EBIOS
ÉTUDE DE CAS

RÉDIGÉS PAR : ANCELLY , BARBIER, CALPETARD, HOUTMANN

DE LA RÉUNION
Institut Universitaire de Technologie

2024- 2025

Sommaire:

1. Introduction :

L'Université de la Réunion (UR) fait face à un enjeu de taille : la sécurisation de son système d'information, devenu de plus en plus complexe et vulnérable aux menaces croissantes de la cybersécurité.

Au cœur de ce défi se trouve le service des finances, dont le rôle crucial dans le fonctionnement de l'établissement exige une attention particulière en matière de sécurité.

Ce service est responsable de la gestion budgétaire, de la comptabilité, des marchés publics et du traitement des salaires, des données souvent sensibles et stratégiques pour l'université.

L'activité du service est néanmoins irrégulière, concentrée principalement en fin de mois pour la paie et de manière plus intense en novembre et décembre lors de la clôture budgétaire.

La Direction du Système d'Information (DSI) a donc initié une démarche proactive pour renforcer la sécurité de ses systèmes d'information.

Pour cela, elle a choisi la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) afin de mener une analyse méthodique des risques et de définir une Politique de Sécurité du Système d'Information (PSSI) robuste et adaptée au contexte spécifique de l'UR.

Cette méthode permet d'identifier les vulnérabilités, d'évaluer les risques et de proposer des mesures de sécurité concrètes et priorisées. La présente étude de cas se focalise sur la sécurité du système d'information financier de l'université, plus précisément sur le logiciel SIFAC (Système d'Information Financier Analytique et Comptable), qui est au cœur des opérations financières de l'établissement.

a) Périmètre de l'étude :

L'étude se concentrera sur le périmètre du système d'information du service des finances intégrant le logiciel SIFAC, ainsi que ses éléments associés : les serveurs d'hébergement, les bases de données, les systèmes de sauvegarde, les accès réseaux, les postes de travail des agents, et les principaux processus métiers du service des finances directement liés à SIFAC. D'autres systèmes d'information, non liés directement au service des finances, ne seront pas inclus dans le périmètre de cette étude.

b) Objectifs :

Cette étude EBIOS vise plusieurs objectifs clés :

- Identifier et analyser méthodiquement les risques: Recenser l'ensemble des menaces et vulnérabilités potentielles affectant le système SIFAC et son écosystème.
- Évaluer quantitativement les risques: Attribuer des scores de probabilité et d'impact à chaque risque afin d'établir une hiérarchisation claire.
- Définir les mesures de sécurité appropriées: Proposer un ensemble de mesures concrètes et réalistes pour réduire les risques identifiés.
- Élaborer un plan d'action: Définir un échéancier précis pour la mise en œuvre des mesures de sécurité, en précisant les responsabilités et les ressources nécessaires.
- Garantir la continuité d'activité: Assurer la disponibilité du système SIFAC, particulièrement lors des pics d'activité, et minimiser l'impact d'éventuels incidents.
- Protéger les données sensibles: Protéger la confidentialité, l'intégrité, et la disponibilité des données financières et personnelles traitées

par le système SIFAC, en conformité avec la règlementation applicable (RGPD notamment).

2. Présentation de l'organisme étudié :

L'Université de la Réunion (UR) est un établissement public d'enseignement supérieur et de recherche pluridisciplinaire, accueillant plusieurs milliers d'étudiants et employant un personnel conséquent composé d'enseignants-chercheurs, de personnels administratifs et techniques.

Son organisation est complexe, répartie sur plusieurs sites, et gérant des ressources financières importantes, soumises à des réglementations strictes imposées par les règles de la comptabilité publique.

La DSI (Direction du Système d'Information) joue un rôle central dans le bon fonctionnement de l'université en assurant la gestion, le maintien et la sécurité de l'ensemble de son système d'information.

