



INSTITUCIÓN EDUCATIVA TÉCNICO INDUSTRIAL - TIBASOSA

Aprobado mediante Resolución 080 del 22 de Enero de 2009.

DANE: 215806000236 - NIT: 800.095.074-4

PROTOCOLO INTEGRAL DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD DIGITAL Y CIBERSEGURIDAD – 2026

1. Clasificación del Incidente (Gravedad y Criticidad)

Ante la sospecha o detección de una anomalía en el ecosistema digital escolar, el Comité de Gestión TIC de la institución clasificará el evento en una de las siguientes tres categorías para determinar la velocidad, prioridad y el alcance de la respuesta inmediata:

- **Nivel 1: Crítico (Ciberseguridad - Alta Complejidad):** Ataques de denegación de servicio (DDoS) que derriben el portal web oficial tecnicotibasosa.edu.co; alteración visual maliciosa de la página web (*Defacement*); secuestro de datos con cifrado de archivos (*Ransomware*) en los servidores de las salas de informática o portátiles rurales; o hackeo de la base de datos de calificaciones en el software **Compucol** con alteración de registros o filtración de datos de menores de edad.
- **Nivel 2: Medio (Seguridad Digital - Identidad y Redes):** Suplantación o hackeo del Perfil Oficial de Facebook de la institución; creación de perfiles falsos a nombre del colegio orientados a estafas o difamación; o acoso virtual sistemático (*Cyberbullying*) en grupos de WhatsApp escolares vinculantes.
- **Nivel 3: Bajo (Operativo / Soporte):** Pérdida u olvido de credenciales de acceso por parte de usuarios en la plataforma Compucol; infecciones aisladas por virus o troyanos en estaciones de trabajo locales controladas eficientemente por el antivirus institucional; o caídas temporales del proveedor del servicio de internet.

2. Ruta Técnica de Contención y Respuesta (Paso a Paso)

Frente a incidentes de **Nivel 1 (Crítico)** o **Nivel 2 (Medio)**, el administrador del sistema y el equipo técnico del Comité Tic ejecutarán de inmediato el siguiente flujograma técnico:

[1. Aislamiento y Contención] → [2. Preservación de Evidencias] → [3. Erradicación del Ataque] → [4. Ruta Legal y Denuncia] → [5. Restauración]



INSTITUCIÓN EDUCATIVA TÉCNICO INDUSTRIAL - TIBASOSA

Aprobado mediante Resolución 080 del 22 de Enero de 2009.

DANE: 215806000236 - NIT: 800.095.074-4

✓ Paso 1: Aislamiento y Contención Técnica Inmediata

El objetivo primordial es frenar el ataque o detener la fuga de información en tiempo real antes de que se propague a otras plataformas o sedes.

- **Para el Portal Web o Plataforma Compucol:** El Rector o el Administrador TIC se comunicará inmediatamente con la mesa de soporte del *hosting* contratado o con el equipo de ingenieros de Compucol para ordenar el bloqueo preventivo temporal de accesos administrativos y suspender el servicio web mientras se realiza la auditoría de cuentas.
- **Para Ataques en Red Local o Servidores (Ransomware):** Se procederá a la desconexión física inmediata (retiro de cables de red LAN y apagado de routers Wi-Fi) de todos los computadores de la sala de informática afectada y de los portátiles en las sedes rurales para evitar el contagio masivo. Nota de seguridad: No se deben apagar los servidores afectados de forma brusca (desconexión de energía), para no destruir los datos volátiles de la memoria RAM, los cuales son útiles para el análisis forense digital.

✓ Paso 2: Preservación de Evidencias Digitales (Cadena de Custodia)

Antes de limpiar, formatear o restaurar cualquier sistema, se deben asegurar las pruebas tecnológicas que sustenten las futuras acciones legales:

- **Capturas de Pantalla:** Tomar capturas de pantalla (*screenshots*) completas donde se evidencie claramente la fecha y hora del sistema, las URLs alteradas y los mensajes o imágenes falsas publicadas en Facebook o la web oficial.
- **Exportación de registros:** Extraer y exportar los registros o *logs* de auditoría (historial de conexiones e inicios de sesión) de los servidores web y de la plataforma Compucol para identificar las direcciones IP de origen, horas del ataque y usuarios comprometidos.

