# CSIRT-NOVIGO Norma RFC 2350

| VERSION CONTROL | | | | | |
|---|---|---|---|---|---|
| VERSION | DRAFTED BY: | REVISED | APPROVED | DATE | DESCRIPTION |
| 1.0 | Angelo Guzman | Alex Martinez | Alex Martinez | 24/10/22 | Approval of document v.1.0 |
| | | | | | |
| | | | | | |

| DISSEMINATION | |
|---|---|
| SAFETY LEVELS | DESCRIPTION OF ACCESS |
| Level 1 ☐ | Confidential. Maximum level of document protection. |
| Level 2 ☐ | Restricted, non-editable, non-downloadable, read-only permission. |
| Level 3 ☒ | Public, non-editable, read permission, downloadable. |

# CSIRT-NOVIGO

# NORMA RFC 2350

Cybersecurity
consulting

# INDEX

# 1. Document Information

## 1.1. Date of last update

Version 1.0, published on October 24, 2022.

## 1.2. Distribution list for notifications

Changes to this document are not distributed through a mailing list. For any specific questions or comments, please contact csirt@novigotek.com.

## 1.3. Document Location:

The latest version of the document is published in: English:
https://n9.cl/rfc2350
English: https://n9.cl/rfc2350-es

# 2. Contact information

## 2.1. Team Name

CSIRT-NOVIGO, NOVIGOTEK's Computer Security Incident Response Team.

## 2.2. Address

Alfil Building - Av. de los Shyris 1548, Quito 170135.

## 2.3. Time Zone

America/Guayaquil (GMT -5)

## 2.4. Phone Number:

(593) 9 8726 8884
(02) 2 6011 702

### 2.5. E-mail address:

csirt@novigotek.com

### 2.6. Public keys and data encryption:

Not available

### 2.7. Team Members

Alex Martinez Eng.
Angelo Guzmán Eng.

### 2.8. More Information

Information general about can be found at about CSIRT-NOVIGO the can be found at at https://www.novigotek.com/csirt

### 2.9. Customer contact points

To communicate with CSIRT-NOVIGO about vulnerability information or security alerts, you can use means such as e-mail or telephone.

### 2.10. Hours of Operation

The incident response team is available during the following hours:

- Service inquiries: office hours (8:00 a.m. - 6:00 p.m.)
- Incidents classified as low, medium or high hazard: office hours (8.00h18.00h)
- Incidents classified as very high or critical danger: 24/7, 365 days a year.

# 3. Constitution

## 3.1. Mission

Protect the information technology infrastructure in organizations and ensure the confidentiality, integrity and availability of information by identifying and mitigating vulnerabilities, managing security incidents and protecting the organization's information assets.

## 3.2. Community Served

All governmental entities and companies.

## 3.3. Sponsorship / Affiliation

The CSIRT-NOVIGO is part of the NVG which is a multinational business group dedicated to Information Security, Cybersecurity, IT Consulting and International Standards Certification Body.

# 4. Policies

Our CSIRT-NOVIGO team operates under the following policies to ensure a fast and effective response to information security incidents:

## 4.1. Incident Reporting Policy

All security incidents must be reported immediately to the CSIRT- NOVIGO team. For this purpose, we have a secure and confidential communication channel that can be used at all times.

### 4.2. Incident Management Policy

Our CSIRT-NOVIGO team has clear procedures and guidelines for responding to and resolving information security incidents. These procedures include incident identification, impact assessment, incident containment and recovery of affected information.

### 4.3. Incident Data Access Policy

Information related to information security incidents is handled confidentially and is only available to authorized members of the CSIRT- NOVIGO team. In addition, access restrictions are applied according to the level of confidentiality of the information.

### 4.4. Confidentiality policy

At CSIRT-NOVIGO, we take the confidentiality of information related to security incidents very seriously. For this reason, additional security measures are put in place to protect the information and the privacy of those affected is guaranteed.

### 4.5. Training and awareness policy

All members of the CSIRT-NOVIGO team receive regular training and education to improve their skills and knowledge in the field of information security. We also provide information and awareness to our network users to reduce the risk of incidents.

### 4.6. Documentation Policy

All information security incidents are documented in detail, including information related to the nature of the incident, the actions taken and the results obtained. The information is stored securely and is only available to authorized members of the CSIRT-NOVIGO team.

### 4.7. Evaluation and continuous improvement policy

We are committed to regularly evaluate the performance of our CSIRT- NOVIGO team and to continuously improve our processes and procedures to keep up with changes in security threats and technological advances.

## 5. Services

Our computer security incident response team. We offer a wide range of proactive, reactive and quality security management services to help protect your organization against cyber security threats.

### 5.1. Proactive services:

- Threat monitoring and detection: CSIRT-NOVIGO can use monitoring and detection tools to identify potential security threats before they become security incidents.
- Vulnerability and risk assessments: CSIRT-NOVIGO may conduct periodic assessments of the security of the organization's network and systems to identify potential security vulnerabilities and risks and take preventative measures before security incidents occur.
- Security education and awareness: The CSIRT-NOVIGO can provide training and education to the organization's employees on IT security best practices to improve the security culture and reduce the likelihood of security incidents.

### 5.2. Reactive services:

- Incident analysis and response: CSIRT-NOVIGO can investigate and respond to computer security incidents, such as cyber attacks, malware and data theft, to minimize the impact and spread of the incident.
- Forensic analysis: CSIRT-NOVIGO can perform forensic analysis on systems affected by security incidents to identify the source of the problem and gather evidence for possible criminal investigations.

### 5.3. Security quality management services:

- Coordination with other incident response teams: CSIRT-NOVIGO can work together with other incident response teams, such as government agencies and industry organizations, to share information and resources and improve the overall response to security threats.
- Continuous improvement: CSIRT-NOVIGO may periodically review and update its security policies and procedures to ensure that they adapt to changes in the threat environment and security technology.

## 6. Incident reporting forms

Incident reporting can be done by:

- E-mail: csirt@novigotek.com
- Security Incident Form: https://www.novigotek.com/csirt

## 7. Disclaimer

The CSIRT-NOVIGO Team is not responsible for any misuse of the information contained herein.