RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

SÉCURISER UNE MIGRATION NUMÉRIQUE

Retrouvez une quinzaine de bonnes pratiques et ressources essentielles de l'ANSSI pour la mise en œuvre sécurisée de projets de migration de systèmes d'information (SI).

1/ VOLET STRATÉGIQUE

→ **Impliquer le plus en amont possible de la migration les équipes métier, DSI et sécurité** (RSSI, SOC, experts sécurité…) pour conduire le changement.

→ **Maintenir à jour la cartographie des SI et leurs inventaires avant, pendant et après la migration**, jusqu'au décommissionnement complet de l'ancienne solution. Identifier les différences d'architecture, de flux et de fonctionnalités métier et techniques**,** afin de définir les adaptations de sécurité nécessaires – voir à ce sujet le guide Cartographie du système d'information.

→ **Mettre à jour l'analyse de risque** et s'assurer que la nouvelle solution est conforme aux exigences de sécurité (disponibilité, intégrité, confidentialité, traçabilité) et aux réglementations *ad hoc*.

→ **Adapter les plans de continuité d'activité (PCA) et de reprise d'activité (PRA).**

→ **Étudier le niveau de sécurité proposé contractuellement par le prestataire ainsi que les conditions de réversibilité en cas d'externalisation.** Dans la mesure du possible, privilégier des services ou des prestataires qualifiés par l'ANSSI.

2/ VOLET TECHNIQUE

→ **Sécuriser les données sensibles en transit lors de la migration**, par exemple en les chiffrant. Porter une attention particulière aux exports massifs de données pour éviter de potentielles fuites.

→ **Anticiper les risques liés à l'altération ou à l'indisponibilité des sauvegardes en :**

> **identifiant les sauvegardes impactées par la migration et leur délai d'expiration** pendant la période de transition, pour maintenir sa capacité à restaurer les données ou l'ensemble du SI ;

> **conservant les infrastructures nécessaires pour accéder et restaurer les anciennes sauvegardes** jusqu'à leur expiration, en accord avec la politique de sauvegarde de l'entité.

→ **S'assurer que les moyens d'administration et de déploiement** (poste/console d'administration, hyperviseur, serveur de déploiement de configurations et de *templates*, etc.) **sont de confiance**, c'est-à-dire intègres et exempts de compromission. Dans un second temps, s'assurer que les socles de la cible (système, réseau et stockage) sont eux aussi de confiance.

→ **Profiter de la refonte du SI pour en améliorer la sécurité** en appliquant les bonnes pratiques d'hygiène informatique et les recommandations de l'ANSSI. En particulier, **implémenter les mesures de protection de l'architecture cible** (ex. : durcissement, filtrage des flux, MCO/MCS). Ne réaliser aucune modification impactante au cours de la phase critique de migration, mais strictement en amont ou en aval de l'opération.

V1.0 (01/26)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr

3/ VOLET OPÉRATIONNEL

→ **Identifier les impacts de la migration sur les activités du centre opérationnel de sécurité** (*Security Operations Center*, SOC) - couverture, supervision, etc. - et mettre à jour les procédures et les outils en conséquence. Communiquer préalablement le planning de migration pour éviter des alertes de sécurité type faux positif.

→ **Confirmer l'absence d'alertes de sécurité en amont** de la migration, ou les traiter le cas échéant.

→ **Contrôler le bon fonctionnement des équipements et logiciels de sécurité** (EDR, pare-feu, anti-virus, etc.) avant et après la migration.

→ **Mettre à jour l'ensemble des procédures opérationnelles et de sécurité,** notamment les procédures d'intervention en heures non ouvrées (HNO) sur site et/ou à distance. La migration ne doit être lancée qu'une fois l'ensemble de ces procédures définies et testées.

4/ POST-MIGRATION

→ **Conduire un audit post-migration pour identifier les problèmes de sécurité résiduels, et y opposer les contre-mesures adaptées.** Dans la mesure du possible, l'audit doit être régulièrement renouvelé tout au long du cycle de vie du nouveau système.

→ **Procéder au décommissionnement des anciens comptes, données et infrastructures en fonction de leur sensibilité**. Se référer aux textes de loi en vigueur (II n°901, arrêté du 20 août 2024 relatif aux normes techniques de destruction des informations et supports classifiés ou protégés) et aux Recommandations pour le reconditionnement des ordinateurs de bureau ou portables de l'ANSSI.