RFC 2350

CSIRT

E-DEA

ENGLISH VERSION

Glossary:

- **CISRT**: Equipo de Respuesta a Incidentes de Seguridad Informática (Computer Security Incident Response Team) is a specialized cybersecurity group that monitors, detects and responds to cybersecurity incidents, generally operating 24/7 to protect critical infrastructures, private or public companies. In addition, it can offer technical support, vulnerability management, and coordination for threat mitigation to ensure operational continuity.

- **RFC:** Solicitud de comentarios (Request for Comments) is a numerical document that describes and defines Internet protocols, concepts, methods, and programs. RFCs are currently managed by the IETF.

- **IETF:** Grupo de Trabajo de Ingeniería de Internet (Internet Engineering Task Force). It is a large international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet's architecture and the smooth functioning of the Internet.

- **PGP:** Privacidad bastante Buena (Pretty Good Privacy) Cryptographic security program designed by Phil Zimmermann in 1991 to protect data, emails, and files. It uses symmetric and asymmetric cryptography techniques to encrypt information and ensure that only the intended recipient accesses it, as well as offering digital signatures to authenticate the sender's identity to maximize the security of communications.

1. Document Information:

This document contains the description of the E-EDEA Computer Security Incident Response Team according to the RFC 2350 standard.

1.1. Date of last update:

The current version of this document is version 0.0, published on March 27, 2026. This document is valid until replaced by a later version and will be notified through the official website: https://www.e-dea.co

1.2. Location latest version of the document:

The updated version of this document can be found on the official website: https://www.e-dea.co

1.3. Authenticity of the document:

This document has been signed with the PGP key of E-DEA.

1.4. Location of the document:
- Spanish: https://www.e-dea.co
- English: https://www.e-dea.co

1.5. Identification of the document:
Title: CSIRT E-DEA RCF 2350
Version 0.0
Publication date: 27-03-2026
Expires: This document will be valid until replaced by a later version.

2. Contact Details:

2.1. Team name:
CSIRT E-DEA

2.2. Location:
Carrera 7 N° 156 - 10 Ofic. 1906 -1801, Centro Empresarial North Point, Torre Krystal, Bogotá D.C. – Colombia.

2.3. Time zone:
GMT/UTC -05:00.

2.4. Telephone: +57 (601) 5188433 (Ext. 1111) and cell phone number 317 441 07 61.

2.5. Email:
To report an incident or vulnerability, request awareness, exchange of information related to incidents or make a general query, you must write directly to: seguridad@e-dea.co.

2.6. Public key and encryption of the information:

The PGP key associated with the official email is published at the URL:
https://www.e-dea.co

2.7. Team Members:
No public information is provided about team members. It will be provided in case of needs with our stakeholders.

2.8. Opening hours:
- Enquiries about services: office hours (8.00h-18.00h)
- Incident and vulnerability reporting: 24x7x365

2.9. Points of contact for the community:

Communication between the CSIRT E-DEA and entities at the public, private and civil society levels takes place mainly through official email.

2.10. Additional information: For additional information, please refer to the https://www.e-dea.co website.

2.11. Community Contact Points:

CSIRT E-DEA prefers to receive incident reports by email to seguridad@e-dea.co. Please use our cryptographic key to ensure integrity and confidentiality. In case of emergency, use the [URGENT] tag in the subject line of your email.

3. Constitution:

3.1. Mission:

The mission of the CSIRT E-DEA is to improve the identification, mitigation and response to cyberattacks in the public and private sectors. We use coordinated methodologies to reduce reaction times and impact of incidents, fine-tuning our technological and human capabilities for effective cybersecurity management.

3.2. Circumscription (Jurisdiction) community to which it provides services:

The CSIRT E-DEA is the technology sector incident response support team of public and private organizations that fosters the collaboration of its members and the exchange of information to effectively deal with cyber threats.

3.3. Affiliation:

The CSIRT E-DEA is located within the E-DEA Operations Process.

3.4. Authority:

The CSIRT E-DEA operates, within the Operations Process, under the authority of the Information Security Officer and the E-EDEA Operations Department.

