

RFC2350

Vie du document :

Historique des versions			
Version	Date	Auteur·e	Nature
V 1.0	25-04-2023	Philippe STEUER	Rédaction
V 1.1	04-03-2024	Philippe STEUER	Modification
V 1.2	16-02-2026	Nicolas VEDRENNE	Modification PGP

Table des matières

Vie du document :.....	1
1. Information.....	1
1.1. Version du document.....	1
1.2. Liste de distribution.....	1
1.3. Lieu de publication du document.....	1
1.4. Authenticité du document.....	1
1.5. Identité du document.....	1
2. Introduction et dénomination.....	2
2.1 Le Campus Régional de Cybersécurité et de Confiance numérique.....	2
2.2 Dénomination.....	2
3. Contacts.....	3
3.1. Nom de l'équipe.....	3
3.2. Adresse.....	3
3.3. Fuseau horaire.....	3
3.4. Numéro de téléphone.....	3
3.5. Numéro de FAX.....	3
3.6. Adresse de courrier électronique.....	3
3.7. Autre canal de communication.....	3
3.8 Clé publique et informations de chiffrement.....	3
3.9. Membres de l'équipe.....	4
3.10. Horaires de fonctionnement.....	4
3.11. Points de contact.....	4
4. Charte.....	4
4.1. Missions.....	4
4.2. Offre bénéficiaires++.....	5
4.3. Circonscription.....	5
4.4. Parrainage.....	5
4.5. Autorité.....	5
5. Politiques.....	6
5.1. Types d'incidents et niveau de support.....	6
5.2. Coopération, échanges et confidentialité de l'information.....	6
5.3. Communication.....	6
6. Services.....	7
6.1. Réponse à l'incident.....	7
6.2. Alertes et Cyberthreat Intelligence.....	7
7. Formulaire de déclaration d'incident.....	7
8. Avertissements.....	7
Annexe 1 : Clé publique.....	8

1. Information

Ce document contient une description du Campus Régional de Cybersécurité et de confiance numérique de Nouvelle-Aquitaine et plus particulièrement du centre de réponse aux incidents cyber (CRiC) conformément aux spécifications RFC 2350. Il fournit des informations de base, décrit ses responsabilités et services offerts.

1.1. Version du document

La version de ce document est la 1.2 publiée le 16/02/2026.

1.2. Liste de distribution

Les modifications apportées à ce document sont notifiées par courriel à :

InterCERT-FR / réseau des CSIRT Français - <http://www.cert.ssi.gouv.fr/csirt/intercert-fr>

Veuillez envoyer des questions sur les mises à jour à l'adresse e-mail du CSIRT du Campus cric-na@campuscyber-na.fr

1.3. Lieu de publication du document

Le lien vers la dernière version de ce document est disponible sur le site du campus dans le pied de page.

1.4. Authenticité du document

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

L'empreinte et son ID sont disponibles dans la section **2.8 et informations de chiffrement** . La clé publique PGP est disponible en **Annexe 1 : Clé publique**.

1.5. Identité du document

Titre : « RFC2350 C3-NA »

Version : 1.2

Date : 16/02/2026

SHA-256

Expiration : ce document est valide jusqu'à ce qu'il soit remplacé par une version ultérieure.

2. Introduction et dénomination

2.1 Le Campus Régional de Cybersécurité et de Confiance numérique

Le Campus Régional de Cybersécurité et de Confiance numérique Nouvelle-Aquitaine est en charge d'assurer un support auprès des entreprises de la région Nouvelle-Aquitaine dans le domaine de la lutte informatique défensive (cyberdéfense) en liaison avec les organismes d'État en charge de ces sujets. Les missions du C3-NA sont :

- Assurer une veille à partir de l'écosystème sécurité informatique régional et national sur les menaces et les vulnérabilités.
- Sensibiliser les entreprises de la région de manière permanente en relayant par mail les informations disponibles auprès des organismes d'état et d'entreprises spécialisées en cybersécurité.
- Alerter par mail ses adhérents à partir d'un maillage des organismes en charge de cybersécurité et des remontées d'informations des entreprises de la région Nouvelle-Aquitaine sur des menaces et vulnérabilités.

