Protocolos de Defensa contra Accesos No Autorizados
Colegio de Estudios Científicos y Tecnológicos del Estado de Coahuila
(CECyTE Coahuila)

1. Objetivo

Definir procedimientos y controles para prevenir, detectar y responder a accesos no autorizados en los sistemas informáticos y de comunicaciones del CECyTE Coahuila, garantizando la seguridad de la información institucional.

2. Alcance

Este documento aplica a todos los sistemas, redes, aplicaciones y equipos de cómputo del CECyTE Coahuila, así como al personal administrativo, docente, estudiantes y terceros que hagan uso de ellos.

3. Principios

- **Prevención:** Implementar medidas que reduzcan la probabilidad de accesos indebidos.
- **Detección:** Identificar oportunamente intentos de intrusión o actividades sospechosas.
- **Respuesta:** Actuar de manera inmediata para contener y mitigar incidentes.
- **Registro:** Documentar todos los eventos de seguridad para análisis y mejora continua.

4. Protocolos de Defensa

4.1 Control de Accesos

- Uso obligatorio de credenciales únicas e intransferibles.
- Implementación de autenticación multifactor (MFA) en sistemas críticos.
- Bloqueo automático de cuentas tras **5 intentos fallidos de acceso**.
- Revisión periódica de permisos de usuario para evitar privilegios innecesarios.

4.2 Monitoreo y Detección

- Implementación de sistemas de **detección y prevención de intrusos (IDS/IPS)**.
- Monitoreo constante del tráfico de red y registros de acceso.
- Alertas automáticas ante intentos de acceso sospechosos o fuera de horario laboral.

4.3 Protección de Infraestructura

- Configuración de **firewalls** para filtrar tráfico no autorizado.
- Segmentación de redes para aislar sistemas críticos.
- Actualización periódica de sistemas operativos y aplicaciones con parches de seguridad.

4.4 Respuesta ante Incidentes

- **Detección:** Identificación del intento de acceso no autorizado.
- **Notificación:** Reporte inmediato al área de TI.
- **Contención:** Bloqueo de la cuenta o dispositivo comprometido.
- **Erradicación:** Eliminación de malware o cierre de vulnerabilidades explotadas.
- **Recuperación:** Restauración de sistemas y datos respaldados.
- **Documentación:** Registro del incidente en bitácora oficial.

4.5 Concientización de Usuarios

- Capacitación anual en seguridad informática.
- Difusión de buenas prácticas de uso de contraseñas y sistemas.
- Campañas de sensibilización sobre riesgos de accesos indebidos.

5. Responsabilidades

- **Dirección General:** Aprobar y supervisar la aplicación de estos protocolos.
- **Área de TI:** Implementar controles técnicos, monitorear accesos y coordinar respuesta a incidentes.
- **Usuarios:** Cumplir con las normas establecidas y reportar cualquier actividad sospechosa.

6. Vigencia

Este documento entra en vigor el **04 de febrero de 2026** y será revisado anualmente o cuando existan cambios relevantes en la infraestructura tecnológica o normativa aplicable.

Última actualización: 04 de febrero de 2026