

CYBERSECURITY



Nancy Ewe

La Fiche FEROS

Expression Rationnelle des Objectifs de Sécurité

La **FEROS** (Fiche d'Expression Rationnelle des Objectifs de Sécurité) est un document technique officiel qui constitue le cœur du processus d'homologation de sécurité de l'ANSSI.

Elle formalise de manière rationnelle et structurée les objectifs de sécurité d'un système d'information, en s'appuyant sur une analyse de risque préalable.

Introduction et contexte réglementaire

L'ANSSI et ses missions

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), créée en 2009 et rattachée au Secrétariat général de la défense et de la sécurité nationale (SGDSN), a pour missions principales :

- Mission de prévention et de protection : Élaboration de doctrines et recommandations techniques
- Mission de détection et de réaction : Centre gouvernemental de veille (CERT-FR)
- Mission de qualification et certification : Certification de produits de sécurité, qualification de prestataires
- Mission de sensibilisation et formation : Programmes de sensibilisation sectoriels

Qui est concerné par l'homologation ?

Systèmes obligatoirement soumis à homologation :

- Systèmes d'Information d'Importance Vitale (SIIV) des OIV
- Systèmes traitant des informations classifiées
- Systèmes des administrations centrales (selon le RGS)
- Systèmes critiques du secteur privé (sur demande volontaire)

Bénéfices de l'homologation volontaire :

- Reconnaissance officielle du niveau de sécurité
- Avantage concurrentiel sur les marchés publics
- Amélioration de la confiance des partenaires
- Conformité anticipée aux évolutions réglementaires

Cadre juridique de l'homologation : Référentiel Général de Sécurité (RGS), Loi de Programmation Militaire (LPM), Directive NIS



Définitions et concepts fondamentaux

Homologation de sécurité

Procédure officielle par laquelle l'ANSSI reconnaît qu'un système d'information présente un niveau de sécurité adapté aux enjeux qu'il porte et aux risques auxquels il est exposé.

Caractéristiques : Durée de validité (3-5 ans), Périmètre défini, Niveau de confiance, Conditions d'exploitation

Système d'information (SI)

Ensemble organisé de ressources (matériels, logiciels, personnels, données, procédures) permettant de collecter, filtrer, traiter, sauvegarder et diffuser des informations.

Composants : Biens essentiels, Biens supports, Architecture logique, Architecture physique

Analyse de risque

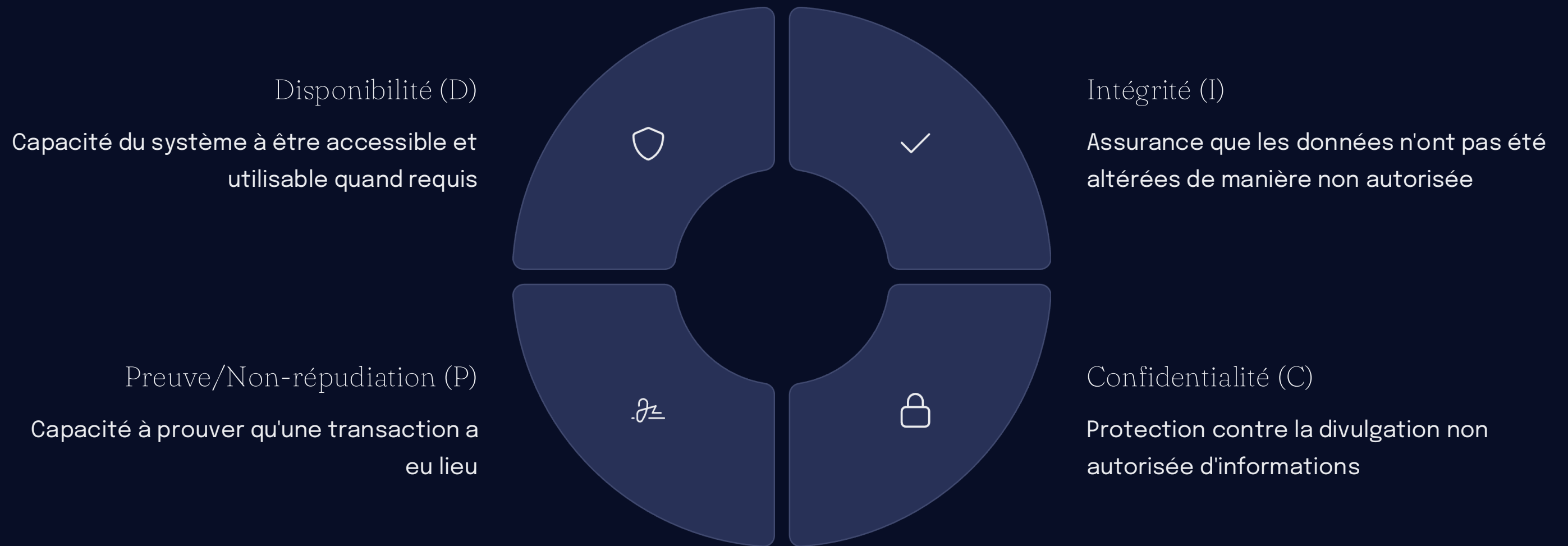
Processus systématique d'identification, d'analyse et d'évaluation des risques pour déterminer les mesures de sécurité appropriées.