Le Centre de Réponse à incident est une entité hébergée par le campus régional de cybersécurité et de confiance numérique.

2.2 Dénomination

Dans la suite du document :

- Le diminutif **C3-NA** désigne le Campus Régional de Cybersécurité et de Confiance numérique Nouvelle-Aquitaine.
- Le diminutif **CRiC-NA** désigne le Centre de Réponse à incident Cyber de la région Nouvelle-Aquitaine.
- Le mot **bénéficiaire** désigne les collectivités (mairies, communautés de communes...) , les organismes publics, les PME, les ETI, ou les associations nationales à ancrage régional qui bénéficient des services de réponse à incident du CriC-NA.
- Le mot **bénéficiaire++** désigne les bénéficiaires qui ont souscrit (gratuitement) aux offres complètes du CriC-NA.

3. Contacts

3.1. Nom de l'équipe

Nom officiel : Centre de Réponse aux Incidents Cyber.

Diminutif : CRiC-NA.

3.2. Adresse

Campus Régional de Cybersécurité et de confiance numérique Nouvelle-Aquitaine

Service CRiC-NA

4 rue Adrienne Bolland

33600 PESSAC

3.3. Fuseau horaire

Heure normale d'Europe Centrale (HNEC) (Central European Time, UTC+1) et heure d'été d'Europe centrale (UTC+2).

3.4. Numéro de téléphone

(+33) 07 56 42 69 18

3.5. Numéro de FAX

Non disponible

3.6. Adresse de courrier électronique

L'adresse électronique du Campus est cric-na@campuscyber-na.fr

3.7. Autre canal de communication

Non disponible

3.8 Clé publique et informations de chiffrement

Le campus utilise une clé publique PGP :

- ID utilisateur : CRIC-NA <cric-na@campuscyber-na.fr>
- ID clé : 9F3C677B90CF7F7C
- Empreinte : 8DAC DD54 39FA F7CA 36F6 B3D6 9F3C 677B 90CF 7F7C

3.9. Membres de l'équipe

L'équipe est constituée d'analystes en cybersécurité.

Aucune information nominative relative aux membres du CRiC n'est diffusée dans ce document.

3.10. Horaires de fonctionnement

Les heures ouvrées concernant le CRiC sont du Lundi au Vendredi de 9h00 à 12h30 et de 13h30 à 17h00. En dehors de ces heures les bénéficiaires peuvent signaler leur incident sur le site du campus, répondre au questionnaire inclus dans le message vocal et/ou auprès de l'Agence Nationale de la sécurité des Systèmes d'Informations (ANSSI) dont les coordonnées figurent à l'adresse suivante : <http://www.cert.ssi.gouv.fr/contact>

Depuis le 21 Octobre 2025, le CriC est intégré dans le dispositif national 17Cyber, canal 24h/24h qui est privilégié pour le parcours des bénéficiaires.

3.11. Points de contact

Il est préférable de contacter le CRiC au travers de la plateforme 17cyber.gouv.fr.

Il est toujours possible d'envoyer un courrier électronique à l'adresse cric-na@campuscyber-na.fr et de contacter le CRiC par téléphone au 0 805 29 29 40 aux horaires indiqués précédemment.

4. Charte

4.1. Missions

Le CRiC est un service gratuit d'intérêt public qui permet :

- d'accompagner les victimes d'un incident cyber avéré ou redouté, de les accompagner dans le dépôt de plainte et/ou la notification à la CNIL et de les orienter vers des prestataires en sécurité informatique référencés de la région.
- de porter conseil aux entreprises, collectivités et associations de Nouvelle-Aquitaine dans les domaines de la cyber.

4.2. Offre bénéficiaires++

L'offre **bénéficiaires++** est une offre proposée gratuitement par le C3-NA et qui permet aux souscrivants de :

- Disposer d'un scan de surface léger.
- Accélérer la réponse à incident.
- Demander un diagnostic de maturité cyber et disposer de conseils personnalisés.
- Effectuer une évaluation de la sécurité du site internet...
- Bénéficier des outils développés par le campus en partenariat avec ses membres.