4. Policies

4.1. Types of incidents and level of support

The CSIRT E-DEA is the central point of contact for security-related IT incidents in public and private organizations that are E-DEA's clients.

The level of assistance it provides varies depending on the type and severity of the incident or problem, the type of user, the significance of the impact on critical or essential infrastructure or services, and the resources available from the CSIRT E-DEA at the time.

E-DEA services include reactive and proactive services:

- Alerts and warnings;
- Incident forensics;
- Assistance and support in incident response;
- Incident response and remediation (also on-site);
- Vulnerability and malware analysis;
- Vulnerability response;
- Analysis and sharing of threat intelligence.

4.2. Cooperation, interaction and distribution of information

Incident-related information, such as names and technical details, is not published without the consent of the interested parties. Unless otherwise agreed, the information provided is kept confidential. The CSIRT E-DEA will never share information with third parties unless required by law.

The CSIRT E-DEA within the normal operation of its activities interacts with various stakeholders, including customers, security organizations at the Colombian and international level, such as groups of CSIRTs and intelligence sources, suppliers, manufacturers and media, according to the relationships that it has with each of them, it can also establish communications with different roles with those in charge of information security, engineers, human resources managers, end users and/or journalists.

It is also considered vitally important to establish contact with other incident response teams such as COLCERT, CSIRT-PONAL, COCIB as part of the process of sharing best practices in incident response and environment hardening.
For the distribution of information, the labeling of documents and communications will be used as described below:

Confidential: Information available only for the company's authorized processes and that, if known by unauthorized entities, may have a negative impact of a legal, operational, image loss or economic nature.

Information is classified as confidential in the following cases:
a) Restricted access to senior management.
b) Customer information.
c) It contains confidential information of interested parties (take into account documentation such as policies, non-disclosure agreements (NDAs), reports

with private technical details of the client, contracts).
d) Contains personal information of any of its categories except for public information.

Restricted: Information available for all the company's processes and that, if known by entities without authorization, can have a negative impact on its processes. This information is the company's own or that of third parties and may be used by all the company's collaborators to carry out tasks related to the processes, but it cannot be known by entities without the owner's authorization. It may be shared with third parties with whom it has commercial relations, it applies to documents that are for internal use of the company, such as procedures, meeting minutes, administrative forms, etc.

Public: Information that may be known or published without restriction to any person inside or outside the company, without this implying damage to third parties, or to the activities and processes of the entity, without generating negative impact of a legal, operational, image loss or economic nature.

Within CSIRT E-EDEA, information will be transmitted according to its classification and the need-to-know principle, whereby only anonymized and specifically relevant extracts are transmitted.

When CSIRT E-EDEa receives information that applies the Traffic Light Protocol (TLP), it will respect the information exchange policy defined by FIRST in: https://www.first.org/tlp/.

4.3. Communication y authentication

The preferred method of communication is email. For the exchange of confidential information and authenticated communications, the E-EDA CSIRT uses PGP to encrypt and/or sign messages. All confidential communications addressed to the E-EDA CSIRT must be encrypted with our PGP public key.

The email account and the PGP public key are as follows:

seguridad@e-dea.co
Fingerprint: A3C5489FF3D878E79837D1300C31E08B1D43C54B

PGP Public Key:
mQINBGnf6ikBEAC9glqGwkj4qjp5fZgz6kW9MxpiWcbyU6kMtOS33zJl0XzaMByV
4aZZF6G4KjqQB/7xVaaWVRDWtRfuhx9DcvEUYdDfQWVCoXuq52tiZ5xUlZQBvp
HwuGUVSNfFKjsrtmkrWRVnC50gP/zRLuEM7jVv0uIZU1HjXtXBGfRlMWDcyClaS8
Vnj0BtPt9+3xmzB35cdArwYO5wo+jLoWZ/f/ioLvcPumCdQpLSCefl7afAU62SOu
Z24s++9HFmhm5kBW50e1L+TdjMqm0dDQsa5JXYIm0Y56np+ZkpcAzGYD/xqd
FZ5WozTHd8SdVlHZhXJ+ha+YTZnMNBt01W3cZaAi2Tf9mD4bpMnVdDtlvymzN