Le service des finances de l'UR est un service critique de l'université, jouant un rôle essentiel dans sa gestion administrative et financière. Il assure différentes missions clés pour le bon fonctionnement de l'ensemble de l'établissement.

a) Activités principales du service des finances:

Le service des finances de l'UR est structuré pour gérer efficacement les flux financiers et la comptabilité de l'université. Ses principales activités se répartissent en quatre pôles :

- **Pôle Comptabilité:** Responsable de la comptabilité générale, de la comptabilité analytique et de la gestion de trésorerie. Ce pôle traite un grand volume de données financières quotidiennes, incluant les recettes et les dépenses de l'établissement.

- **Pôle Budget:** Ce pôle est chargé de l'élaboration du budget annuel de l'université, de son suivi d'exécution, et du contrôle budgétaire. Il

travaille en étroite collaboration avec les différents services de l'université pour la planification et la gestion des ressources. Il assure également la production de rapports réguliers sur l'état des finances de l'établissement.

- **Pôle Marchés publics:** Ce pôle assure la gestion des appels d'offres, le suivi des contrats avec les fournisseurs, et les relations avec ces derniers. Il gère un important volume de documents administratifs et financiers liés aux marchés publics.
- **Pôle Paie:** Ce pôle est le plus sensible, responsable du traitement des salaires de l'ensemble du personnel de l'université, incluant la gestion des primes, des indemnités et des déclarations sociales et fiscales. Il fait appel à des données personnelles et bancaires sensibles et respecte une réglementation extrêmement stricte.

b) Système d'information global:

Le bon fonctionnement de ces pôles et des activités qu'ils gèrent repose sur le système d'information du service des finances, basé sur l'application SIFAC.

Ce système est hébergé sur des serveurs sécurisés dans le bâtiment de la DSI. Il comprend plusieurs composants clés :

- **Serveurs et infrastructures:** Serveurs dédiés hébergeant SIFAC, bases de données relationnelles, serveurs de sauvegarde et de réplication, et infrastructure réseau sécurisée.
- **Logiciel SIFAC:** Application principale de gestion financière et comptable, intégrant les modules nécessaires au traitement des données financières pour chaque pôle du service des finances.
- **Modules complémentaires:** Des modules intégrés au sein de SIFAC, ou des applications interfacées, permettent la gestion des aspects spécifiques comme le calcul et le versement des salaires (pôle paie).

- **Postes de travail:** Les agents du service des finances travaillent sur des postes de travail sécurisés, équipés de logiciels adaptés à leurs tâches.

La robustesse et la sécurité de ce système d'information sont primordiales pour assurer la continuité des opérations financières de l'Université de la Réunion et la protection des données sensibles.

La DSI assure la maintenance et la sécurité de ce système, en accord avec les directives de la direction de l'université. L'étude EBIOS permettra de renforcer encore ce dispositif existant.

3. Module 1 : Étude du contexte

Ce module vise à analyser l'environnement du système d'information financier de l'Université de la Réunion afin d'identifier les enjeux et les contraintes qui influenceront les choix de sécurité.

a) Identification des enjeux métier:

Le service des finances de l'Université de la Réunion joue un rôle central dans le bon fonctionnement de l'établissement.

Sa mission est essentielle pour la gestion financière de l'université, la conformité réglementaire et la stabilité de l'institution. Les enjeux sont multiples et peuvent se résumer en trois axes principaux :

- **Enjeux Financiers:** La gestion rigoureuse du budget annuel (estimé à 100 millions d'euros), la sécurisation des transactions financières (environ 5000 transactions par mois en moyenne) et la prévention des fraudes financières sont des préoccupations majeures. Une fraude, même à petite échelle, pourrait avoir de fortes répercussions sur la réputation de l'université et entraîner des sanctions, avec un impact financier potentiellement important, de même que des coûts de gestion de crise importants.