4.3. Circonscription

La circonscription est composée des collectivités, des associations nationales ainsi que de l'ensemble PME et ETI dont le siège social ou un établissement est basé dans un des départements de la région Nouvelle-Aquitaine. Il est conseillé d'adhérer préalablement aux services du CRiC pour bénéficier de l'entièreté des services offerts par le CRiC. Un formulaire de contact est disponible sur le site du campus pour en faire la demande. Les actions suivantes sont nécessaires à l'adhésion :

- La nomination d'un correspondant Cyber au sein de l'entreprise/association bénéficiaire.
- La réponse à un questionnaire d'identification des composants du Système d'Information de l'entreprise/association bénéficiaire.

Le CRiC pourra ainsi optimiser les services d'alerte et de réponse à l'incident pour l'ensemble des entreprises qui auront préalablement adhéré au Campus.

4.4. Parrainage

Le CRiC est un CSIRT public. Il maintient des relations avec les différents CERT et CSIRT en France et en Europe.

4.5. Autorité

Le C3-NA est placé sous l'autorité de l'association loi 1901.

5. Politiques

5.1. Types d'incidents et niveau de support

Le CRiC-NA est autorisé à coordonner et assurer un premier diagnostic de tout incident de sécurité informatique qui cible ou pourrait cibler un de ses bénéficiaires. En fonction de la nature de l'incident, le Campus propose une liste de prestataires en Cybersécurité, susceptibles d'aider l'entreprise dans la résolution de l'incident. Un suivi de la résolution de l'incident est assuré dans le but d'établir des statistiques et de capitalisation, et pour améliorer nos capacités de d'anticipation.

Le niveau de support offert par le Campus peut varier en fonction du type d'incident, de sa criticité et des ressources disponibles pour le prendre en charge.

5.2. Coopération, échanges et confidentialité de l'information

Le Campus échangera toutes les informations nécessaires avec les autres CERT/CSIRT susceptibles d'être concernés selon le besoin d'en connaître. Le partage d'informations se fera dans le respect des différentes réglementations de protection existantes et respectera le CSIRT Code of Practice <https://tf-csirt.org/documents/13/TI-CCoP.pdf>

Les renseignements généraux relatifs aux incidents, tels que les noms et les détails techniques ne sont pas publiés sans l'accord des parties désignées. S'il n'est pas convenu autrement, les renseignements fournis restent confidentiels. Le Campus ne transmet jamais d'informations à des tiers à moins que la loi ne l'exige.

Par conséquent, ces informations peuvent être transmises partiellement à des entités telles que :

- Les groupes concernés dans notre circonscription.
- Nos partenaires.
- Les groupes de coopération CERT/CSIRT.

Toutes les informations sont transmises en fonction de leur classifications et du principe du besoin de savoir, conformément au protocole TLP défini par FIRST (<https://www.first.org/tlp>). Seuls les extraits spécifiquement pertinents et anonymisés sont transmis. Le Campus traite l'information dans des environnements physiques et techniques sécurisés conformément aux réglementations existantes en manière de protection de l'information.

5.3. Communication

Notre méthode de communication principale est le courrier électronique. Lors de l'échange d'informations sensibles, le chiffage du mail via PGP est requis.

6. Services

6.1. Réponse à l'incident

Le Campus propose les services suivants dans le cadre de la réponse à l'incident de sécurité informatique :

- Réception des signalements d'incident.
- Diagnostic de l'incident.
- Accompagnement dans le dépôt de plainte et la notification à la CNIL
- Mise en relation vers des prestataires spécialisés.
- Compte rendu d'intervention concernant le traitement de l'incident.
- Capitalisation de la connaissance.
- Suivi et clôture de l'incident.

6.2. Alertes et Cyberthreat Intelligence

Afin d'adapter ses capacités de diagnostic et d'anticipation de la menace, le Campus réalise une veille active sur :

- La collecte de connaissances sur les acteurs de la cybermenace.
- Les menaces, les vulnérabilités, les scénarios d'attaques et les mesures de sécurité nécessaires.

Le C3-NA assure aussi une sensibilisation et une communication de ces informations, par courriel et publication sur son site Web, sous une forme appropriée à la compréhension des entreprises.