U8Z84rh3GdzfI0C3uqxUVJdASoEzMBtBIr0IHFDMcP4KhRh0caMwf7HaiLsnNHk
SbW0+ucUjz0NQzqRgbvaKTDpd6PSlYsYh5YfMrXw0LIkw0ggj6re38P8AX28Tip
pZVIKnoLyvL/Eiuve7lJx61lEbbu2XBpma6Xsskt2Fl2kXHBcZm5b1cuY0+Eu0n8i
WzBWS1onTyEmueh/4JYPKQDDTEhXmNMJgpQg08fm2qG3KMU6J6X/e4jPjtyL
uqdpMG7jSLwkXhqm0Wjwgs16hR6EzHIkTZHH5Mj18u9g0A1u/ItnDTpgfDhN0HI
uqSNl+23QARAQABtCBDU0ISVCBFLURFQSA8c2VndXJpZGFkQGUtZGVhLmNvP
okCcwQTAQgAXRYhBKPFSJ/z2HjnmDfRMAwx4IsdQ8VLBQJp3+opGxSAAAAA
AAQADm1hbnUyLDIuNSsxLjEyLDIsMQIbgQUJBaTF5wULCQgHAgIiAgYVCgkICwI
EFgIDAQIeBwIXgAAKCRAMMeCLHUPFSyvsD/4kTw+NRbVGmJfvvaR8WPnmDA
WvILI0Em05q/YSd4xjUVARcmV0Fh0i4QfLVTCw3ykKVgyGTSs65Y6SpTvuiSFV
PWWoxpxfmfGkzFW/18GUUf7w0RdanG3Z7ZQQTSqLvhEM7NU7HF/3S/Lf3TyQQ
t3RLdBeHHuNvajxiwqZ++tqyfC7KlqbAY2o0rBPSkPAVImdnFXA7hdHStwHEGtS
8HeoE1Ak/O3gL+7BilXDUFhstpRGf7h3BJKgq8s5dtxyjJHTHR0JP3W+nmrD+Ib
PEo1QqqV3AazqJJHEcw/yMvFO735XnDy5+JexipyYAtZSdwmaBq/2KzFxYVGV
H7p8s6wScwoact7RMY0wxGICfbawTNVjGwz560n27JLv4vkzlADi0mqvZm7AE
Wh8IrcALIBduYeen1ScdG/2aNGa7H7mYrzynKLDCm2x8MgJyS4S9BBTI4J46wH
CjN0z6EbN7zHQhYc/ELX0oBPZgc1ylEJ0aIbFV/hv3+NMDg6RjmUCI/z0TMghUc
0AS91pNzhSoekRYFS2vcVQ0xxJ/Jli0DfnOnAX0mH/yUt++RoBBQDuC0jHRMhp
dpsrh0kD0XQ3kf7Gipy/2d4mwivWdZt0b12Al1flqbTzsFUZG3LhmTHk2XH0//LsZ
BzBlPlmvivwmaIBnGl8sol0sUB0WEhLCluQxbkCDQRp3+opARAAtcfkv0Bv4pK0
T1Xrc9f0CoRQU8klTajjeg9l8vvdl9oS4m81pPx5kjViwB9PPmGA9/0rgYPiavj0e5/
5/K0HeGldUEUrZbIe7fu4LvFMJcX9zDsJHCA+S3KmF05bM9ae3bX4XlYjXSeMN
emJAGvTlXab6XYzWSxtRj0h5402yr0awQytihhIcaj37EDQ7tikgapY/9Jh3rCZeYv
