CULLETTIVITÀ DI CORSICA
COLLECTIVITÉ DE CORSE

Soutenu par
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité


# RFC 2350

VERSION 1 – JANVIER 2024

Financé par l'Union européenne
NextGenerationEU

FRANCE RELANCE

Bénéficiaire du plan de relance

RÉPUBLIQUE FRANÇAISE

TABLE DES MATIERES

# 1. À PROPOS DU DOCUMENT

Ce document contient une description du centre de réponse d'urgence face aux incidents cyber, le CSIRT CyberCorsica tel que recommandé par la RFC 2350 : http://www.ietf.org/rfc/rfc2350.txt

Il présente des informations sur l'équipe, les services proposés et les moyens de contacter le CSIRT CyberCorsica.

## 1.1 DATE DE DERNIERE MISE A JOUR

Ceci est la version V1.0 de ce document, éditée le 02/01/2024

## 1.2 LISTE DE DISTRIBUTION POUR LES MODIFICATIONS

Toutes les modifications apportées à ce document seront partagées via les canaux suivants :

- InterCERT-FR / réseau de Français CSIRT -www.cert.ssi.gouv.fr/csirt/intercert-fr

## 1.3 OU TROUVER CE DOCUMENT

Ce document peut être trouvé en pied de page du site du CSIRT CyberCorsica : www.cyber.corsica

## 1.4 AUTHENTICITE DU DOCUMENT

Ce document a été signé à l'aide de la clé PGP du CSIRT CyberCorsica.

La clé PGP publique, son identifiant et son empreinte sont disponibles sur le site internet du CSIRT CyberCorsica à l'adresse suivante : https://cyber.corsica/index.php/pgp/

## 1.5 IDENTIFICATION DU DOCUMENT

Titre : RFC 2350 du CSIRT CyberCorsica

Version : version V1.0

Date de mise à jour : 02/01/2024

Durée de validité : ce document est valide tant qu'il n'existe pas de version ultérieure.

# 2. INFORMATIONS DE CONTACT

## 2.1 NOM DE L'EQUIPE

Nom court : Cybercorsica

Nom complet : CSIRT CyberCorsica

## 2.2 ADRESSE

10 rue Général Fiorella

20000 AJACCIO

## 2.3 ZONE HORAIRE

CET/CEST : Paris (GMT+01:00, et GMT+02:00 heure d'été)

## 2.4 NUMERO DE TELEPHONE

04 20 97 00 97

## 2.5 Numero de Fax

Néant

## 2.6 Autres moyens de communication

- https://www.linkedin.com/company/csirt-cybercorsica/

## 2.7 Adresse E-Mail

contact@cyber.corsica

## 2.8 Cle publique et informations liees au chiffrement

PGP est utilisé pour garantir la confidentialité et l'intégrité des échanges avec le CSIRT CyberCorsica.

Clé publique :

*mDMEZd3mjBYJKwYBBAHaRw8BAQdAHB1q8lYUfkCwVW5pULnBssvBk5KaVPOAJYrc*
*JlayrcO0KkNTSVJUIEN5YmVyQ29yc2ljYSA8Y29udGFjdEBjeWJlci5jb3JzaWNh*
*PoiTBBMWCgA7FiEEKJ63P8qKn0TwjD7O4TicEv7LRg8FAmXd5owCGyMFCwkIBwIC*
*IgIGFQoJCAsCBBYCAwECHgcCF4AACgkQ4TicEv7LRg9DHAD/cPj9DHiQQ78jB2Mi*
*nwbMNsS18XL1ouetqCS0oSO06b8A/2BtGwSYkmrKHX/5Zo/7Q2UIev+yljk44GFR*
*a/PuaI8EuDgEZd3mjBIKKwYBBAGXVQEFAQEHQDaxzoXfOQ2JopupXah3viZaJzsE*
*1uHSIXWHpfKHnMsnAwEIB4h4BBgWCgAgFiEEKJ63P8qKn0TwjD7O4TicEv7LRg8F*
*AmXd5owCGwwACgkQ4TicEv7LRg8TXwD8D7dZB4w8EkgvXAmgVJ7hmlSNO1yl97Py*
*LGXTJGXnYiABAJyDlSS/7p9OWbq/VG2eUoLZXGeLYhH7VbRP5Wat/kAD*
*=hSb0*
*-----END PGP PUBLIC KEY BLOCK-----*

Identifiant de la clé : E138 9C12 FECB 460F

Empreinte : 289EB73FCA8A9F44F08C3ECEE1389C12FECB460F

La clé PGP publique est disponible à cette adresse : https://cyber.corsica/index.php/pgp/ ainsi que sur les principaux serveurs de clés PGP (MIT, CIRCL)

## 2.9 Membres de l'equipe

L'équipe est constituée de 3 membres :

- Un responsable du CSIRT ;
- Deux Analystes en cyber sécurité ;

## 2.10 Autres informations

Aucune à ce jour.