✓ Paso 3: Erradicación y Mitigación del Riesgo

- **Desinfección:** Ejecutar análisis profundos y rigurosos con el antivirus licenciado de la institución en todos los terminales y nodos afectados.
- **Actualización de Credenciales:** Forzar un cambio masivo y obligatorio de contraseñas de todas las cuentas directivas, docentes y administrativas del colegio. Las nuevas claves deberán cumplir con estándares de alta seguridad



INSTITUCIÓN EDUCATIVA TÉCNICO INDUSTRIAL - TIBASOSA

Aprobado mediante Resolución 080 del 22 de Enero de 2009.

DANE: 215806000236 - NIT: 800.095.074-4

(mínimo 12 caracteres, combinando letras mayúsculas, minúsculas, números y caracteres especiales como *, #, \$, @).

- **Eliminación de Sesiones:** Cancelar y revocar todos los tokens de acceso activos en las configuraciones de seguridad del Perfil Oficial de Facebook y correos electrónicos de dominio institucional @sedboyaca.gov.co.

✓ **Paso 4. Ruta de Reporte Legal y Denuncia Pública (Leyes 1273 y 1581)**

Una vez contenido el ataque en su parte técnica, el Rector, en representación legal de la entidad pública, activará las siguientes acciones jurídicas obligatorias:

- Denuncia por Delitos Informáticos (Ley 1273 de 2009): Radicar formalmente la denuncia penal por el delito aplicable (Acceso abusivo a sistema informático, daño informático, violación de datos personales o suplantación de sitios web). Esta se tramitará de forma virtual a través del CAI Virtual de la Policía Nacional (caivirtual.policia.gov.co) o ante la Fiscalía General de la Nación, adjuntando las evidencias recolectadas en el Paso 2.
- Reporte de Brecha de Seguridad ante la SIC (Habeas Data): Si el ataque comprometió datos personales, historias académicas, observadores o números de documento de los estudiantes, el Rector notificará el "Incidente de Seguridad" ante la Superintendencia de Industria y Comercio (SIC), dentro de los quince (15) días hábiles siguientes a su detección, en cumplimiento de la Ley 1581 de 2012.
- Comunicado Informativo a la Comunidad Educativa: Con el fin de mitigar estafas o desinformación, la institución emitirá un boletín oficial firmado por las directivas. Se publicará en el portal web (una vez restablecido de forma segura) y de manera paralela se notificará a los acudientes a través del canal unidireccional de alertas de WhatsApp, aclarando la contingencia y recordando que la institución **nunca** solicita dinero, claves ni datos confidenciales por medios informales.

✓ **Paso 5: Restauración del Sistema y Auditoría Post-Incidente**

- Carga de Copias de Seguridad (Backups): El Administrador TIC procederá a restaurar el sitio web o los sistemas afectados utilizando la última copia de seguridad limpia, validada y almacenada de forma aislada (fuera de línea) de manera previa al ataque.



INSTITUCIÓN EDUCATIVA TÉCNICO INDUSTRIAL - TIBASOSA

Aprobado mediante Resolución 080 del 22 de Enero de 2009.

DANE: 215806000236 - NIT: 800.095.074-4

- Lecciones Aprendidas: El Comité TIC elaborará un informe técnico final que detalle la vulnerabilidad explotada por los atacantes (por ejemplo: *Phishing* a un docente, contraseña débil o falta de parches de seguridad). Con base en este, se redefinirán las metas del Plan de Mejoramiento Institucional (PMI) para la adquisición de herramientas de protección (*Firewalls*) o la programación de capacitaciones obligatorias en ciberseguridad.

Registro Oficial de Incidentes Tecnológicos (Formato de Bitácora PEI)

Toda alerta digital que obligue a la ejecución de este protocolo deberá quedar registrada en la siguiente matriz para control de las auditorías de calidad y visitas de inspección de la Secretaría de Educación de Boyacá:

Ejemplo:

Fecha: _____

Hora de detección: _____

Sala de Informática / Sede: _____

ID Incidente	Canal Afectado (Web / Facebook / Compucol)	Nivel de Riesgo (1/2/3)	Acciones Técnicas Ejecutadas	Nº Radicado de Denuncia (CAI / SIC)	Fecha de Cierre del Evento
INC-2026-01	Perfil Oficial de Facebook	Nivel 2	Contención de accesos, cambio de clave y reporte a Meta.	N/A (Soporte Meta)	06/07/2026 04:30 pm

Docente: (Nombre)

Administrador TIC

Atentamente

Mg. JORGE ELIECER SIERRA ÁLVAREZ

Rector

Proyecto: DIANA MALAVER - Aux. Administrativo

Tibasosa - Vereda Peña Negra – Sector Santa Teresa

E-mail: tibasosatecnico@sedboyaca.gov.co - Celular 3138157676