## 1. Objetivo

Disponer de una guía de contactos con las autoridades y grupos de interés especial para que la Escuela Tecnológica Instituto Técnico Central - ETITC tengan identificados los medios apropiados para la gestión de comunicación de un incidente de seguridad de la información que requiera mayor escalamiento.

## 2. Alcance

Esta guía debe ser de conocimiento de todos los funcionarios y contratistas del proceso de Gestión Informática y telecomunicaciones - IT, y demás partes que estén interesadas del Sistema de Gestión de Seguridad de la Información de la ETITC.

## 3. Responsables

• Gestión Informática y telecomunicaciones – IT.
• Gestión de Seguridad de la Información.

## 4. Definiciones de Términos

**Autoridad Competente**: Entidad con facultad para atender, investigar o apoyar incidentes de seguridad de la información.

**COLCERT**: Grupo nacional encargado de coordinar la respuesta a incidentes de ciberseguridad en Colombia.

**Centro Cibernético Policial (CCP)**: Dependencia de la Policía Nacional especializada en delitos informáticos y ciberseguridad.

**CSIRT:** Equipo especializado en la gestión y respuesta ante incidentes de seguridad informática.

**Grupo de Interés Especial**: Entidad externa que puede brindar apoyo técnico, operativo o de coordinación durante la atención de un incidente.

**Incidente de Seguridad de la Información**: Evento que afecta o puede afectar la confidencialidad, integridad o disponibilidad de la información institucional.

**Incidente Crítico**: Incidente de alto impacto que compromete significativamente la operación, los servicios o la información institucional.

**Proveedor Crítico**: Tercero cuya afectación puede impactar la continuidad o seguridad de los servicios institucionales.

**Trazabilidad**: Capacidad de reconstruir y verificar las actividades realizadas durante la gestión de un incidente.

## 5. Generalidades

Esta guía contiene los lineamientos para para establecer el contacto con las autoridades y grupos de interés a los que la ETITC puede escalar en caso de incidente de Seguridad de la información que pueda poner en peligro la confidencialidad, integridad, y disponibilidad de la información.

La decisión de escalar, reportar o establecer contacto con autoridades, organismos de control, CSIRT sectoriales, fuerza pública, entidades regulatorias o terceros externos será evaluada por el Profesional de Seguridad de la Información y validada por la Secretaría General/Jurídica cuando existan implicaciones legales o regulatorias. Para incidentes clasificados como críticos o de alto impacto institucional, la autorización deberá contar adicionalmente con la aprobación de la Alta Dirección.

## 6. Autoridades de la Seguridad de la Información

En el siguiente cuadro se relacionan las autoridades y entidades competentes en caso de que se presentara un incidente de cualquier índole que pusiera en riesgo la confidencialidad, integridad y disponibilidad y de la información y que amerite el llamado a las autoridades.

| Descripción del riesgo materializado | Autoridad / Grupo de interés | Contacto | Teléfono |
|---|---|---|---|
| Investigación de crímenes cibernéticos. Análisis de malware y vulnerabilidades. Respuesta a incidentes cibernéticos. Ciberataques dirigidos a la infraestructura TIC. Acceso abusivo a sistemas informáticos. Hurto por medios informáticos. Suplantación de sitios web. Transferencia no consentida de activos. Ingeniería social. Uso de software malicioso. | **Centro Cibernético Policial (CCP)** | http://www.ccp.gov.co/<br>https://cc-csirt.policia.gov.co/ | +57 312 345 7422 |
| Violación de datos personales. Phishing. Ingeniería social. Ataques de ransomware que afecten la operación. Propagación de noticias falsas. Respuesta a emergencias cibernéticas de Colombia. Atención a incidentes de seguridad informática. | **ColCERT - Grupo de Respuesta a Emergencias Cibernéticas en Colombia** | www.colcert.gov.co | (601) 295 9897<br>(601) 344 2222 |
| Coordinación y atención de incidentes de seguridad informática a nivel nacional. | **CSIRT-CCIT - Centro de Coordinación de Seguridad Informática Colombia** | https://cc-csirt.policia.gov.co | (571) 515 9090<br>(571) 515 9586 |
| Fallas en la infraestructura de las TIC. Ciberataques que comprometan la seguridad de la información y la privacidad de los datos. | **Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)** | minticresponde@mintic.gov.co<br>https://www.mintic.gov.co/portal/inicio/ | (601) 344 3460<br>(601) 692 8999 |
| Emergencia por incendio. | **Bomberos** | Línea de emergencias | 119 |
| Robo o hurto de equipos tecnológicos. | **Policía Nacional** | Línea de emergencias | 112 |
| Siniestros ambientales o desastres. | **Defensa Civil** | Línea de emergencias | 144 |