## 2.11 Contact

Le CSIRT CyberCorsica est disponible durant les heures ouvrées, soit de 8h30 à 12h30 et de 14h00 à 17h30 du lundi au vendredi (hors jours fériés).

Pour joindre le CSIRT CyberCorsica, le moyen de communication privilégié est par courriel à l'adresse contact@cyber.corsica

Nous encourageons l'utilisation de chiffrement avec les informations présentées dans le paragraphe 2.8 *Clé publique et informations liées au chiffrement* pour assurer l'intégrité et la confidentialité des échanges.

En cas d'urgence, veuillez spécifier la balise [URGENT] dans le champ objet de votre courriel.

Le CSIRT CyberCorsica est aussi joignable par téléphone au 04 20 97 00 97.

# 3. CHARTE

## 3.1 ORDRE DE MISSION

Le CSIRT CyberCorsica est l'équipe de réponse aux incidents de sécurité informatique pour la Corse. Son objectif est d'apporter une assistance aux organisations de son territoire (décrites dans le paragraphe 3.2 *Bénéficiaires*) pour répondre aux incidents cyber auxquels elles font face.

Les missions du CSIRT CyberCorsica sont les suivantes :

- Accompagner les bénéficiaires (décrits dans le paragraphe 3.2 *Bénéficiaires*) victimes d'un incident informatique et les orienter vers des prestataires en sécurité informatique, référencés,
- Assurer une veille sur les menaces et les vulnérabilités,
- Alerter les bénéficiaires (décrits dans le paragraphe 3.2 *Bénéficiaires*) de ces menaces et vulnérabilités,
- Contribuer à la sensibilisation des acteurs du territoire de la collectivité de Corse en relayant les informations disponibles auprès des organismes d'état et d'entreprises spécialisées en cybersécurité.

## 3.2 BENEFICIAIRES

Les entités pouvant bénéficier de l'accompagnement du CSIRT CyberCorsica sont les organisations localisées sur le territoire de la collectivité de Corse, comprenant notamment :

- Les PME,
- Les ETI,
- Les collectivités territoriales et les établissements publics associés,
- Les associations.

## 3.3 AFFILIATION

Ce CSIRT est affilié à la Cullettività di Corsica - Collectivité de Corse.

## 3.4 AUTORITE

Le CSIRT CyberCorsica réalise ses activités sous la responsabilité de son Directeur, lui-même sous l'autorité du Président du Conseil Exécutif de Corse.

# 4. POLITIQUES

## 4.1 TYPES D'INCIDENTS ET NIVEAU D'INTERVENTION

Le périmètre d'action du CSIRT CyberCorsica couvre tous les incidents de sécurité informatique touchant les organisations de son territoire décrites dans le paragraphe 3.2 *Bénéficiaires*.

Les missions principales du CSIRT CyberCorsica sont :

- Offrir une réponse de premier niveau pour les incidents cyber survenant chez ses bénéficiaires ;
- Rediriger ses bénéficiaires vers des prestataires référencés pour la remédiation de l'incident ;
- Agir comme un relai entre le CERT-FR, les prestataires régionaux, les services de Police et de Gendarmerie et les bénéficiaires ;

- Consolider les statistiques d'incidentologie à l'échelle du territoire de la collectivité de Corse.

### 4.2 COOPERATION, INTERACTION ET PARTAGE D'INFORMATION

Les informations relatives à un incident telles que le nom de la structure et les détails techniques ne sont pas publiées sans l'accord de la partie nommée.

Le CSIRT CyberCorsica peut être amené à communiquer des informations aux autres CSIRT régionaux ou au CERT-FR lorsqu'une structure sollicite leur appui. De la même manière, des informations pourront être partagées avec un CSIRT sectoriel (santé, maritime…) à des fins de capitalisation des incidents propres au secteur concerné.

La diffusion d'information sera traitée en accord avec le protocole TLP défini par FIRST (https://www.first.org/tlp).

