CSIRT-NOVIGO

NORMA RFC 2350

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.

1. DOCUMENT INFORMATION

1.1. Date of Last Update
The current and definitive version is 3.0, formally approved and published on June 3, 2026.
1.2. Distribution List for Notifications
Changes to this document are not distributed via a public mailing list. Critical updates and modifications to operational policies are exclusively notified to our strategic partners, affiliated government entities, and corporate clients through our secure intelligence distribution channels.
1.3. Locations where this Document May Be Found
The official and current version of this document is always available for review on the official Novigotek public security and incident response portal.

2. CONTACT INFORMATION

2.1. Name of the Team
CSIRT-NOVIGO (Computer Security Incident Response Team - Novigotek).
2.2. Address
Av. de los Shyris 37-313 y Telegrafo edf Rubio ofc 301. Quito, Ecuador.
2.3. Time Zone
America/Guayaquil (GMT -5). Our jurisdiction does not observe Daylight Saving Time (DST).
2.4. Telephone Number
- **Administrative and General Inquiries:** (593) 2 6011 702
- **24/7 Emergency Line (Strictly for critical incidents):** (593) 9 8726 8884

2.5. Email Address
For incident reporting, operational inquiries, and intelligence coordination: nv.csirt@novigotek.com
2.6. Public Keys and Encryption
CSIRT-NOVIGO strictly requires the use of PGP/GPG for all communications containing sensitive information, Zero-Day vulnerability reports, non-public Indicators of Compromise (IoC), or confidential victim data. The public key is published on our official portal.
Fingerprint: csirt-novigotek_0x91CFF8FC06845F43_public.asc
2.7. Team Members
The executive direction of CSIRT-NOVIGO is overseen by the cybersecurity general management (Alex Martinez). The core operational team consists of threat intelligence analysts, incident response engineers, a project manager, and commercial support staff.
2.8. Other Information
For detailed corporate information, service scope, and credential validation, please refer to the main Novigotek website.
2.9. Customer Contact Points
Corporate clients with active support agreements must prioritize the channels defined in their Service Level Agreements (SLA) or utilize the designated monitoring platform for automated escalated attention.
2.10. Hours of Operation
Standard Business Hours: Monday to Friday, 8:00 a.m. to 6:00 p.m. (Ecuador Local Time).
Emergency Support (High and Critical Severity): 24/7 reactive support, 365 days a year.

3. CHARTER

3.1. Mission
To provide advanced, comprehensive cyber defense—both proactive and reactive—to protect the technological infrastructure of organizations, enterprises, and governmental institutions. CSIRT-NOVIGO identifies and mitigates vulnerabilities leveraging structured threat intelligence (CTI), ensuring the Confidentiality, Integrity, and Availability (CIA triad) of critical information assets.
3.2. Constituency
Our protected community includes national critical infrastructures, government entities, our portfolio of corporate clients based in Ecuador and the United States, and allied organizations within our technological supply chain.

3.3. Sponsorship and Affiliation
CSIRT-NOVIGO is a specialized operational arm belonging to Novigotek, a firm focused on technological architecture, information security, and Governance, Risk, and Compliance (GRC) platform development.

3.4. Authority
The team operates under the executive mandate of Novigotek's leadership. For incidents within its own infrastructure, CSIRT-NOVIGO possesses absolute and immediate authority to isolate nodes, suspend services, and execute remediations. For external operations, intervention authority is strictly limited to and governed by the legal contracts and pre-established incident response agreements with each respective client.

4. POLICIES

4.1. Types of Incidents and Level of Support
The CSIRT categorizes incidents based on standardized methodologies (e.g., NIST SP 800-61). Operational prioritization is determined by technical impact and business risk. Incidents involving active data exfiltration, ransomware, or denial of service against critical infrastructure receive unconditional top priority.

4.2. Co-operation, Interaction and Disclosure of Information
CSIRT-NOVIGO recognizes the critical need for cross-sector collaboration. We share structured intelligence with other global response teams through federated platforms (e.g., MISP nodes). All shared information is strictly governed by the Traffic Light Protocol (TLP), ensuring data is not disseminated beyond the authorized audience.

4.3. Communication and Authentication
Emitter authentication for critical reports is verified using cryptographic signatures (PGP). CSIRT-NOVIGO reserves the right not to process executive requests or infrastructure change orders originating from unauthenticated or anonymous sources.

4.4. Rights and Obligations
To ensure corporate and governmental compliance, our incident management policies strictly adhere to:

- **National:** The Organic Law on Personal Data Protection (LOPDP) of the Republic of Ecuador.
- **International:** The General Data Protection Regulation (GDPR) of the European Union.

4.5. Data Retention and Handling
All collected digital evidence (memory dumps, logs, network captures) is handled under strict chain-of-custody controls. This data is stored in offline or heavily encrypted local repositories, ensuring access is exclusively granted to explicitly authorized personnel.