7. Formulaire de déclaration d'incident

Nous vous remercions de signaler l'incident via le site Web 17cyber.gouv.fr ou en nous contactant par téléphone aux horaires d'activité.

Les bénéficiaires des services du Campus pourront fournir un certain nombre d'informations selon leur niveau de compréhension de celles-ci. Ils seront par la suite recontactés par le Campus.

8. Avertissements

Bien que les informations transmises dans le document aient été vérifiées, le C3-NA refuse toute responsabilité en cas d'erreur ou d'omission ou pour tout préjudice résultant d'information contenues dans ce document.

Si vous constatez une erreur dans ce document merci de nous le signaler par mail. Nous tâcherons de rectifier les informations au plus vite.

Annexe 1 : Clé publique

-----BEGIN PGP PUBLIC KEY BLOCK-----

```
mQINBGmTFycBEACy9xXC00pnpOD/364SR5riCNJL8LF8yvSoFhP8QQvdxblD3wm9
8V84hasQwGay29vQi+9T3fcrN0wd0cky5cnV+pdukEsuQIoDQ3tkiMNsaggiVEh++
7KzYvLwPeA+TCjhEM+b4BsJ031S0eh2WB1IcBL0uGdhwo84IIUjqE2Ph5Dz8N8BH
egTRoFKg/qKkIoMyVUtprgWtBS0ukQSWYPufe0JyeDc61pigJOERZT6AQRKtMr20
zFUgSc/qVZIrMYpuo6nsVLZ7zdTUozxwBSHKt/Lr+QGilm6/xBkkChpZFmSwuM3G
0FS9veM8dPc+Wdb+w9uoNT0127ao86SJTWzBiBX2TMdXSXiZYmEB62e76l9Rgynu
87Rkdtf5vQxBzJHH04h9+p8R6LsPKw/9gqPny8UekAJC0ZXNDevjt5ZKUmHvKm0u
DNeM2w/u0HIH9uxYT/luUUhXXwudZCx0a44zRJbIh3PCJaH9zY7wsQ7STmjHxR6g
EqjrQpLhNrcowwtpg66hHlm3VMw7vIjC++97hDOCKETdD00aG2YuosaTvLNUz8R
W4bYfv9ULt1Rb2P/qjka354fPsb4ogJKVw+3EJKL02m0rsJx6qHPQBY0H6JPK45+
dn8aigr07TTKRUG4nIcTZvA4sAZ9gj9zJJGRpLj6C+hvn2xD4W5aCcd7pQARAQAB
tCNDUMlDIE5BIDxjcmllLW5hQGNhbXB1c2N5YmVYLW5hLmZyPokCVAQTAQoAPhYh
BI2s3VLQ5+vfKNvaz1p88Z3uQz398BQJpkxcnAhsDBQkBzU6JBQsJCACCBhUKCQgL
AgQWAgMBAh4BAheAAAJEJ88Z3uQz398WVUP/jaeSZ7vGLz0pEquR8fymPJG9pNS
BMZLLsJYYNPcpHryzw4NttzyczoY9Xg53yh40yTNRnNy052V7lqP2IatvTtwR8U
QIZLVNB31VEYCEmfqiMRlCJlSolZ2zFPMcoorc3yR5o0rMYL2EAVpuPI5rNiXfJf
ZJdojDFQOFrm3AM3ewd0n0VQqwu/hCF9nI5XcYXKV8eYIxukPPRRFaxNBGFhlQjb
6xQJYHm6uhiiUdx5oorqXg60BbBBHK79e5TsSHCMwBIiHJTj5y64dAGzi6Xcowu0
