



**ISERVICES SYSTEMS SAS**  
Plot 6170-1065, Parcel "J"  
Cadjèhoun Area Cotonou  
Tel : 0121387143  
[contactbenin@iservices.africa](mailto:contactbenin@iservices.africa)

## Mandat du CSIRT

| État       | Nom                   | Service     | Date       |
|------------|-----------------------|-------------|------------|
| Rédaction  | Ezeckiel DADJO        | DOPEX/CSIRT | 21/11/2025 |
| Update     | Jean-Robert HOUNTOMEY |             | 18/12/2025 |
| Validation | Edouard HOUNTOMEY     | CODIR       | 07/01/2026 |

### Historique de version

| Version | Date       | Objet            |
|---------|------------|------------------|
| 1.0     | 21/11/2025 | Version initiale |
| 1.1     | 18/12/2025 | updated          |

## IservicesCSIRT RFC2350

### RÉFÉRENCES ET STANDARDS

IservicesCSIRT s'appuie sur des références et standards reconnus pour assurer la conformité réglementaire, l'efficacité opérationnelle et la robustesse de ses pratiques. Ces références sont les suivantes :

- **le Security Incident Management Maturity Model (SIM3)** : un modèle de maturité utilisé pour évaluer et améliorer les capacités des équipes de réponse aux incidents de sécurité informatique (CSIRT). Il permet au CSIRT de l'Assurance Maladie d'évaluer et d'améliorer ses capacités à travers 4 domaines principaux : organisationnel, humain, outils et processus
- **Le Security Operations Center Capability Maturity Model (SOC-CMM)** est un cadre gratuit et open source permettant aux organisations d'évaluer et d'améliorer la performance de leur SOC à travers les domaines Business, Personnel, Processus, Technologie et Services. En utilisant des niveaux de maturité (0–5) et de capacité (0–3), il permet d'identifier les écarts, d'orienter les investissements et de démontrer les progrès réalisés. Le SOC-CMM s'aligne également sur des cadres tels que le NIST CSF afin de renforcer la résilience et d'assurer l'alignement du SOC sur les objectifs de l'entreprise.
- **Le FIRST CSIRT Services Framework** : un référentiel international qui définit clairement les services essentiels qu'une équipe CSIRT doit fournir pour atteindre un niveau opérationnel cohérent et reconnu. Il aide le CSIRT à structurer, prioriser et développer ses capacités autour de plusieurs familles de services, notamment : la gestion des incidents, la surveillance de sécurité, l'analyse de renseignements sur les menaces, la gestion des vulnérabilités, l'assistance en forensic, ainsi que la communication et la coordination avec les parties prenantes. Ce framework permet au CSIRT d'organiser son catalogue de services, de clarifier ses responsabilités et d'assurer une qualité homogène de prise en charge sur l'ensemble de ses missions.
- **Les AfricaCERT Guidelines** : un ensemble de recommandations opérationnelles élaborées pour harmoniser le fonctionnement des CSIRT africains et renforcer leur capacité à coopérer au niveau régional. Elles permettent aux équipes de définir un cadre commun pour le partage d'informations sur les menaces, l'usage du TLP, la gestion coordonnée des incidents transfrontaliers, la mise en place d'infrastructures de threat-intel (comme MISP), et l'adoption de bonnes pratiques en matière de

communication, de coordination et de confidentialité. Ces lignes directrices aident les CSIRT à structurer leurs activités autour de piliers essentiels tels que la collaboration régionale, la standardisation des procédures, l'amélioration continue et le renforcement des capacités techniques au sein de l'écosystème africain.

---

## INFORMATION

Ce document contient une description de IservicesCSIRT selon le [document RFC 2350](#). Il fournit les informations essentielles concernant IservicesCSIRT, ses canaux de communication, son rôle et ses responsabilités.

### Version du document

Version 1.0, mise à jour le 21 novembre 2025.  
Version 1.1, mise à jour le 18 Décembre 2025

### Liste de distribution

Il n'existe aucune liste de distribution.