zT17xfwqEV5B53jSbQLNSi3BRUiAPAIW1g3vTZt7aPlW+eTSNM2wTE7N4Fuk0RCj
6wAVEWoSh0hzugakgF0UGwS4VFgkV3a52RP5fBMW22Bk6qpp0kHRQR3bcy/z
vMP+VarI2PB++7LrU/vvTHGcXDoVN6pb/jYzIRkbQh8bkTHsH7NfuegJFxIvbP00
qx+Zx+29ARZmNUJYy0YSsShUqo8Savj36ahHHSSatudUk9LjShISRAdFZqYc10
eKms6IKWqeIcBS95b8yNafazPL00K1vh4Fbe2nzpl0mDJ+fFgFwLPfeKW52sNJ/
koqZNwfbTzuY3/A5W7kRbsiurZLwEQ0VgNRvA7OBO9n7uLUd/1up2mFn0UBGft
FGSD4YQO9MainZunM/pGClMpRmrm+kUSNDQ8q5u9WsnZeru1CZBwZow00TjY
cNoK1P3wZHq7S+0VBy/klSm64nTI9QZN92Cg2seP0AEQEAAYkCWAQYAQgAQh
YhBKPFSJ/z2HjnmDfRMAwx4IsdQ8VLBQJp3+opGxSAAAAAAAQADm1hbnUyL
DIuNSsxLjEyLDIsMQIbDAUJBaTF5wAKCRAMMeCLHUPFSw3GEACTw/2DzB8GX
NW2ZFVty6N0wZW4wAtrV1xK9KaDw0Qs8CT3bsMXC9gyhZNDnxGK8/ZcLsgyb
85/fAL4RuhbFxCXiT0at21mrkn0dzTCRtNFX9Dr7H6XgZs2ltzHdHNf0JtrFcND42
sW+mLBbvDCJCzyEvtDRJx0dArXNkwt5XTgEerQTr5iFUUn1EfkCKPIBg7Z4Nc6P
NqIcwV+fNdrsIfAY4dIKxA4+E6UB8frSXZEhch7p7fPoYfbr01iw3qYviEWSrAX/48
0C4NfsYajrJlZ0d3DuKF2uj0qPdI68ID4RzLhfqUfgV84BwcAYXq+3bQNrEoGKUV
b/DjBTKnGeBl638I5SJDwBbGZVYkSC3Y2cq9aBZNQsm9/ITWAM+glrxWf3z8X8
GjNI1ohlwZI6oCgdCM/NxqsOolZI5uhn17DzmUswpPPhMJWjRtZ0B5Z/FSG4745g
cHahX5vwixi66J9rJjTwTH2bW2Wufg/KS3d1n7tLYLA0r+FhP8MCie/guHmLX2A
0EJEjONSp6HvA3Gg69SFE6cThudm0Glf8Xvt4MQVyvta40eE8HazBAQx6AFaY
akPMtzcn5WkEaQQfixY53IovjUb7L8Fs0d7uaWjW9U9ffKYus3amZ1g45RvhJcKF
TyAl8lq60Kr2k5PzDKwThJwe8ayBrezRbiGpzvE57kCDQRp3+pDARAAn8z0DLgc
GYTQkDDKr+IXMjlBfxwAswRXxxNl8i/Zv+dbRDe216X/xuX/2hk6SMvWIntWk57+1