1tZ1HrOmV2XnZNPf7ajfhvLIhT6j6G0M9a0jyRdvKyo4R5kfmcD2rTyX7rLFH1Mc
vsjayV9e20KOMsLbKS7GG/rmvPHBBNNGOF3s/YgPRFbhY7W/Eftr7JX+kmrDYD0y
sdK40pINhbhouTkEg+2wlh40wiHtAvQzWxqig/fCf2RhRm3nYGj1JncJhuJoxhoy
p1W9Pnbqpli9pZB3fZJp5s35QlnA8B3pdvixFRhniIXmLK7MjdZhoYfC2M6CcLRP
fK0fNhjvWnqgCS00oeNGPo1IoJqo29CrXFuBWWwZib6Ml0Ah9yC6Bx2/0F7sC12
WleAhetCI9GTbXA6iPBhd23Uj3Yxn5ud+uS8V1N5sSgfAZXwb3P0gTaAr7sJMqQ+
Alk5C8jBQjYfSsi+uQINBGmTFycBEADds9FVvhQrhITapBb1MrvhaD63VCyxz1UI
QcXHe9BJSvrweJfstMrGTL4rsmAYsD8oS9FND68GZBebJmSzLhrH/t81c7xkV8pR
WZH+0Na6dwihK+1arUOCCCh5Lj9r4IeHyBMNBnWwnviZ0hvt3CZI1aBZiybA72ps
kaw28+zNxHTNVT4DwqPMkUX1yeJabNuPFW7d4SqbtvPjmjbomrA0it9JoNIcncX
9+mMpIOTMHZ0HBZjVBvcX/FRIyPiSlwzP2u2ervVAYAu4+iF6C3/82KW5h1LCDDLk
OXPTIGAY2c8SPNIepdT1F1pPc5g+4fdaDIoy1100lU3s85EBw3eE0Hq99hdpPB/s
ev8MBFGWE380Gv1vPQtijorS/yMsoucf1Qfm/fAVE5NqwfFbEuuEs13J99hRKbrG
KFsefiqMN5lIvzhQbYedQlFQ3NnTaxkMW35qmd9yX8VFNKew0J7VuF0D6cNZsLh
6nApFzeLbgvLnLUHopPUqs2E2t/pbXKbzmN0+HAFD/Cbhh+LQ3fxowHyBf5vjeD7
jzar2ywKJoVkm1pE9NNxACVEjoMbXb74z3IXrxJ9WVhB41utkHTPpf/AfDh0czMj
PhHeY8EZpEsm3AEv09IGwVeIH1rwoWyAfKrCXfZ/EBE4tDLenhpPHfTV/M7tQ53T
0tvxp00LywARAQABiQI8BBgBCgAmFiEEjazdVDn698o29rPWnzxne5DPf3wFAMmT
FycCGwwFCQHNTokACGkQnzxne5DPf3wCEBAALiUFBC09VoAUpsk63R/swWeuNNXA
0lCx0YPh+B7i213BvfIDTxL4o7KZJsKSgWmHFKjphH1vNR0kF5mgZsat4BkWHThp
5nPEorWBQ9IqTdGf+8zPtwKmiwzgGcaeR64i5Hh9JjhLk56bb7AtrYRChnMXSJor
rLZ/mnbBrdEaSzIi4mWoAC3E8ZnqhAlFqWPKL3DkV0/AP09rYm8RGJ4U+Vaf6y33
3DejuMVdHPULk+kvLHXZn655tSY9e0XCirzCKRufYb1sDvexrqMAjaU0rpgSXXAo
6Ujxl2IP80w+g5h/FonPThP+i4MsFa2jTh1ZIEGk1VdJ0fRMdrBKZBpVj2MDdBi
sG7B+WsIgp6c+pP6zFwVeP5oRzsNadp8n3nuQtffIeSCyH+rQD2Gb0YJfa+lBjUT
Qdq+Ghg0r80CqAu2VoTw4mYCBz3Yilc9JOIiBN9KkHlw9ITKgd00Nb+q46koskh
C9jwEziFfQpzRePzzgCT37MBZFAYrY+LeYfUYdPr2+x1pQr7SVgFstZK/EYJUgZW
LRY8sGh5NQA5xvAvOck7qsN990eqPvqbQtwnVplgPfhbcIHhurKx+DAxuaT+JWnZ
t60fcTdgJ6d2IRxr9iE8XNTKUIJnUMgyeG08LI4zcX/z1ehM8QYFBh2Npu4SJB0n
5lnXijcdShC9vjo=
=NSTr
```

-----END PGP PUBLIC KEY BLOCK-----