- **Enjeux Opérationnels:** La continuité des opérations financières quotidiennes est indispensable. L'indisponibilité du système SIFAC, même pour une courte période, pendant le traitement des payes (plus de 500 employés) ou la clôture budgétaire, peut entraîner des retards de paiement avec des conséquences sociales significatives et une dégradation de l'image de l'université. Ceci induit des coûts importants tant au niveau des ressources humaines que de la gestion des relations avec les employés.

- **Enjeux Réglementaires:** L'UR, en tant qu'établissement public, est soumise à des réglementations strictes en matière de comptabilité publique et de protection des données personnelles (RGPD). Toute violation de ces réglementations peut entraîner des sanctions financières importantes et des dommages importants à la réputation de l'université.

b) Définition du périmètre de l'étude de sécurité:

L'étude EBIOS portera sur le système SIFAC et son écosystème direct, incluant :

- **Système SIFAC:** Le logiciel de gestion financière et comptable, incluant tous ses modules et bases de données associées.

- **Infrastructures:** Les serveurs physiques sur lesquels SIFAC est hébergé, les équipements réseau permettant l'accès au système, les systèmes de sauvegarde et de réplication des données.

- **Accès et Utilisateurs:** Le contrôle d'accès au système, les authentifications, et la gestion des habilitations pour les 25 utilisateurs qui accèdent directement à SIFAC.

- **Processus métiers:** Les processus de travail directement associés à l'utilisation de SIFAC (paie, comptabilité, budget, marchés publics). Les processus non directement gérés par SIFAC sont exclus de cette étude initiale.

c) Paramètres à prendre en compte:

- **Temporalité:** Le système SIFAC est soumis à des pics d'activité importants en fin de mois (paies) et en fin d'année (clôture

budgétaire). Ces pics augmentent sensiblement le risque de surcharges et de pannes.

- **Volumétrie des opérations:** Le volume de données traitées par SIFAC est important (plus de 10 Go de données générées chaque mois), nécessitant une gestion et une maintenance appropriées tenant compte de la croissance prévisible des volumes de données.

- **Criticité des données:** Les données traitées par SIFAC incluent des informations financières sensibles et des données personnelles des agents de l'université. La protection de ces données est primordiale.

d) Contraintes applicables:

- **Contraintes Techniques:** Disponibilité maximale du système SIFAC (objectif de 99,9% de disponibilité), performance du système pendant les pics d'activité, interopérabilité avec les systèmes existants de l'université. Le choix des solutions doit prendre en compte l'évolution probable des besoins et des volumes de données dans les années à venir.

- **Contraintes Organisationnelles:** Respect des processus de validation internes, séparation des tâches pour limiter les risques d'erreur humaine, et implication des parties prenantes dans la mise en œuvre des mesures de sécurité.

- **Contraintes Réglementaires:** Respect strict du RGPD pour les données personnelles, et des réglementations spécifiques à la comptabilité publique.

Ce module a établi les enjeux, le périmètre, les paramètres, et les contraintes de l'étude de sécurité pour le système SIFAC.

Les modules suivants approfondiront l’identification et l’évaluation des risques selon la méthode EBIOS. Le coût des solutions sera optimisé pour répondre au mieux aux besoins de sécurité tout en restant compatible avec les ressources d'une université.

4. Module 2 : Étude des événements redoutés

Ce module vise à identifier et à caractériser les événements indésirables susceptibles d'affecter le fonctionnement du système d'information financier de l'UR et, plus précisément, le système SIFAC.

L'objectif est de dresser un inventaire des situations critiques qui pourraient avoir des conséquences significatives sur l'université.

a) Sources de menaces:

L'analyse des sources de menaces a permis d'identifier plusieurs catégories, classées selon leur origine et leur nature:

- **Menaces Humaines Internes:** Ces menaces proviennent du personnel de l'UR. Elles peuvent être accidentelles (erreurs de manipulation, négligences) ou malveillantes (vol, sabotage, fraude interne). L'analyse des profils d'accès et des droits des utilisateurs permet d'évaluer la gravité d'événements liés à des acteurs internes malveillants.