46LsJo0HLuRiHeouME5R5pENDimsQAW7us8nw7fnZzntM0t2mlzpuKKUiq+TX6
0QQTF6er0IDap1WrxQTaQnDYKqti9yWf2dmXaB9eZLZ8hcr0uoQSnFVYQ6zKGzz
NTWweEsAFH46p3n3bnzf/k8CLpY82vBMNi0/pZi145jmDastAG4ILKlx69dbwbn
R0UipWVTAZgbKqE+vMeGfeJQcDb/cr8dfR0PztX1Y5wIvZvRSsXggCgEWjtijdGC
zHPVxBTwO/IVV0DWxKWx4zr0Is1Lgkf9CeFdBl1QaLZudwQYgsc6wUo3dWRMu5
E6MCNAdo52NaRo4cedkQdC3ejxyKZlNjUtGtr5Yq6/2xU8mIv5hZNsIwZrA1xQZY
tCr+UYmIltfueYxS4wx9qXw5mHWvKZ4GOOxP3dWW1ElMbLLnjNSQDpP/DJ3f0j
GAn9RTE/6LEToR6wQKhf+GLyAPdMantw05Z0YNS57ESxkumkaVzMdPFxtC5Q
6xhyMfCmLoJNSEgPmpXN6a4pSQLb9qxN7sBzYpiD0XxLj5vT2OENzDdoCIhwY
D42Ir5qU4KgVyR5tRrs70eJL3m3qq1tUQq7vCITmR5Drifj8sAEQEAAYkEiAQYAQ
gAPBYhBKPFSJ/z2HjnmDfRMAwx4IsdQ8VLBQJp3+pDGxSAAAAAAAQADm1hb
nUyLDIuNSsxLjEyLDIsMQIbAgJACRAMMeCLHUPFS8F0IAQZAQgAHRYhBPQQVg
P6l1gafYtg7PycTP7zYKasBQJp3+pDAAoJEPycTP7zYKasrPcQAJFsd7L23A1K8qi
Cr4pyKst5VqcoahbULn+OO0UkcHNzhTzkLQ1D2jGQkdilXnXcYaZsWLc5aWU70u
+gKKSpxdCHi+lJBl5W7ffH6iatsPkywZQDKHRqJbjlxCxNSye78xzELhnvw93e88G
S/pbdS3kpVWGVw3dNHtzF2LcdWxda9+6Z49D5ob2TavXCvWW63dl/pv0MjBko
JjF4+RMjrvcTrjytuVAKFq+W9sTLkTnAKRLUliSRK8ne+ExZkUXMf07xaUDoq9NU
TZfrBQ0NM2pV6a0cqFezgtoZm1WydGjJHgTwTVf1Ps60G7A09khfymaTQJBT7O
ynA5QRgi53HLN8EVUPoMOy0YggRlicQhuQIWmXII/JCe78rKlq0dfgq5mH7KFiZd
uNvcY6BjVXRx7Gj9SZqLrT9uCYwr1fUEAMv0xQqm7kfxoF9MVXvCGcbeg5BEiBB
HpU5vEAERJ3kTmNozmBHxVq9rHsnJv99pZFYDEpZYQ8LQ+TVtf9ZXd9iH0Azt
KBTEbRlj4SGHuTZeurNgmF8v5hqxEQhLzK04EMMljrEUoUhS0/0gHwIES3Ksb8A
MtsbPhn0sZBGZMeeXcEEsPv3KXuTYLnH67r021YJXY+xfnbA/ge5u0uEfPIBh83
08LTRgNyAZKKv26aXyjfXwV30qfK90LgdILuWT6FaQsQAJvQKMi/PwLLYcoIbw9
FYQvkRoUciEx0j6oUx74H9cifYYXGUKEU6H8vpYcoU1s0qZ83nkB5rxysyd90Ua
U8clJcfCG9cT0cYVAcBt2XE4uEJMK5hdqZtNrYc6HtKnf0aNXdjuII5EadY8VDby
H0zHbm2m9WMcsr14vgigKJT9zYqh0cqfNGdIT2Ju3tayNKyLtDNr1Jo0Io39wdE
b5IbQa6/JNpCDy1LYZJ1LI7LXc0/ex143a3q07jjdfAtAurFiV72O9511tjxQGbUoT2g
RXQIUF7nnvCce9maV9m9nbdfspIS+sSnenu21uaWaLahhlqRxG3qevFs4ix1pZw
WqXSdB7ao3jWVN38hpBGaHnPHQgEeQG4m8YWFrka5TleY5X3J5/hQpyXOpOy
RqxaKLAyUUKw7MHwD+KnrIxTTdyeZlxq7TW8ex4vNjCd+5xmpDvb2x2U67qHyR
MW7IYBuoZ1oFEpIv1TFgZyVJ+kxO+iNeoiMxKZbDnpC5tQIxWwriPlPJdQywuOIvrI
lOuUBNfCoEW3UPgSPmHtaDKL2Y/bdvsfcZi344EK6evJ2wIIMLp5x9FU4qF7y+
wwa7IUa86GI+pu9boH9vyDKkx4kWvyIQznQUAfB3ZGw1QE/SUKiiU7Im6sEFNNR
ULis13oS263sKKq+h/Z0vKiFnnRL78o
=2iO6

