# CSIRT-NOVIGO Norma RFC 2350

| CONTROL DE VERSIONES | | | | | |
|---|---|---|---|---|---|
| **VERSIÓN** | **ELABORADO POR:** | **REVISADO** | **APROBADO** | **FECHA** | **DESCRIPCIÓN** |
| 1.0 | Angelo Guzmán | Alex Martínez | Alex Martínez | 24/10/22 | Aprobación del documento v.1.0 |
| | | | | | |
| | | | | | |

| DIFUSIÓN | |
|---|---|
| **NIVELES DE SEGURIDAD** | **DESCRIPCIÓN DE ACCESO** |
| Nivel 1 ☐ | Confidencial. Máximo nivel de protección del documento. |
| Nivel 2 ☐ | Restringido, no editable, no descargable, solo permiso de lectura. |
| Nivel 3 ☒ | Público, no editable, permiso de lectura, descargable. |

## ÍNDICE

# CSIRT-NOVIGO

# NORMA RFC 2350

# 1. Información del Documento

## 1.1. Fecha de la última actualización

Versión 1.0, publicada el 24 de octubre de 2022.

## 1.2. Lista de distribución para notificaciones

Los cambios a este documento no se distribuyen por una lista de correo. Cualquier pregunta o comentario específico, por favor diríjase a la dirección de correo csirt@novigotek.com

## 1.3. Ubicación del Documento:

La última versión del documento se encuentra publicada en:
Español: https://n9.cl/rfc2350
Inglés: https://n9.cl/rfc2350-es

# 2. Información de contacto

## 2.1. Nombre del Equipo

CSIRT-NOVIGO, Equipo de Respuesta a Incidentes de Seguridad Informática de NOVIGOTEK.

## 2.2. Dirección

Edificio Alfil – Av. de los Shyris 1548, Quito 170135.

## 2.3. Zona Horaria

América/Guayaquil (GMT -5)

## 2.4. Número de Teléfono:

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

### 2.5. Dirección de Correo Electrónico:

csirt@novigotek.com

### 2.6. Llaves Públicas y encriptación de información:

No disponible

### 2.7. Miembros del Equipo

Ing. Alex Martinez
Ing. Angelo Guzmán

### 2.8. Más Información

Información general acerca del CSIRT-NOVIGO la puede encontrar en https://www.novigotek.com/csirt

### 2.9. Puntos de contacto para clientes

Para comunicarse con el CSIRT-NOVIGO acerca de información de vulnerabilidades o alertas de seguridad, puede utilizar medios como correo electrónico o teléfono.

### 2.10. Horario de Atención

El equipo de respuesta a incidentes está disponible en los siguientes horarios:

- Consultas sobre servicios: horario de oficina (8.00h-18.00h)
- Incidentes catalogados con peligrosidad baja, media o alta: horario de oficina (8.00h18.00h)
- Incidentes catalogados con peligrosidad muy alta o crítica: 24/7 los 365 días.

# 3. Constitución

## 3.1. Misión

Proteger la infraestructura de tecnología de la información en las organizaciones y garantizar la confidencialidad, integridad y disponibilidad de la información a través de la identificación y mitigación de vulnerabilidades, la gestión de incidentes de seguridad y la protección de los activos de información de la organización.

## 3.2. Comunidad a la que brinda Servicios

Todos los entes gubernamentales y empresas.

## 3.3. Patrocinio / Afiliación

El CSIRT-NOVIGO forma parte del NVG que es un grupo empresarial multinacional dedicado a la Seguridad de la Información, Ciberseguridad, Consultoría IT y Entidad Certificadora de Normas internacionales.

# 4. Políticas

Nuestro equipo CSIRT-NOVIGO opera bajo las siguientes políticas para garantizar una respuesta rápida y efectiva ante incidentes de seguridad de la información:

## 4.1. Política de notificación de incidentes

Todos los incidentes de seguridad deben ser notificados inmediatamente al equipo CSIRT-NOVIGO. Para ello, contamos con un canal de comunicación seguro y confidencial que se puede utilizar en todo momento.

### 4.2. Política de manejo de incidentes

Nuestro equipo CSIRT-NOVIGO cuenta con procedimientos y pautas claras para responder y resolver incidentes de seguridad de la información. Estos procedimientos incluyen la identificación del incidente, la evaluación del impacto, la contención del incidente y la recuperación de la información afectada.