- **Menaces Humaines Externes:** Ces menaces proviennent de l'extérieur de l'UR. Leurs motivations sont souvent malveillantes (cyberattaques, vol de données, hameçonnage). Il est crucial d'évaluer les risques liés aux failles de sécurité potentielles permettant l'accès non autorisé au système.

- **Menaces Techniques:** Ces menaces correspondent aux incidents techniques liés aux équipements, aux logiciels, ou aux infrastructures réseaux. Elles peuvent être accidentelles (pannes matérielles, bugs logiciels, coupures de courant) ou malveillantes (attaques par déni de

service – DDoS, intrusions). La vétusté du matériel ou l'absence de maintenance adéquate augmentent la probabilité de ce type d'événement.

- **Menaces Environnementales:** Dans le cas de l'UR, le risque de catastrophe naturelle (cyclone, tremblement de terre) est faible, mais doit être pris en compte dans la stratégie globale de sécurité. Cette menace est peu probable mais l'impact peut être très important au regard des pertes de données et des coûts de remise en état des infrastructures.

b) Identification des biens sensibles:

L'identification des biens sensibles permet de déterminer les éléments critiques qui, s'ils étaient compromis, pourraient causer le plus de dommages à l'université. Pour le service des finances, les biens sensibles comprennent :

- **Système SIFAC:** Le logiciel SIFAC et ses données configurent l'actif principal, dont l'indisponibilité aurait des conséquences significatives.
- **Bases de données:** Les bases de données contenant les informations financières et les données personnelles des employés, des étudiants, et des partenaires de l'université.
- **Serveurs d'hébergement:** Les serveurs physiques hébergeant SIFAC et ses bases de données.
- **Système de sauvegarde:** Le système de sauvegarde est critique pour assurer la résilience du système en cas d'incident.
- **Réseau:** L'infrastructure réseau assurant la connectivité entre les différents éléments du système.
- **Postes de travail:** Les postes de travail des agents du service des finances sont également considérés comme sensibles en raison des droits d'accès qu'ils possèdent.

c) Analyse des impacts potentiels:

L'analyse des impacts potentiels vise à déterminer la gravité des conséquences d'un événement redouté. Les impacts peuvent être financiers, opérationnels, réglementaires, et réputationnels :

- **Impact financier:** Perte de données, coût de la remise en état du système, amendes en cas de non-conformité (RGPD), pertes liées à des fraudes.
- **Impact opérationnel:** Arrêt du système SIFAC et interruption de la gestion financière, retards de paiements, difficulté à respecter les échéances réglementaires.
- **Impact réglementaire:** Sanctions financières pour non-respect du RGPD, des réglementations de la comptabilité publique.
- **Impact réputationnel:** Atteinte à la crédibilité de l'université, perte de confiance des partenaires, des étudiants et des employés.

d) Classification des événements redoutés (Tableau récapitulatif):

Un tableau récapitulatif, présenté dans le Module 4, permettra de classifier les événements redoutés en fonction de leur probabilité et de leur impact (voir Module 4). Ce tableau sera le point de départ de l'évaluation des risques.

5. Module 3 : Étude des scénarios de menaces

Ce module vise à élaborer des scénarios de menace concrets basés sur les événements redoutés identifiés précédemment. L'objectif est de décrire des situations réalistes pour mieux évaluer les risques associés. Chaque scénario est décrit, sa probabilité et son impact sont évalués, contribuant à la hiérarchisation du risque global.

a) Identification des scénarios de menaces:

Plusieurs scénarios de menaces sont envisageables, illustrant des combinaisons de failles avec des risques différents:

- **Scénarios liés à l'indisponibilité du système SIFAC:**
  - **Panne matérielle:** Défaillance d'un serveur ou d'un élément réseau critique, entraînant une indisponibilité partielle ou totale du système SIFAC. La probabilité est jugée faible mais l'impact serait très élevé en cas de défaillance pendant un traitement de paie ou une échéance comptable.
  - **Attaque par déni de service (DDoS):** Un flot massif de requêtes sur le système SIFAC provoque son indisponibilité pour les utilisateurs légitimes. La probabilité est jugée modérée, et l'impact pourrait être élevé selon la durée et l'intensité de l'attaque.
  - **Erreur de configuration:** Une mauvaise configuration du système ou une erreur humaine lors de la maintenance peut rendre le système SIFAC indisponible. La probabilité est jugée modérée en fonction du niveau de compétence des administrateurs et des tests effectués, mais l'impact est moyen.
- **Scénarios liés à la compromission des données:**
  - **Piratage:** Un attaquant accède illégalement au système SIFAC en exploitant une vulnérabilité de sécurité (ex: injection SQL). La probabilité est faible si des mises à jour sont régulières et que les failles connues sont corrigées rapidement, mais

l'impact pourrait être catastrophique, avec vol de données, compromission de la réputation, et sanctions financières.
    - **Hameçonnage (Phishing):** Les employés reçoivent des courriels frauduleux leur demandant leurs identifiants de connexion à SIFAC. La probabilité est modérée, en fonction de la sensibilisation à la sécurité des employés, l'impact peut aller de faible à élevé en fonction des droits de l'utilisateur ciblé.
    - **Attaque par ingénierie sociale:** Un individu, par manipulation ou ruse, obtient les informations d'accès au système SIFAC et accède donc aux données. La probabilité est faible, mais l'impact est très élevé si l'attaquant obtient les droits d'un administrateur système.
- **Scénarios liés à la perte ou à la corruption des données:**
    - **Catastrophe naturelle:** Un évènement naturel tel qu'une inondation impacte le bâtiment hébergeant les serveurs de la DSI. Bien que peu probable, l'impact sur la perte de données et la continuité d'activité serait très important.
    - **Erreur humaine:** Une mauvaise manipulation, une suppression accidentelle de données par un employé, ou une défaillance humaine lors d'une restauration de données peut conduire à une perte ou une corruption de données critiques. La probabilité est assez élevée en fonction de la qualité des procédures en place et de la formation des utilisateurs. L'impact est moyen.

b) Évaluation des scénarios:

Pour chaque scénario, une évaluation quantitative de la probabilité et de l'impact sera présentée au Tableau des risques du module 4. Cette évaluation nécessite une analyse approfondie tenant compte des mesures de protection déjà existantes et de la vulnérabilité du système.

c) Détermination des objectifs de sécurité:

L'analyse des scénarios de menace permet de définir des objectifs de sécurité clairement mesurables. Ainsi, des objectifs quantifiables viendront compléter les objectifs qualitatifs déjà mentionnés:

- **Disponibilité:** Objectif de disponibilité de SIFAC supérieur à 99,9 % pendant les périodes critiques (clôture budgétaire, paie). Temps de restauration maximal (RTO) de 4 heures en cas de panne.
- **Confidentialité:** Chiffrement des données au repos et en transit pour protéger les informations sensibles.
- **Intégrité:** Mécanismes de contrôle d'accès pour restreindre l'accès aux données sensibles, audit complet des opérations, et validation multi-niveaux des transactions financières.
- **Résilience:** Plan de continuité d'activité (PCA) robuste incluant des moyens de reprise et de restauration des données (sauvegardes régulières et tests réguliers).