5. SERVICES

Service Category	Technical Description
Proactive Services	• Continuous Cyber Threat Intelligence (CTI) monitoring. • External Attack Surface Management (EASM) assessments. • Security audits, penetration testing, and continuous vulnerability scanning.
Reactive Services	• Rapid deployment for incident response (identification, containment, and eradication). • Digital forensics (file system and memory analysis). • Secure restoration and business continuity support.
Quality Management (GRC)	• Synchronization of intelligence and Indicators of Compromise (IoC) with the broader community. • Continuous updating and simulation of Incident Response Playbooks.

6. INCIDENT REPORTING FORMS
Community members and external actors may report anomalous events or confirmed incidents via:

- **Direct Email:** Addressed to the official support account, attaching headers, log files, and a chronological description of the event. We strongly recommend encrypting the email body with our PGP key.
- **Online Form:** Utilizing the secure reporting portal available within the CSIRT section of our corporate website.

7. DISCLAIMER

While the team invests maximum technical effort in ensuring the accuracy of security warnings, vulnerability bulletins, and mitigation guidelines, CSIRT-NOVIGO assumes no legal or financial liability arising from errors, omissions, or the direct application of this information by third-party entities. The implementation of countermeasures remains the sole responsibility of the local network administrators.

CSIRT-NOVIGO - Norma RFC 2350 (Perfil Operativo)

1. INFORMACIÓN DEL DOCUMENTO

1.1. Fecha de última actualización
La versión actual y definitiva es la 3.0, aprobada y publicada formalmente el 3 de junio de 2026.
1.2. Lista de distribución para notificaciones
Los cambios en este documento no se distribuyen a través de una lista de correo pública general. Las actualizaciones críticas y modificaciones a las políticas operativas se notifican exclusivamente a nuestros socios estratégicos, entidades gubernamentales afiliadas y clientes corporativos a través de nuestros canales seguros de distribución de inteligencia.
1.3. Ubicación del documento
La versión oficial y vigente de este documento se encuentra siempre disponible para su consulta en el portal web público oficial de seguridad y respuesta a incidentes de Novigotek.

2. INFORMACIÓN DE CONTACTO

2.1. Nombre del equipo
CSIRT-NOVIGO (Computer Security Incident Response Team - Novigotek).
2.2. Dirección postal
Av. de los Shyris 37-313 y Telegrafo edf Rubio ofc 301. Quito, Ecuador.
2.3. Zona horaria
America/Guayaquil (GMT -5). Nuestra jurisdicción no aplica horarios de verano (DST).
2.4. Números telefónicos
- **Atención administrativa y general:** (593) 2 6011 702
- **Línea de emergencia 24/7 (Exclusiva para incidentes críticos):** (593) 9 8726 8884

2.5. Dirección de correo electrónico
Para el envío de reportes de incidentes, consultas operativas y coordinación de inteligencia: nv.csirt@novigotek.com
2.6. Claves públicas y cifrado
CSIRT-NOVIGO exige el uso de PGP/GPG para toda comunicación que contenga información sensible, reportes de vulnerabilidades Zero-Day, indicadores de compromiso (IoC) no públicos o datos confidenciales de víctimas. La clave pública se encuentra publicada en el repositorio de nuestro portal oficial.
Identificador de la huella digital (Fingerprint): csirt-novigotek_0x91CFF8FC06845F43_public.asc
2.7. Miembros del equipo
La dirección ejecutiva de CSIRT-NOVIGO está a cargo de la gerencia general de ciberseguridad (Alex Martinez). El equipo operativo central está compuesto por analistas de inteligencia de amenazas, ingenieros especialistas en respuesta a incidentes, un gestor de proyectos y personal de soporte comercial.
2.8. Otra información
Para obtener información corporativa detallada, alcance de servicios y validación de credenciales, consulte el sitio web principal de Novigotek.
2.9. Puntos de contacto para clientes
Los clientes corporativos con acuerdos de soporte activo deben utilizar prioritariamente los canales definidos en sus Acuerdos de Nivel de Servicio (SLA) o remitirse a la plataforma de monitoreo designada para una atención escalada automática.
2.10. Horario de operación
Atención ordinaria: Lunes a viernes de 8:00 a.m. a 6:00 p.m. (Horario de oficina en Ecuador).
Atención de emergencias (Severidad Alta y Crítica): Soporte reactivo 24/7, los 365 días del año.

3. CONSTITUCIÓN Y MISIÓN

3.1. Misión
Proporcionar defensa cibernética integral de grado avanzado, tanto proactiva como reactiva, para proteger la infraestructura tecnológica de organizaciones, empresas e instituciones gubernamentales. CSIRT-NOVIGO identifica y mitiga vulnerabilidades aprovechando inteligencia de amenazas estructurada (CTI), asegurando la Confidencialidad,

Integridad y Disponibilidad (tríada CIA) de los activos de información críticos.