## 7. Comunicación

Cuando se presente un incidente que ponga en riesgo la confidencialidad, integridad y disponibilidad y de la información, debe ser informado al Oficial de seguridad, quien analizará y coordinará las acciones a seguir e informará al Jefe de la Oficina de las Tecnologías de la Información y las Comunicaciones de la Corporación, quien será el encargado de realizar el llamado a las autoridades correspondientes. En caso de que el Jefe de la Oficina de las Tecnologías de la Información y las Comunicaciones de la Corporación no esté disponible el llamado a las Autoridades lo podrá hacer directamente el Oficial de Seguridad de la Información.

## 8. Grupos de Interés Especial

Se debe mantener contacto permanente con los grupos de investigación, entidades del gobierno, proveedores de tecnología y autoridades que trabajan para mantener informadas y actualizadas a las instituciones y al personal encargado sobre las amenazas, incidentes y soluciones que a diario se presentan.

| Tipo de Incidente | Grupo de Interés | Correo Electrónico / Sitio Web | Teléfono |
|---|---|---|---|
| Infraestructura crítica nacional | **Comando Conjunto Cibernético (CCOC)** | contacto@ccoc.mil.co | +57(1) 221 6336 |
| Incidentes de ciberseguridad de alto impacto | **Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)** | minticresponde@mintic.gov.co<br>https://www.mintic.gov.co/portal/inicio/ | (601) 344 3460<br>(601) 692 8999 |
| Coordinación y análisis de incidentes | **CSIRT-CCIT - Centro de Coordinación de Seguridad Informática Colombia** | csirt@ccit.org.co<br>https://cc-csirt.policia.gov.co | (571) 515 9090<br>(571) 515 9586<br>(601) 620 7799 |

| Tipo de Incidente | Grupo de Interés | Correo Electrónico / Sitio Web | Teléfono |
|---|---|---|---|
| Incidentes de ciberseguridad de alto impacto | **ColCERT - Grupo de Respuesta a Emergencias Cibernéticas en Colombia** | contacto@colcert.gov.co | (601) 295 9897<br>(601) 344 2222 |
| Delitos informáticos, fraude, phishing, ransomware | **Centro Cibernético Policial (CCP)** | https://www.ccp.gov.co/ | (601) 515 9711 |
| Cooperación internacional (cuando aplique) | **FIRST (Forum of Incident Response and Security Teams)** | first-sec@first.org | No registra |

## 9. Control de Cambios

| FECHA | VERSIÓN | CAMBIOS |
|---|---|---|
| 2026-09-21 | 1 | Creación del documento para formalizar el proceso de contacto con autoridades y grupos de interés, definiendo responsables, criterios de escalamiento y mecanismos de comunicación ante incidentes de seguridad de la información, en cumplimiento de los lineamientos del SGSI y los requisitos de ISO/IEC 27001:2022. |

| ELABORÓ | REVISÓ | APROBÓ |
|---|---|---|
| **LUIS JAVIER TOVAR TURCIO**<br>Líder del Sistema de Gestión de Seguridad de la Información | **YAZMIN ANTONIA SANTIAGO CABRERA**<br>Profesional Sistema de Gestión de Calidad | **YANETH JIMENA PIMIENTO CORTÉS**<br>Líder de Gestión del Sistema Integrado de Aseguramiento |