6. Module 4 : Étude des risques

Ce module vise à analyser les risques identifiés précédemment, en les quantifiant et en les hiérarchisant afin de prioriser les actions de sécurité.

a) Analyse des risques:

L'analyse des risques combine l'évaluation de la probabilité d'occurrence de chaque scénario avec l'évaluation de son impact potentiel. Plusieurs méthodes d'évaluation des risques existent (qualitative, quantitative...). Dans le cadre de cette étude, une approche semi-quantitative a été retenue afin d'obtenir une hiérarchisation des risques claire tout en tenant compte des aspects subjectifs. Une échelle de 1 à 5 est utilisée pour la probabilité (1 = Très faible, 5 = Très élevée) et l'impact (1 = Négligeable, 5 = Catastrophique).

b) Évaluation des risques:

Le tableau suivant présente la matrice d'évaluation des risques, basée sur les scénarios de menace décrits dans le module précédent. Les scores de probabilité et d'impact sont des estimations basées sur l'expérience et l'analyse du système SIFAC, en prenant en compte les mesures de sécurité déjà en place. Un score de criticité est calculé comme le produit de la probabilité et de l'impact.

c) Tableau de risques:

Risques	Probabilité (1-5)	Gravité (1-5)	Criticité (P × G)
Panne matérielle critique (serveur SIFAC)	2	5	10
Attaque DDoS sur SIFAC	3	4	12
Erreur de configuration entraînant indisponibilité	3	3	9
Piratage du système SIFAC	1	5	5
Hameçonnage réussi (accès utilisateur standard)	3	3	9
Hameçonnage réussi (accès administrateur)	1	5	5
Ingénierie sociale (accès administrateur)	1	5	5
Catastrophe naturelle endommageant les serveurs	1	5	5
Perte/corruption de données par erreur humaine	4	3	12

d) Hiérarchisation des risques:

En se basant sur le score de criticité, les risques sont hiérarchisés comme suit :

- **Risques intolérables (Criticité > 10):** Panne matérielle critique, Attaque DDoS, Perte/corruption de données par erreur humaine. Ces risques doivent être traités en priorité absolue en raison de leur impact significatif sur l'activité et la réputation de l'université.

- **Risques élevés (Criticité entre 5 et 10):** Erreur de configuration, Hameçonnage réussi (utilisateur standard), Piratage du système SIFAC, Ingénierie sociale (accès administrateur), Catastrophe naturelle. Ces risques nécessitent une attention particulière et des mesures de sécurité adéquates.
- **Risques faibles (criticité <5) :** Hameçonnage réussi (accès administrateur). Bien que le score soit faible, les conséquences d'un tel événement pourraient être importantes, la surveillance et la sécurité doivent quand même être assurées.

7. Module 5 : Traitement des risques

Ce module propose des mesures de sécurité concrètes pour traiter les risques identifiés et hiérarchisés dans le module précédent. La stratégie de traitement repose sur une combinaison de réduction, transfert et acceptation du risque.

a) Stratégie de traitement:

La stratégie de gestion des risques est basée sur la réduction du risque comme approche principale pour les risques majeurs, combinée à une acceptation du risque résiduel après la mise en place des mesures de sécurité. L'acceptation se justifie par le fait qu'il n'existe aucun moyen de supprimer totalement tout risque dans un système informatique. Le transfert de risque via une assurance est envisagé pour les risques liés aux catastrophes naturelles.

b) Mesures de sécurité proposées:

Ce tableau propose des mesures de sécurité pour chaque risque majeur. L'objectif est de proposer des solutions concrètes avec une justification de l'efficacité de la solution retenue. En plus du coût estimé, le niveau de sécurité apporté est indiqué (bas, moyen ou élevé) afin d'évaluer l'impact sur le risque avant et après mise en place de la solution (voir matrice des risques en annexe).