### 4.3. Política de acceso a datos de incidentes

La información relacionada con los incidentes de seguridad de la información se maneja de manera confidencial y solo está disponible para los miembros autorizados del equipo CSIRT-NOVIGO. Además, se aplican restricciones de acceso según el nivel de confidencialidad de la información.

### 4.4. Política de confidencialidad

En CSIRT-NOVIGO, nos tomamos muy en serio la confidencialidad de la información relacionada con los incidentes de seguridad. Por esta razón, se establecen medidas de seguridad adicionales para proteger la información y se garantiza la privacidad de los afectados.

### 4.5. Política de capacitación y concienciación

Todos los miembros del equipo CSIRT-NOVIGO reciben capacitación y formación periódica para mejorar sus habilidades y conocimientos en el ámbito de la seguridad de la información. También proporcionamos información y concienciación a los usuarios de nuestra red para reducir el riesgo de incidentes.

### 4.6. Política de documentación

Todos los incidentes de seguridad de la información se documentan de manera detallada, incluyendo la información relacionada con la naturaleza del incidente, las medidas tomadas y los resultados obtenidos. La información se almacena de manera segura y solo está disponible para los miembros autorizados del equipo CSIRT-NOVIGO.

### 4.7. Política de evaluación y mejora continua

Nos comprometemos a evaluar regularmente el desempeño de nuestro equipo CSIRT-NOVIGO y a mejorar continuamente nuestros procesos y procedimientos para mantenernos al día con los cambios en las amenazas de seguridad y los avances tecnológicos.

## 5. Servicios

Nuestro equipo de respuesta a incidentes de seguridad informática. Ofrecemos una amplia gama de servicios proactivos, reactivos y de gestión de calidad de seguridad para ayudar a proteger a su organización contra las amenazas de seguridad informática.

### 5.1. Servicios proactivos:

- Monitoreo y detección de amenazas: El CSIRT-NOVIGO puede utilizar herramientas de monitoreo y detección para identificar posibles amenazas de seguridad antes de que se conviertan en incidentes de seguridad.
- Evaluaciones de vulnerabilidades y riesgos: El CSIRT-NOVIGO puede realizar evaluaciones periódicas de la seguridad de la red y los sistemas de la organización para identificar posibles vulnerabilidades y riesgos de seguridad y tomar medidas preventivas antes de que se produzcan incidentes de seguridad.
- Educación y concientización de seguridad: El CSIRT-NOVIGO puede proporcionar capacitación y educación a los empleados de la organización sobre las mejores prácticas de seguridad informática para mejorar la cultura de seguridad y reducir la probabilidad de incidentes de seguridad.

### 5.2. Servicios reactivos:

- Análisis y respuesta a incidentes: El CSIRT-NOVIGO puede investigar y responder a los incidentes de seguridad informática, como ataques cibernéticos, malware y robo de datos, para minimizar el impacto y la propagación del incidente.
- Análisis forense: El CSIRT-NOVIGO puede realizar análisis forenses en los sistemas afectados por incidentes de seguridad para identificar la fuente del problema y recopilar pruebas para posibles investigaciones criminales.

### 5.3. Servicios de gestión de calidad de seguridad:

- Coordinación con otros equipos de respuesta a incidentes: El CSIRT-NOVIGO puede trabajar en conjunto con otros equipos de respuesta a incidentes, como agencias gubernamentales y organizaciones de la industria, para compartir información y recursos y mejorar la respuesta global a las amenazas de seguridad.
- Mejora continua: El CSIRT-NOVIGO puede revisar y actualizar periódicamente sus políticas y procedimientos de seguridad para garantizar que se adapten a los cambios en el entorno de amenazas y la tecnología de seguridad.

## 6. Formas de notificación de incidentes

La notificación de incidentes puede realizarse mediante:

- Correo electrónico: csirt@novigotek.com
- Formulario de incidentes de seguridad: https://www.novigotek.com/csirt

## 7. Disclaimer

El Equipo CSIRT-NOVIGO no se responsabiliza del mal uso que pueda darse de la información aquí contenida.