3.2. Comunidad servida (Constituency)

Nuestra comunidad protegida incluye infraestructuras críticas nacionales, entidades de gobierno, nuestra cartera de clientes corporativos con sede en Ecuador y Estados Unidos, y organizaciones aliadas de nuestra cadena de suministro tecnológico.

3.3. Patrocinio y afiliación

CSIRT-NOVIGO es un brazo operativo especializado perteneciente a Novigotek, firma enfocada en arquitectura tecnológica, seguridad de la información, y desarrollo de plataformas de gestión de riesgos (GRC).

3.4. Autoridad

El equipo actúa bajo el mandato ejecutivo de la dirección de Novigotek. Para incidentes dentro de la infraestructura propia, CSIRT-NOVIGO posee autoridad absoluta e inmediata para aislar nodos, suspender servicios y ejecutar remediaciones. En operaciones externas, la autoridad de intervención está estrictamente supeditada y limitada a lo establecido en los contratos legales y acuerdos de respuesta a incidentes preestablecidos con cada cliente.

4. POLÍTICAS

4.1. Tipos de incidentes y nivel de soporte

El CSIRT categoriza los incidentes basándose en metodologías estandarizadas (como NIST SP 800-61). La priorización operativa se determina por el impacto técnico y el riesgo de negocio. Incidentes que involucran exfiltración activa de datos, ransomware o denegación de servicio en infraestructuras críticas reciben prioridad máxima incondicional.

4.2. Cooperación, interacción y divulgación de información

CSIRT-NOVIGO reconoce la necesidad crítica de la colaboración sectorial. Compartimos inteligencia estructurada con otros equipos de respuesta a nivel global a través de plataformas federadas (ej. nodos MISP). Toda la información compartida se rige estrictamente por el Traffic Light Protocol (TLP), garantizando que los datos no se difundan más allá de la audiencia autorizada.

4.3. Comunicación y autenticación

La autenticación de emisores en reportes críticos se verifica mediante firmas criptográficas (PGP). CSIRT-NOVIGO se reserva el derecho de no procesar solicitudes ejecutivas o de cambios en infraestructura que provengan de fuentes no autenticadas o anónimas.

4.4. Derechos y obligaciones

Para asegurar el cumplimiento corporativo y gubernamental, nuestras políticas de gestión de incidentes se adhieren a:

- **Nacional:** La Ley Orgánica de Protección de Datos Personales (LOPDP) de la República del Ecuador.
- **Internacional:** El Reglamento General de Protección de Datos (GDPR) de la Unión Europea.

4.5. Retención y manejo de la información

Toda la evidencia digital recopilada (volcados de memoria, logs, capturas de red) se maneja bajo estrictos controles de cadena de custodia. Estos datos se almacenan en repositorios locales fuera de línea (offline) o cifrados, asegurando que solo el personal con autorización explícita pueda acceder a ellos.

5. CATÁLOGO DE SERVICIOS

Categoría de Servicio	Descripción Técnica
Servicios Proactivos	● Monitoreo continuo de inteligencia de amenazas (CTI). ● Evaluación de la superficie de ataque externa (EASM). ● Auditorías de seguridad, pruebas de penetración y escaneo continuo de vulnerabilidades.
Servicios Reactivos	● Despliegue rápido para respuesta a incidentes (identificación, contención y erradicación). ● Análisis forense de sistemas de archivos y memoria. ● Restauración segura y apoyo en la recuperación de la operatividad del negocio.
Gestión de Calidad (GRC)	● Sincronización de inteligencia e indicadores de compromiso (IoC)

Categoría de Servicio	Descripción Técnica
	con la comunidad. ● Actualización y simulacros de los planes de respuesta a incidentes (Playbooks).

6. FORMULARIOS DE REPORTE DE INCIDENTES

Los miembros de nuestra comunidad y actores externos pueden notificar eventos anómalos o incidentes confirmados mediante:

- **Correo Electrónico Directo:** Dirigido a la cuenta oficial de soporte, anexando cabeceras, archivos de bitácora y una descripción cronológica del evento (recomendamos enfáticamente cifrar el cuerpo del correo con nuestra clave PGP).
- **Formulario en Línea:** Utilizando el portal de reporte seguro habilitado en la sección del CSIRT dentro de la página corporativa.

7. DESCARGO DE RESPONSABILIDAD

A pesar de que el equipo invierte el máximo esfuerzo técnico en garantizar la precisión de las advertencias de seguridad, los boletines de vulnerabilidad y las guías de mitigación, CSIRT-NOVIGO no asume ninguna responsabilidad legal o financiera derivada de errores, omisiones o de la aplicación directa de esta información por parte de entidades de terceros. La implementación de contramedidas es responsabilidad de los administradores locales de cada red.