CULLETTIVITÀ DI CORSICA
COLLECTIVITÉ DE CORSE

Soutenu par
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CSIRT CYBER CORSICA

RFC2350 : VERSION 1.3 – 22 OCTOBRE 2026

CULLETTIVITÀ DI CORSICA
COLLECTIVITÉ DE CORSE

TABLE DES MATIERES

1. À PROPOS DU DOCUMENT 3

1.1 LISTE DE DISTRIBUTION POUR LES MODIFICATIONS 3
1.2 OU TROUVER CE DOCUMENT 3
1.3 AUTHENTICITE DU DOCUMENT 3
1.4 IDENTIFICATION DU DOCUMENT 3

2. INFORMATIONS DE CONTACT 3

2.1 NOM DE L'EQUIPE 3
2.2 ADRESSE 3
2.3 ZONE HORAIRE 3
2.4 NUMERO DE TELEPHONE 3
2.5 AUTRES MOYENS DE COMMUNICATION 3
2.6 ADRESSE E-MAIL 4
2.7 CLE PUBLIQUE ET INFORMATIONS LIEES AU CHIFFREMENT 4
2.8 MEMBRES DE L'EQUIPE 4
2.9 AUTRES INFORMATIONS 4
2.10 CONTACT 4

3. CHARTE 5

3.1 ORDRE DE MISSION 5
3.2 BENEFICIAIRES 5
3.3 AFFILIATION 5
3.4 AUTORITE 5

4. POLITIQUES 5

4.1 TYPES D'INCIDENTS ET NIVEAU D'INTERVENTION 5
4.2 COOPERATION, INTERACTION ET PARTAGE D'INFORMATION 5
4.3 COMMUNICATION ET AUTHENTIFICATION 6

5. SERVICES 6

5.1 ASSISTANCE AUX VICTIMES ET TRAITEMENT DES INCIDENTS 6
5.1.1 RECEPTION ET QUALIFICATION 6
5.1.2 COORDINATION ET COMMUNICATION 6
5.1.3 ACCOMPAGNEMENT A LA RESOLUTION 6
o ANALYSE DE SURFACE D'EXPOSITION ET DIAGNOSTICS MON PARCOURS CYBER 7
5.2 VEILLE CYBER ET ALERTES CIBLEES 7
5.3 SITUATION CYBER TERRITORIALE ET PANORAMA DE LA MENACE 7
5.4 SENSIBILISATION, ATELIERS ET FICHES REFLEXES 7
5.5 ANIMATION DU RESEAU CYBER ET COOPERATION AVEC LES PARTENAIRES 7
5.6 ANALYSE D'URL ET D'E-MAILS SUSPECTS 8
5.7 INFORMATION, PUBLICATIONS ET COMMUNICATION 8

6. FORMULAIRES DE NOTIFICATION D'INCIDENT 8

7. DECHARGE DE RESPONSABILITE 9

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 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

1.2 OU TROUVER CE DOCUMENT

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

1.3 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/

1.4 IDENTIFICATION DU DOCUMENT

Titre : RFC 2350 du CSIRT CyberCorsica

Version : version V1.3

Date de mise à jour : 22/10/2026

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 AUTRES MOYENS DE COMMUNICATION

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

2.6 Adresse E-Mail

contact@cyber.corsica

2.7 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 :

—–BEGIN PGP PUBLIC KEY BLOCK—–
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)

2.8 Membres de l'equipe

L'équipe est constituée de 3 membres :

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

2.9 Autres informations

Aucune à ce jour.

2.10 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 2.7 *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 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 Entreprises,
- Les collectivités territoriales et les établissements publics associés,
- Les associations.

3.3 AFFILIATION

Ce CSIRT est une mission de la Cullettività di Corsica - Collectivité de Corse et effectue ainsi une mission de service public.

3.4 AUTORITE

Le CSIRT CyberCorsica réalise ses activités sous la responsabilité de son responsable, 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

Le CSIRT CyberCorsica propose à ses bénéficiaires (décrits dans le paragraphe 3.2 Bénéficiaires) huit services, structurés à partir du FIRST CSIRT Services Framework (v2.1) et détaillés dans le catalogue des services du CSIRT CyberCorsica. Ces services sont rendus dans le cadre d'une mission de service public, avec une autorité consultative et d'accompagnement : le CSIRT conseille, guide et oriente, sans pouvoir d'injonction ni de contrôle.

5.1 ASSISTANCE AUX VICTIMES ET TRAITEMENT DES 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 accompagner jusqu'à résolution ou le cas échéant de les orienter vers l'expertise adaptée pour la suite de la résolution. Il propose en particulier les services détaillés ci-dessous.

5.1.1 Réception et qualification

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

5.1.2 Coordination et communication

- Si la résolution n'est pas possible en interne, identification du meilleur partenaire de réponse aux incidents insulaire pour accompagner le demandeur ;
- Information du demandeur sur ses obligations, notamment le dépôt de plainte et, en cas de violation de données à caractère personnel, la déclaration à la CNIL ;
- Accompagnement dans la diffusion, le cas échéant, de signalements vers les autorités compétentes de l'État selon la nature de l'incident, notamment, mais de manière non exhaustive :
    - À l'ANSSI en cas d'incident majeur de cybersécurité pouvant impacter d'autres secteurs;
    - À la Commission Nationale de l'Informatique et des Libertés (CNIL) en cas de violation de données à caractère personnel.