### Lieu de publication du document

La version actuelle de cet article sous forme de document est disponible sur demande auprès du IservicesCSIRT.

Elle est également téléchargeable sous fichier PDF dans la section « Documents utiles », en bas de page de cet article.

### Authenticité du document

L'authenticité de ce document peut être confirmée sur demande auprès de IservicesCSIRT.



**ISERVICES SYSTEMS SAS**  
Plot 6170-1065, Parcel "J"  
Cadjèhoun Area Cotonou  
Tel : 0121387143  
[contactbenin@iservices.africa](mailto:contactbenin@iservices.africa)

## Identification du document

Titre : Mandat du IservicesCSIRT- RFC2350

Expiration : ce document est valide jusqu'à la publication d'une nouvelle version.

---

## CONTACT

### Nom

IservicesCSIRT

Iservices Computer Security Incident Response Team

### Adresse

- Plot 6170-1065, Parcel "J" Cadjèhoun Area Cotonou

Autres Pays.

- Boulevard de la Victoire, TOKOIN PROTESTANTS Lomé - TOGO

### Fuseau horaire

UTC/CET

### Numéro de téléphone

+ 2290121387143

+2290166201883

Les heures ouvrées sont les suivantes : du lundi au vendredi, de 8 h à 18 h (UTC).



## Numéro de fax

Non disponible.

## Autre canal de communication

Non disponible.

## Adresse de courrier électronique

[csirt@iservices.africa](mailto:csirt@iservices.africa)

## Clé publique et informations de chiffrement

Le moyen de communication privilégié est la messagerie électronique. Les informations sensibles sont chiffrées avant d'être transmises. En fonction des acteurs, IservicesCSIRT utilise PGP pour garantir la confidentialité et l'intégrité des documents échangés. PGP pourra être utilisé pour authentifier les fichiers échangés.

IservicesCSIRT utilise une clé publique PGP avec les caractéristiques suivantes :

- ID: C30F561942F253CB
- empreinte : 209D 71C9 E64C D159 43DD D1C0 C30F 5619 42F2 53CB

La clé publique peut être récupérée à tout moment à partir des serveurs de clés publiques applicables tels que <https://keys.openpgp.org>. La clé doit être utilisée chaque fois que des informations doivent être envoyées au IservicesCSIRT de manière sécurisée.

## Composition de l'équipe

Pour des raisons de confidentialité, la liste des membres de l'équipe n'est pas publiquement diffusée. Plus d'informations sont disponibles sur demande auprès du IservicesCSIRT.

## Point de contact clients

Il est préférable de contacter IservicesCSIRT par mail.

Dans les cas d'urgence, il est possible de contacter le IservicesCSIRT par téléphone.



Les heures ouvrées sont les suivantes : du lundi au vendredi, de 9 h à 18 h (UTC).

---

## CHARTRE

### Mission

La mission de IservicesCSIRT est de protéger, détecter, analyser et répondre efficacement aux incidents de sécurité affectant les systèmes d'information, les services numériques et les actifs critiques de nos clients et partenaires. Notre objectif est de garantir un niveau élevé de résilience face aux menaces cyber, tout en apportant un soutien opérationnel, stratégique et préventif adapté aux besoins du contexte africain et international.

IservicesCSIRT poursuit notamment les finalités suivantes :

1. **Assurer une réponse rapide, coordonnée et efficace aux incidents de sécurité**, en appliquant des procédures conformes aux bonnes pratiques internationales (ISO 27035, NIST 800-61, FIRST CSIRT Services Framework).
2. **Fournir une surveillance continue et une capacité d'anticipation**, en détectant les activités malveillantes, les vulnérabilités et les comportements anormaux susceptibles d'impacter les organisations que nous accompagnons.
3. **Produire et diffuser du renseignement sur les menaces (CTI)**, adapté au contexte local et régional, afin d'aider les entités partenaires à améliorer leur posture de sécurité et à prévenir les attaques émergentes.
4. **Accompagner les organisations dans la gestion de crise cyber**, en assurant coordination, communication technique et support décisionnel lors d'incidents majeurs ou d'attaques complexes.
5. **Renforcer les capacités de cybersécurité au sein de l'écosystème africain**, en favorisant la collaboration, le partage d'informations (TLP), les exercices cyber, et en s'alignant sur les recommandations AfricaCERT et AF-ISAC.

