnelles, communication, décisions), avec date, heure et responsables associés. ○ adapter la réponse à l'impact de l'incident sur les systèmes critiques, les données sensibles, la disponibilité des services, ou la réputation de l'organisation.	incidents de sécurité

Acteurs	Descriptions des tâches	Outils et interfaces
	- informer les parties prenantes internes conformément à la politique de gestion des incidents de sécurité de l'information : RSSI, DSI, responsables métiers, direction générale, comité de crise si nécessaire. - établir, si nécessaire, la communication avec les autorités compétentes (régulateur, autorité de protection des données, etc.), ainsi qu'avec les partenaires ou clients, en fonction du type d'incident. Si incident à forte technicité, transférer par mail, le traitement aux **experts techniques spécialisés (N3)**	
Experts techniques spécialisés (N3)	- Réceptionner le mail de traitement de l'incident. - Réaliser des investigations approfondies - Identifier la cause racine (Root Cause Analysis) des incidents récurrents ou critiques - Corriger la cause profonde (Root Cause Analysis). - Déployer des correctifs, reconfigurations ou patchs. - Conseiller le RSSI et le comité de crise. - Si incident a un impact majeur ou systémique, transférer le traitement de l'incident au Comité de sécurité	Plan d'action détaillé, décrivant les étapes à suivre pour gérer les incidents de sécurité
Comité de sécurité	- Décider des actions stratégiques à mener - Activer le PCA/PRA - Déclarer aux autorités compétentes (régulateur, autorités de protection des	Plan de Continuité d'Activité

Acteurs	Descriptions des tâches	Outils et interfaces
	données), ainsi que la communication interne et externe	
IV. <u>Action post-incident</u>		
Equipe en charge de la réponse aux incidents	- organiser systématiquement une revue post-morterm pour chaque incident majeur et significatif. - identifier les causes profondes, les défaillances techniques, humaines ou organisationnelles ayant conduit à l'incident. - analyser le temps de détection, le temps de réponse, la coordination entre les équipes, et l'efficacité des mesures de remédiation. - Documenter de manière rigoureuse et structurée l'ensemble de l'incident, en retraçant toutes les étapes : détection, analyses menées, actions mises en œuvre, communications réalisées et décisions prises. - archiver les rapports techniques, les journaux, les indicateurs, les preuves numériques et les recommandations. - mettre à jour les politiques de sécurité, procédures d'intervention, guides techniques et référentiels internes selon les enseignements tirés. - ajuster les règles de détection dans les outils (SIEM, EDR, IDS) pour prévenir la réapparition du scénario. - mettre en œuvre de nouveaux contrôles correctifs ou préventifs : segmentation réseau, durcissement, filtrage, supervision renforcée. - intégrer les nouvelles menaces identifiées dans la cartographie des risques, le registre des vulnérabilités et enrichir la base des IOC. - ajouter les incidents traités, leurs causes et leurs traitements dans une base de connaissance interne ou dans des playbooks d'incidents. - partager ces éléments avec les équipes concernées pour améliorer la réactivité future. - confirmer ou compléter les notifications officielles transmises aux autorités (ex. :	Rapport d'incident

Acteurs	Descriptions des tâches	Outils et interfaces
	régulateur bancaire, autorité de protection des données). - préparer un rapport final de conformité, si l'incident est soumis à une obligation de déclaration. - informer les collaborateurs des leçons tirées et des bonnes pratiques à renforcer, sans exposer inutilement les détails techniques. - intégrer les nouveaux scénarios dans les campagnes de sensibilisation ou formations ciblées. - mettre à jour les clauses contractuelles ou renforcer les obligations en matière de sécurité. - réévaluer si nécessaire la performance des prestataires impliqués dans l'incident. - définir, suivre et clôturer formellement les actions correctives issues du plan d'action de résolution d'incident et de la revue post-incident. - déclarer officiellement par la voie du responsable de résolution de l'incident que l'incident est résolu et clôturé	

Annexes / Enregistrements

- **Fiche de déclaration d'incidents et de pertes opérationnelles**
- **Liste des membres de l'équipe de réponse aux incidents**
- **Hotline sécurité / DSI (liste de numéros de téléphone de l'équipe en charge de la réponse aux incidents)**

Liste des ampliations

N°	Structures	Date	Visa	Observations
01				
02				

Liste des modifications

N°	Nature de la modification	Date	Chapitre ou page concerné (e)	Observations
01				
02				

Rédigé par : RESPONSABLE DE LA SECURITE DES SYSTEMES D'INFORMATION	Validé par : COMITE PROCEDURES	Approuvé par : DIRECTION GENERALE
Date : 06/11/2025	Date : 06/11/2025	Date :
Signature :	Signature :	Signature :