Formule : $\text{Risque} = \text{Menace} \times \text{Vulnérabilité} \times \text{Impact}$

Méthodes : EBIOS, ISO 27005, MEHARI, OCTAVE

Objectifs de sécurité

Les objectifs de sécurité définissent les propriétés de sécurité que doit respecter le système. Ils s'articulent autour des critères DICP(N) :



Critères complémentaires : Authenticité (garantie de l'identité des utilisateurs et de l'origine des données), Traçabilité (capacité à suivre et enregistrer les actions réalisées), Imputabilité (possibilité d'associer une action à son auteur)

Le processus d'homologation ANSSI

Phase 1 : Initialisation

Objectifs : Définir le périmètre d'homologation, Identifier les enjeux et contraintes, Constituer l'équipe projet, Planifier les activités

Livrables : Note de cadrage, Dossier d'architecture, Analyse des enjeux

Phase 2 : Analyse de sécurité

Analyse de risque (méthode EBIOS) : Module 1 - Cadrage et biens essentiels, Module 2 - Événements redoutés, Module 3 - Scénarios stratégiques, Module 4 - Scénarios opérationnels, Module 5 - Mesures de sécurité

Élaboration de la FEROS : Objectifs de sécurité rationalisés, Architecture de sécurité cible, Fonctions de sécurité requises, Contraintes d'exploitation

Phase 3 : Évaluation

Types d'évaluation : Auto-évaluation, Évaluation par prestataire qualifié PASSI, Évaluation ANSSI

Méthodes : Tests de pénétration, Audit de code source, Revue d'architecture, Audit organisationnel

Phase 4 : Homologation

Dossier d'homologation : Fiche FEROS, Dossier de sécurité, Rapport d'évaluation, Plan de gestion des risques

Décision : Autorisation d'exploitation, Autorisation conditionnelle, Refus

Phase 5 : Maintien en condition

Surveillance continue : Monitoring de sécurité, Gestion des vulnérabilités, Audits périodiques, Évolution du système

Structure détaillée de la fiche FEROS

La fiche FEROS est structurée en plusieurs sections logiques qui permettent une description complète et rationnelle des objectifs de sécurité :

FEROS = Contexte + Enjeux + Objectifs + Architecture + Contraintes



Section 1 : Identification du système

- Informations générales (nom, version, propriétaire, exploitant)
- Classification (niveau de sensibilité, criticité métier)
- Contexte d'utilisation (utilisateurs, environnement, interconnexions)



Section 2 : Contexte sécuritaire

- Enjeux métier (mission, processus, valeur des informations)
- Environnement de menaces (sources de risque, niveau d'exposition)
- Contraintes particulières (réglementaires, opérationnelles)



Section 3 : Objectifs de sécurité

- Biens essentiels et critères (DICP)
- Fonctions de sécurité requises (authentification, contrôle d'accès)



Section 4 : Architecture de sécurité

- Vue d'ensemble architecturale (zonage, composants)
- Mesures organisationnelles (gouvernance, gestion opérationnelle)



Section 5 : Contraintes d'exploitation

- Contraintes techniques (performance, interopérabilité)
- Contraintes organisationnelles (ressources, processus)
- Contraintes de coûts (investissement, ROI sécurité)

Méthodologie d'élaboration

Préparation de la démarche

Constitution de l'équipe :