### 4.3 COMMUNICATION ET AUTHENTIFICATION

Le CSIRT CyberCorsica conseille fortement l'utilisation de canaux de communication sécurisés et du chiffrement PGP, en particulier pour communiquer des informations confidentielles ou sensibles.

Les informations non confidentielles ou non sensibles (peuvent être transmises via des courriels non chiffrés).

## 5. SERVICES

### 5.1 REPONSE AUX INCIDENTS

L'activité principale du CSIRT CyberCorsica est de venir en aide à ses bénéficiaires en proposant un service de réponse de premier niveau aux incidents cyber et de les aider à affiner leur choix de prestataire pour les accompagner dans la suite de la résolution des incidents.

En particulier, il propose les services détaillés dans les paragraphes suivants.

### 5.2 RECEPTION ET QUALIFICATION

- Récupération du signalement et prise de contact avec le déclarant ;
- Collecte d'informations sur l'incident et confirmation ou évaluation de la nature de l'incident ;
- Détermination de la sévérité de l'incident (son impact) et de son périmètre (nombre de machines affectés) ;
- Enregistrement et catégorisation de l'incident.

### 5.3 COORDINATION ET COMMUNICATION

- Identification du meilleur partenaire au sein du dispositif national[1] de réponse aux incidents pour accompagner le demandeur ;
- Accompagnement dans la diffusion, le cas échéant, de signalements vers les autorités compétentes de l'Etat selon la nature de l'incident. Notamment, mais de manière non exhaustive :
    - A l'ANSSI en cas d'incident majeur de cybersécurité pouvant impacter d'autres secteurs ;
    - A la Commission Nationale de l'Informatique et des Libertés (CNIL) en cas de violation de données à caractère personnel.

[1] Redirection éventuelle vers ACYMA, le CERT-FR ou autre CSIRT (e.g. sectoriel)

### 5.4 ACCOMPAGNEMENT A LA RESOLUTION

- Proposition d'actions réflexes, notamment des mesures d'urgence pour limiter l'impact de l'incident ou des mesures destinées à faciliter les investigations et le traitement de l'incident ;
- Partage d'une liste restreinte de prestataires de proximité capables d'assurer la résolution et la remédiation de l'incident ;
- Suivi des phases de résolution et de remédiation.

### 5.5 ACTIVITES PROACTIVES DE VEILLE ET D'INFORMATION

Le CSIRT CyberCorsica pourra aussi proposer des services proactifs à ses bénéficiaires, notamment :

- Des services de veille ;
- Des analyses de menaces ;
- Un bulletin de veille à destination d'abonnés.

## 6. FORMULAIRES DE NOTIFICATION D'INCIDENT

Un formulaire de déclaration d'incident est disponible en ligne à l'adresse : www.cyber.corsica

En cas de déclaration par courriel, pour faciliter la prise en compte des signalements il est demandé dans la mesure du possible de fournir dans le courriel, les éléments suivants :

- Informations sur l'organisation touchée (nom, contact de la direction et des équipes techniques, taille…) ;
- Informations de contact du demandeur comprenant notamment : nom, fonction et numéro de téléphone portable ;
- Informations de contact du responsable du Système d'Information comprenant notamment : nom, numéro de téléphone portable ;
- Chronologie de l'incident : date et heure du début de l'incident et de sa détection ;
- Description de l'incident comprenant notamment l'impact sur l'organisation et le nombre et type de machines touchées ;
- Actions effectuées depuis la détection de l'incident ;
- Toute autre résultat d'investigations déjà menées ;
- Architecture du système d'informations ;
- Outils et politiques de défense contre les incidents en place ;
- Si le demandeur est déjà en contact avec un prestataire de réponse aux incidents de sécurité informatique ;
- Services attendus de la part d'une équipe de réponse aux incidents.

## 7. DECHARGE DE RESPONSABILITE

Bien que toutes les précautions soient prises dans la préparation des informations, notifications et alertes, le CSIRT CyberCorsica n'assume aucune responsabilité pour les erreurs ou omissions, ou pour les dommages résultant de l'utilisation des informations contenues.

# RFC2350 : VERSION 1 – JANVIER 2024

INFOS :

| | |
|---|---|
| | www.cyber.corsica |
| | 04 20 97 00 97 |
| @ | contact @ cyber . corsica |
| | https://www.linkedin.com/company/csirt-cybercorsica/ |