5.1.3 Accompagnement à la résolution

- Proposition d'actions réflexes, notamment des mesures d'urgence pour limiter l'impact de l'incident ou 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 si besoin ;
- Suivi des phases de résolution et de remédiation ;
- Clôture et retour d'expérience lorsque cela est possible.

ANALYSE DE SURFACE D'EXPOSITION ET DIAGNOSTICS MON PARCOURS CYBER

- À la demande d'un bénéficiaire et avec son autorisation, le CSIRT CyberCorsica propose :
- Une analyse de la surface d'exposition de l'organisation accessible depuis Internet, sans intrusion dans ses systèmes d'information ;
- Un diagnostic d'hygiène numérique, s'appuyant sur les outils MesServicesCyber de l'ANSSI ;
- Une restitution des constats, des recommandations classées par priorité et, si des travaux plus approfondis sont nécessaires, une orientation vers des ressources ou prestataires adaptés.

5.2 VEILLE CYBER ET ALERTES CIBLEES

Le CSIRT CyberCorsica assure une veille sur les menaces, les vulnérabilités exploitées, les campagnes d'attaque et les fraudes susceptibles de concerner ses bénéficiaires. Les informations sont vérifiées, qualifiées et mises en contexte avant d'être relayées. Il propose :

- Des alertes de portée générale, publiées sur www.cyber.corsica ;
- Des alertes ciblées, adressées directement aux bénéficiaires concernés lorsqu'une menace vise un secteur ou un type de structure ;

Ce service est en cours de structuration. La veille ne garantit pas la détection de toutes les menaces.

5.3 SITUATION CYBER TERRITORIALE ET PANORAMA DE LA MENACE

- À partir des incidents dont il a connaissance et de sa veille, le CSIRT CyberCorsica élabore progressivement une vision agrégée et anonymisée de la menace cyber sur le territoire corse. Il peut produire :
- Un bilan annuel et des synthèses d'incidentologie ;
- Un panorama de la menace cyber propre au territoire ;
- Sa contribution au bilan annuel commun des CSIRT territoriaux.

Les publications préservent la confidentialité des informations traitées et ne permettent pas d'identifier, même indirectement, une victime (cf. paragraphe 4.2).

5.4 SENSIBILISATION, ATELIERS ET FICHES REFLEXES

Le CSIRT CyberCorsica mène des actions de sensibilisation sur l'ensemble du territoire, au plus près de ses bénéficiaires :

- Tables rondes et ateliers thématiques ;
- Interventions adaptées au type de structure et à son niveau de maturité, aux secteurs d'activité ou aux territoires ;
- Conseils pratiques et fiches réflexes, diffusés aux bénéficiaires.

Les thèmes peuvent inclure le phishing, les mots de passe, les sauvegardes, les mises à jour, la fraude au président ou la conduite à tenir en cas d'incident. Les formats, durées et disponibilités sont convenus au cas par cas.

5.5 ANIMATION DU RESEAU CYBER ET COOPERATION AVEC LES PARTENAIRES

Le CSIRT CyberCorsica anime et co-anime le réseau des acteurs de la cybersécurité en Corse.. Il assure :

- La mise en relation des organisations avec les interlocuteurs adaptés ;

- Le partage d'informations utiles, selon le protocole TLP et les règles applicables à chaque partenaire;
- La coopération avec les CSIRT/CERT sectoriels, avec son réseau, les partenaires locaux, nationaux, notamment dans le cadre de conventions.

La coordination ne transfère pas automatiquement la responsabilité d'un incident au CSIRT.

5.6 Analyse d'URL et d'e-mails suspects

Les bénéficiaires peuvent soumettre au CSIRT CyberCorsica une URL, un e-mail ou un fichier suspect. Le CSIRT :

- Examine l'élément, pour un e-mail, ses en-têtes, dans un environnement d'analyse adapté pouvant inclure un bac à sable, sans exécution sur le poste de l'utilisateur ;
- Restitue ses observations et ses recommandations de prudence (blocage, signalement, conservation de l'élément).

Il est demandé de ne pas transmettre de données sensibles sans canal sécurisé (formulaire en ligne ou chiffrement PGP, cf. paragraphe 2.8). Cette analyse de premier niveau ne vaut ni expertise forensique complète ni preuve judiciaire et nécessite une prise de contact en amont.

5.7 Information, publications et communication

Le CSIRT CyberCorsica diffuse une information cyber compréhensible et utile à ses bénéficiaires et partenaires :

- Publications sur son site www.cyber.corsica et sur sa page LinkedIn : informations de prévention, alertes, actualités et bonnes pratiques ;
- Relations avec la presse, dans le cadre défini avec la Direction de la Communication de la Collectivité de Corse.

Les informations publiées sont vérifiées et ne contiennent aucune information sensible.

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 1.3 – 22 OCTOBRE 2026

INFOS :

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