Panne matérielle critique (serveur SIFAC)	Infrastructure redondante (clustering, virtualisation), système de stockage SAN haute disponibilité,	Maximise la disponibilité du service en cas de panne d'un serveur. Le clustering assure un basculement automatique.	50 000	Élevé	Réduction significative

	surveillance système				
Attaque DDoS sur SIFAC	Protection DDoS via un CDN (Content Delivery Network)	Filtre le trafic malveillant avant qu'il n'atteigne les serveurs SIFAC. Absorption des requêtes malveillantes.	10 000	Moyen	Réduction importante
Erreur de configuration entraînant indisponibilité	Automatisation des tâches de configuration, tests rigoureux avant mise en production, politique de configuration standardisée	Réduit le risque d'erreur humaine dans la configuration des serveurs.	5 000	Moyen	Réduction modérée
Piratage du système SIFAC	Pare-feu avancé, IDS/IPS (Intrusion Detection/Prevention System), analyse régulière des vulnérabilités, mises à jour régulières des logiciels	Détection et prévention des intrusions, protection contre les exploits connus.	15 000	Élevé	Réduction significative

Hameçonnage réussi (accès utilisateur standard)	Authentification multifacteur (MFA), sensibilisation du personnel, formation à la sécurité informatique, analyse des courriels suspects	MFA renforce la sécurité des identifiants, la formation sensibilise les employés, la gestion des courriels augmente la sécurité.	10 000	Élevé	Réduction importante
Hameçonnage réussi (accès administrateur)	Authentification multifacteur (MFA) renforcée (clés matérielles), gestion des privilèges restreinte, surveillance accrue des connexions	MFA fournit une sécurité supplémentaire pour les comptes administrateurs. Le principle de moindre privilège limite l'impact.	5 000	Élevé	Réduction importante
Ingénierie sociale (accès administrateur)	Formation à la sécurité, politique de sensibilisation, procédures de vérification renforcées pour les demandes d'accès	Sensibilise le personnel aux tentatives de manipulation. Les procédures renforcées limitent les risques d'accès non autorisés.	2 000	Moyen	Réduction modérée

Catastrophe naturelle endommageant les serveurs	Sauvegarde cloud avec réplication géographique, contrat d'assurance couvrant les pertes matérielles et les interruptions de service	Protection contre les pertes physiques et la perte de données en cas de catastrophe naturelle.	15 000 + assurance	Élevé	Réduction importante
Perte/corruption de données par erreur humaine	Sauvegardes régulières avec réplication, formation des utilisateurs, contrôles d'intégrité des données	Réduit le risque de perte de données à cause d'erreurs humaines. La réplication offre une sécurité additionnelle.	20 000	Élevé	Réduction importante

c) Justification des choix:

Le choix des mesures se base sur une évaluation du coût et de l'efficacité pour chaque risque. Des solutions plus coûteuses sont privilégiées pour les risques les plus critiques afin de minimiser les impacts potentiels majeurs.

d) Plan d'action:

Un plan d'action détaillé en annexe précisera les tâches, les responsabilités, les échéances, le budget alloué et les indicateurs de suivi pour chaque action. Un responsable de projet sera désigné pour piloter la mise en œuvre du plan d'action. La mise en place impliquera une gestion

rigoureuse des changements afin de prévenir les incidents liés au déploiement des nouvelles mesures.

e) Gestion de projet et suivi:

La mise en œuvre des mesures de sécurité sera gérée via un plan de projet avec des livrables clairement définis et un calendrier précis. Des revues de projet régulières permettront de suivre l'avancement des travaux, d'ajuster le plan si nécessaire, et de garantir le respect des contraintes techniques et temporelles. Des indicateurs de performances (KPI) clairement définis seront utilisés pour suivre l’efficacité des mesures mises en place.

8. Conclusion et recommandations

Cette étude EBIOS a permis d'identifier, d'analyser et de hiérarchiser les risques pesant sur le système d'information financier de l'Université de la Réunion (UR), plus précisément sur le système SIFAC. Elle a également proposé des mesures de sécurité concrètes pour réduire ces risques et améliorer la sécurité globale du système.

a) Synthèse générale:

L'analyse a révélé une vulnérabilité significative du système SIFAC face à différentes menaces, notamment les pannes matérielles, les attaques par déni de service, les intrusions malveillantes et les erreurs humaines. Les conséquences d'événements indésirables peuvent avoir des impacts importants sur les plans financier, opérationnel, réglementaire et réputationnel pour l'université. Les risques liés à la perte de données sensibles et à l'indisponibilité du système pendant les périodes de forte activité (paie, clôture budgétaire) sont particulièrement préoccupants.