6. **Contribuer à l'amélioration continue de la sécurité**, via des activités de gestion des vulnérabilités, d'audit technique, de sensibilisation, de formation et de revue post-incident.

## Circonscription

Le périmètre d'intervention d'IserVICESCSIRT couvre les systèmes d'information d'IserVICES Systems SAS et de ses entités associées, ainsi que ceux des organisations clientes ayant souscrit un service de réponse aux incidents ou de supervision de la sécurité (CSIRT/SOC) auprès d'IserVICES Systems SAS.

Pour obtenir une liste complète et des informations détaillées sur les entités couvertes, se référer aux contrats de services en vigueur et à la documentation officielle remise aux clients dans le cadre des offres CSIRT/SOC.

---

## STRATEGIE

### 1. Types d'incidents et niveau de support

Le IserVICESCSIRT s'occupe de tous types d'incidents de cybersécurité impactant sa circonscription.

### 2. Coopération, échange et confidentialité de l'information

IserVICESCSIRT soutient la coordination opérationnelle et l'échange d'information entre CERT, CSIRT, SOC et autres entités similaires. IserVICESCSIRT estime que de telles actions sont positives pour IserVICESCSIRT et les parties tierces, et peuvent aider à réaliser de manière plus efficace leur devoir ainsi que la résolution d'incidents de sécurité.

De plus, IserVICESCSIRT attache une importance cruciale à la confidentialité de la donnée et au principe du besoin d'en connaître. IserVICESCSIRT applique le protocole Traffic Light Protocol version 2.0. Dès lors, les informations seront classifiées CLEAR, GREEN, AMBER, AMBER+STRICT, et RED.

IserVICESCSIRT applique également le Permissible Actions Protocol (PAP), qui définit les actions autorisées lors des échanges d'informations sensibles avec des partenaires. Le PAP permet de formaliser les règles d'utilisation, de partage et de manipulation des données, garantissant ainsi leur confidentialité, leur intégrité et une approche sécurisée des collaborations.

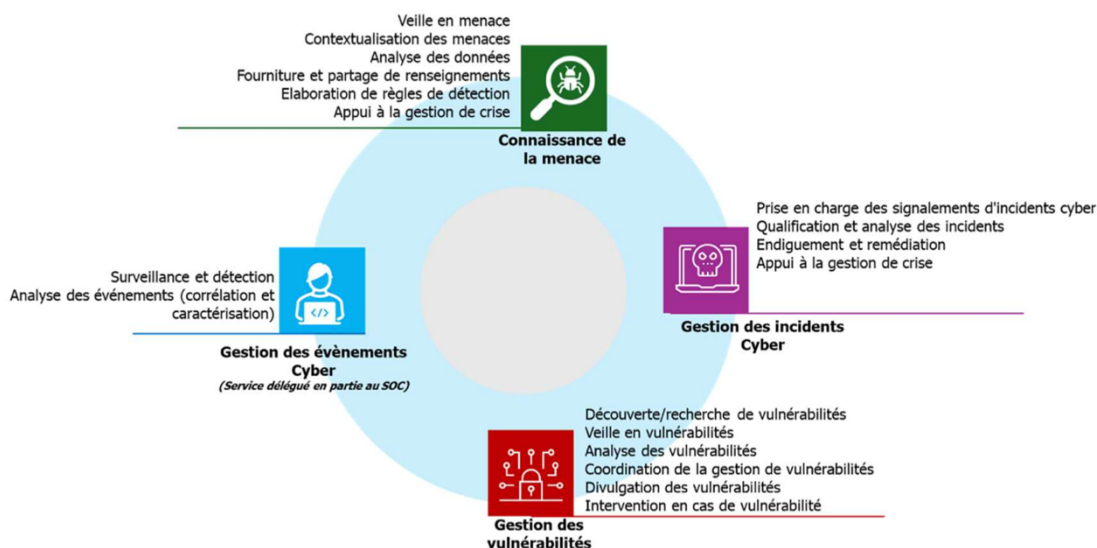
IservicesCSIRT opère selon le cadre légal Béninois.