5. Services

5.1. Proactive Services

Proactive services are a set of actions and strategies implemented to identify, prevent, and mitigate potential threats and vulnerabilities in computer systems

before security incidents occur. Proactive services aim to anticipate threats. These services allow organizations to strengthen their security posture, reduce the risk of attacks, and minimize the impact of potential incidents.

Alerts and warnings.
This service provides early notifications about threats, vulnerabilities, and suspicious activity in an organization's digital environment.

Vulnerability analysis.

Vulnerability analysis is a service that identifies, evaluates, and prioritizes weaknesses in systems, networks, or applications to prevent potential attacks and strengthen cybersecurity.

Communications and announcements.

To disseminate clear and timely information on threats, vulnerabilities, updates and best practices to protect organizations and users against cyberattacks, strengthening awareness and digital security.

Security assessments or audits.

Systematic processes that analyze and verify an organization's policies, controls, and systems to identify vulnerabilities, ensure regulatory compliance, and improve protection against digital threats.
Network monitoring.
Monitoring of IOC and IOA.
The monitoring service for Indicators of Compromise (IOCs) allows you to identify specific evidence of a threat, such as files, IP addresses, or hashes, while Indicators of Attack (IOAs) show how these threats are affecting or compromising the integrity of systems, allowing for a quick and effective response to security incidents.

5.2. Reactive Services
Services that consist of responding to and managing security incidents, such as attacks or breaches, to quickly detect, contain and remedy threats and minimize their impact on the organization.

Incident analysis.
It consists of identifying, assessing and responding to events or threats that compromise the security of systems and data, with the aim of mitigating damage, preventing future occurrences and strengthening the protection of digital infrastructure.

Incident response.

It consists of the detection, analysis and mitigation of attacks or security breaches in computer systems, with the aim of minimizing the impact and restoring the security of the organization effectively and quickly.

Incident response coordination.
Activities that seek to execute an organized process involving different teams and entities to effectively detect, contain, mitigate and recover from cyber threats and attacks, ensuring the protection of digital assets and the continuity of operations.

Remote assistance for vulnerabilities and incidents.

Remote vulnerability and incident assistance involves providing remote technical support to identify, analyze, and resolve cybersecurity issues, such as vulnerabilities, attacks, or incidents, through secure remote connections.

5.3. Security Management

It consists of planning, implementing and maintaining policies, procedures and controls to protect digital assets, prevent threats and respond effectively to incidents, ensuring the confidentiality, integrity and availability of information.

Security consulting.

Specialized service that helps organizations identify, assess and mitigate digital risks, ensuring the protection of their systems, data and assets against cyber threats in processes or areas.

Awareness.

Activities that seek to raise awareness among users about good digital practices, promoting the responsible and safe use of technology to prevent threats such as malware, phishing and online fraud.

Knowledge transfers.

It consists of sharing and disseminating information, technical skills, and best practices among individuals, organizations, and communities to improve the protection of systems, data, and networks against digital threats.

Risk analysis.

It consists of identifying, evaluating and prioritizing the threats and vulnerabilities that can affect an organization's digital assets, in order to

implement preventive and corrective measures to protect critical information and systems.

6. Incident reporting form

No special forms are needed to report third-party security incidents.

When a customer detects a security event or incident, they can report it to the CSIRT E-DEA via seguridad@e-dea.co email. In the exchange of this information, protection measures will be used, through the use of PGP keys. These measures will take into account both the classification of the information and the agreements that have been established with each customer at the beginning of the provision of the service.

7. Disclaimer

While all necessary precautions will be taken in the preparation of information, notifications and alerts, CSIRT E-DEA assumes no responsibility for errors or omissions, or for any damage resulting from the use of the information contained therein.

Version	Date	Description of the change
00	27/03/2026	Document creation

Prepared by:	Reviewed by:	Approved by:
German Serrato	Maure Muñoz Luna	Juan Fernández
Chief Information Security Officer (CISO)	Security and Information Compliance Officer	Chief Technology Officer (CTO)