Les mesures de sécurité proposées visent à réduire ces risques en se concentrant à la fois sur l'amélioration de la résilience du système (redondance, sauvegarde), sur le renforcement de la sécurité des accès (authentification multifacteur, gestion des privilèges), sur la prévention des intrusions (pare-feu, IDS/IPS), et sur la sensibilisation des utilisateurs aux bonnes pratiques de sécurité. Le choix des solutions s'est fait en tenant compte de la criticité des risques, du coût des mesures envisagées et de l'impact sur la continuité de l'activité de l'université.

b) Points clés à retenir:

- Les risques liés à l'indisponibilité du système SIFAC sont majeurs, particulièrement en période de paie et de clôture budgétaire. Des solutions de sauvegarde et de haute disponibilité sont primordiales.
- La sécurité des accès est un élément critique pour protéger les données sensibles. L'authentification multifacteur doit être implémentée rapidement, ainsi que des contrôles efficaces.
- La sensibilisation des utilisateurs est essentielle. Des formations régulières sur les bonnes pratiques de sécurité sont nécessaires pour réduire l'impact des erreurs humaines.
- Le plan d'action doit définir des objectifs clairs, des responsabilités clairement précisées, et des indicateurs de mesure pour suivre l'efficacité des mesures de sécurité mises en place.

c) Recommandations prioritaires:

Les recommandations ci-dessous sont organisées par priorité et par échéance (court, moyen et long terme).

Court terme (0-6 mois):

- Mettre en œuvre immédiatement l'authentification multifacteur (MFA) pour tous les utilisateurs de SIFAC.
- Lancer un programme de sensibilisation et de formation des utilisateurs aux risques de sécurité et aux bonnes pratiques.
- Mettre en place un système de surveillance des activités suspectes (SIEM) pour détecter rapidement d'éventuelles intrusions.
- Améliorer le système de sauvegarde avec réplication géographique et chiffrement des données.

Moyen terme (6-12 mois):

- Implémenter l'infrastructure redondante et le système de haute disponibilité pour SIFAC.
- Déployer un système de protection contre les attaques DDoS.
- Réaliser un audit de sécurité complet du système SIFAC pour identifier et corriger les vulnérabilités.

- Formaliser et tester régulièrement le Plan de Continuité d'Activité (PCA).

Long terme (>12 mois):

- Réviser régulièrement la politique de sécurité et adapter les mesures aux évolutions des menaces.
- Intégrer la sécurité dans les processus de développement et de maintenance du système d'information.
- Mettre en place un processus de gestion des risques permanent pour surveiller et réévaluer régulièrement les risques.
- Envisager un renouvellement du système d'information en tenant compte des besoins de sécurité et des évolutions technologiques à moyen et long terme.

d) Conclusion:

La mise en œuvre de ces recommandations permettra d'améliorer significativement le niveau de sécurité du système d'information financier de l'UR, et de protéger les données sensibles de l'université. Le suivi régulier de l'efficacité des mesures mises en place est essentiel pour garantir la sécurité à long terme. Une veille technologique permanente et une adaptation constante sont cruciales face à l'évolution permanente des menaces informatiques.

9. Annexe:

La méthode EBIOS Risk Manager : La méthode EBIOS Risk Manager - Le guide | ANSSI

French Cybersecurity Agency (ANSSI) :
French Cybersecurity Agency (ANSSI)

EBIOS Risk Manager - 1. Pourquoi ? :
EBIOS Risk Manager - 1. Pourquoi ?

EBIOS RM dans la pratique :
EBIOS RM dans la pratique - Ep7 | Quel référentiel pour le socle de sécurité ?