- Maître d'ouvrage : Porteur des enjeux métier
- RSSI : Responsable de la sécurité du SI
- Architecte sécurité : Conception des mesures techniques
- Chef de projet : Coordination et planning
- Experts métier : Connaissance des processus

Collecte d'informations :

- Dossier d'architecture du système
- Politique de sécurité de l'organisation
- Analyses de risque existantes
- Cartographie du SI
- Procédures d'exploitation

Déroulement de l'analyse EBIOS

L'analyse EBIOS se déroule en 5 modules :

1. Étude du contexte (cadrage, identification des biens, cartographie)
2. Expression des besoins de sécurité (évaluation des impacts)
3. Étude des menaces (sources de risque, motivations)
4. Étude des vulnérabilités (techniques, organisationnelles)
5. Études des risques (calcul, stratégies de traitement)

Rédaction de la FEROS : Structuration du document (règles rédactionnelles, format), Cohérence et validation (vérifications, processus de validation)

STEPS OF THE EBIOS CYBERSECURITY METHODOLOGY



Cas d'étude : Système de télémédecine



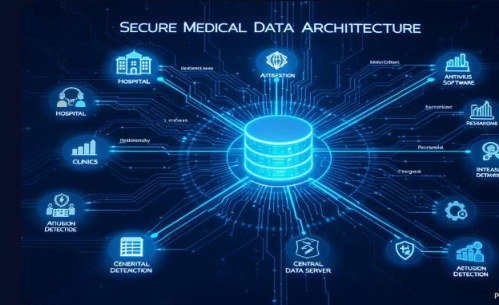
Contexte

Organisme : Établissement de santé public (CHU)

Système : Plateforme de consultation à distance

Enjeux : Continuité de soins, confidentialité des données de santé

Réglementation : Code de la santé publique, RGPD, HDS



Architecture de sécurité

Zonage sécuritaire : Zone Internet → DMZ (Reverse Proxy) → Zone Applicative → Zone Données

Mesures techniques : WAF avec règles OWASP Top 10, SIEM pour corrélation d'événements, Sauvegarde 3-2-1 avec test de restauration, PKI interne pour certificats serveurs

4

Niveau de confidentialité

Impact critique (secret médical, sanctions pénales)

3

Niveau de disponibilité

Impact grave si indisponible (urgences)

4

Niveau d'intégrité

Impact critique (erreurs thérapeutiques)

Processus de validation et de suivi

Validation initiale

Revue interne :

- Équipe projet FEROS
- RSSI et équipe sécurité
- Responsables métier concernés
- Direction informatique

Validation ANSSI :

1. Recevabilité : Vérification formelle du dossier
2. Instruction technique : Analyse par experts ANSSI
3. Évaluation complémentaire : Tests si nécessaire
4. Décision : Homologation, conditions, ou refus

Maintien en condition de sécurité

Surveillance continue :

Indicateurs de sécurité : Disponibilité, Intégrité, Confidentialité, Conformité



Gestion des évolutions :

- Mineures : Corrections, ajustements paramétriques
- Majeures : Nouvelles fonctionnalités, changements d'architecture
- Critiques : Modification des objectifs de sécurité

Renouvellement de l'homologation : Échéance (fin de validité 3-5 ans), Évolution majeure, Incident grave, Changement réglementaire



Conclusion

La fiche FEROS constitue un outil central de la démarche d'homologation ANSSI. Elle permet de formaliser de manière rigoureuse et traçable les objectifs de sécurité d'un système d'information, en s'appuyant sur une analyse de risque méthodique.



Approche rationnelle

La FEROS impose une justification de chaque objectif de sécurité par l'analyse de risque



Vision globale

Elle couvre tous les aspects (technique, organisationnel, humain)



Adaptabilité

Les mesures doivent être proportionnées aux enjeux réels



Pérennité

Le maintien en condition de sécurité assure la validité dans le temps

Bénéfices pour l'organisation : Sécurité maîtrisée (niveau de protection adapté aux besoins), Conformité réglementaire (respect des obligations légales), Confiance des parties prenantes (reconnaissance officielle), Optimisation des investissements (mesures ciblées et efficaces)

La réussite d'une démarche FEROS repose sur l'implication de toutes les parties prenantes, la qualité de l'analyse de risque préalable, et la capacité de l'organisation à maintenir dans le temps le niveau de sécurité défini.