### 3. Communication

IservicesCSIRT protège les informations sensibles selon les politiques et réglementations du Bénin, des pays de résidence de ses clients et de l'Union africaine. Les communications sécurisées, incluant le chiffrement et l'authentification, sont réalisées en utilisant une clé PGP ou les outils Bluefiles et ZED, selon la sensibilité et le contexte.

### 4. Services

IservicesCSIRT propose à ses membres les services suivants :



#### 1. Gestion des incidents Cyber

- Évaluation de la sévérité de l'incident.
- Catégorisation de l'incident.
- Résolution des incidents.
- ❖ Réalise les investigations et forensic en vue de déterminer la raison racine de l'incident ;
- ❖ Partage les informations avec les autorités légales et institutionnelles quand nécessaire ;
- ❖ Propose des plans d'endiguement, éradication, et récupération ;
- ❖ Collecte des preuves à des fins légales et institutionnelles

- Fourniture des éléments techniques nécessaires à la cellule de crise.

## 2. Connaissance de la menace

Le service CTI du IservicesCSIRT est responsable de la supervision de la menace et des vulnérabilités susceptibles d'impacter sa circonscription.

- Fournit une connaissance du paysage de la menace permettant d'orienter les actions du CSIRT.
- Veille et collecte les informations pertinentes pour la circonscription du CSIRT.
- Capitalise et contextualise les informations brutes récoltées.
- Analyser les données collectées pour aider à la prise de décision.
- Partager les renseignements avec les différentes parties prenantes, au niveau stratégique, tactique et opérationnel, selon le TLP.
- Fournit les renseignements nécessaires relatifs aux exploitations de vulnérabilités par des acteurs menaçants.
- Fournit les renseignements nécessaires à la cellule de crise.
- Partage les relations avec les autres CSIRT, CERT, et autres communautés selon le principe du besoin d'en connaître.
- Élabore les règles de détection et signatures.

## 3. Gestion des événements cyber (service délégué en partie au SOC)

IservicesCSIRT est responsable de la détection de circonstance, en vue de :

- Anticiper et gérer l'incident en fonction des menaces identifiées pouvant cibler ses clients.

## 4. Gestion des vulnérabilités

- Évalue l'exposition des actifs ciblés.
- Évalue la criticité des vulnérabilités ainsi que ses composantes techniques.
- Fournit les recommandations relatives aux vulnérabilités.

## 5. Engagements de niveaux de services

A ce jour, le IservicesCSIRT n'a pas d'engagement de niveaux de services.

## 6. Formulaire de déclaration d'un incident

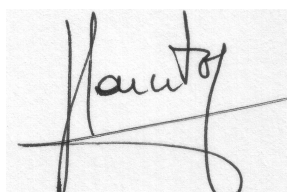
IservicesCSIRT encourage à déclarer les incidents en utilisant des courriels chiffrés avec les informations suivantes :

- Contact et information de l'organisation ;

- Un résumé de l'incident/urgence/crise ;
- La date et le type d'évènement ;
- La source de l'information ;
- Les systèmes affectés ;
- L'évaluation de l'impact ;
- Les détails des observations qui ont menées à la découverte de l'incident ;
- Les données techniques pertinentes ;
- Le TLP/PAP.

## 7. Clause de non-responsabilités

Non Applicable.

A handwritten signature in black ink, appearing to read "Hountomey".

*Edouard Hountomey*