Claustro Gómez
Instituto Superior Tecnológico
El Instituto de la Gente Bonita

Políticas Institucionales de Seguridad y Privacidad del Instituto Superior Tecnológico del Claustro Gómez

1. **Política de Acceso y Autenticación:**
   - Todo usuario deberá contar con credenciales únicas y seguras para acceder a las plataformas virtuales UDEKI y Claustro Learning.
2. **Política de Protección de Datos:**
   - Todos los datos personales y académicos almacenados en las plataformas serán tratados bajo estrictas medidas de confidencialidad y cifrado avanzado.
   - La institución garantizará la privacidad y protección de los datos personales según las normativas vigentes nacionales e internacionales.
3. **Política de Gestión de Copias de Seguridad:**
   - Se realizarán copias de seguridad periódicas y automáticas de toda información académica relevante, almacenándose en lugares seguros externos.
   - La recuperación de datos se efectuará de manera rápida y efectiva ante cualquier incidente, asegurando la continuidad académica y administrativa.
4. **Política de Auditoría y Control Interno:**
   - Se implementarán auditorías regulares para evaluar la efectividad de los protocolos de seguridad informática, detectando y corrigiendo posibles vulnerabilidades.
   - Cualquier vulnerabilidad detectada será solucionada inmediatamente mediante la aplicación de parches y actualizaciones correspondientes.
5. **Política de Capacitación y Concienciación:**
   - Se desarrollarán programas constantes de formación y actualización en seguridad informática para todo el personal administrativo, técnico y docente.

- Se realizarán campañas periódicas para sensibilizar a los estudiantes sobre prácticas seguras en el uso de la tecnología y gestión de información personal.

6. **Política de Monitoreo y Prevención:**
   - Se implementará un sistema integral de monitoreo en tiempo real para identificar actividades sospechosas o intentos no autorizados de acceso.
   - Se establecerán protocolos claros para responder oportunamente ante incidentes o alertas de seguridad.
7. **Política de Cumplimiento Normativo:**
   - La institución cumplirá estrictamente con las normativas y leyes vigentes sobre protección de datos personales y privacidad.
   - Se fomentará una cultura institucional basada en la transparencia, responsabilidad y respeto por la privacidad de todos los usuarios.

Protocolo Institucional de Seguridad Informática del Instituto Superior Tecnológico del Claustro Gómez

Objetivo: Establecer procedimientos claros y efectivos para garantizar la seguridad de la información académica y administrativa en las plataformas virtuales UDEKI y Claustro Learning, previniendo y mitigando riesgos relacionados con accesos no autorizados, pérdidas o vulneraciones de datos.

Alcance: Este protocolo aplica a estudiantes, docentes, personal administrativo y técnico del Instituto Superior Tecnológico del Claustro Gómez, y es aplicable para todas las actividades que involucren acceso, uso, almacenamiento y transmisión de información institucional.

Procedimientos:

1. **Acceso y Autenticación:**
    - Los usuarios recibirán credenciales personales e intransferibles para acceder a las plataformas.
    - La institución proveerá mecanismos de autenticación multifactor (MFA) obligatorios para personal administrativo o usuarios con acceso a información sensible.
    - Se deberá cambiar periódicamente las contraseñas y seguir criterios de complejidad y seguridad establecidos por la institución.
2. **Gestión de Datos:**
    - Todo manejo de información sensible y datos personales debe realizarse bajo estrictas medidas de confidencialidad.
    - Los datos almacenados y en tránsito deben estar siempre cifrados mediante protocolos avanzados SSL/TLS.
3. **Copias de Seguridad y Recuperación:**
    - Se realizarán copias de seguridad automáticas con una periodicidad semanal, almacenándose en ubicaciones externas seguras.

- El personal técnico encargado realizará simulacros periódicos de recuperación de datos para validar la eficacia del procedimiento de restauración ante incidentes.

4. **Auditorías y Evaluaciones:**
   - Semestralmente se llevarán a cabo auditorías internas y anualmente auditorías externas para evaluar la seguridad informática.
   - Se documentarán todas las vulnerabilidades detectadas, aplicando inmediatamente las soluciones necesarias.
5. **Capacitación Continua y Concienciación:**
   - Se programarán sesiones trimestrales de capacitación en seguridad informática para todo el personal institucional.
   - Se desarrollarán campañas de concienciación dirigidas a estudiantes, docentes y personal administrativo sobre la importancia de mantener la seguridad de la información.
6. **Monitoreo y Detección Temprana:**
   - La institución utilizará herramientas tecnológicas avanzadas para monitorear constantemente el acceso y uso de los sistemas, identificando patrones anómalos y amenazas potenciales.
   - Frente a incidentes de seguridad detectados, se activará inmediatamente el protocolo de respuesta, notificando a los responsables y tomando acciones correctivas inmediatas.
7. **Respuesta ante Incidentes:**
   - Ante la detección de incidentes de seguridad, el responsable técnico activará el procedimiento de contención y mitigación, documentando el evento y notificando oportunamente a las autoridades competentes.
   - Se comunicará de manera transparente y oportuna a los usuarios afectados por incidentes relacionados con sus datos personales.
8. **Cumplimiento Normativo:**
   - La institución revisará regularmente el cumplimiento de normativas y leyes vigentes sobre protección de datos, realizando actualizaciones necesarias para asegurar su plena adherencia.
   - Se mantendrán registros documentales que permitan evidenciar el cumplimiento de las políticas y procedimientos establecidos.