UNIVERSIDAD TÉCNICA DE AMBATO
Facultad de Ingeniería en Sistemas, Electrónica e Industrial
Febrero 2025 – Julio 2025

Título: **Seguridad y Etica**
Estudiantes participantes: Pazmiño Bryan
Asignatura: Realidad Nacional **Nivel y Paralelo:** **6to "A"**
Docente: Ing.Angel Carranza, mg. **Fecha:** 20/04/2025

1. **Plantear 10 valores fundamentales con su definición que deberá mantener un Ingeniero en Software**

1. Ética Profesional
Actuar con integridad, responsabilidad y respeto por los derechos humanos en todas las decisiones técnicas, evitando daños a usuarios o sociedad.

2. Privacidad y Confidencialidad
Proteger los datos sensibles de los usuarios mediante prácticas seguras y cumplir con normativas de protección de información.

3. Transparencia
Comunicar claramente cómo funcionan los sistemas, incluyendo limitaciones y riesgos, para generar confianza en los usuarios.

4. Calidad y Precisión
Garantizar que los sistemas sean robustos, funcionales y libres de errores críticos mediante pruebas rigurosas.

5. Equidad e Inclusión
Diseñar soluciones que eviten sesgos y sean accesibles para personas de diversas culturas, géneros o capacidades.

6. Responsabilidad Social
Evaluar el impacto social y ambiental de las tecnologías, priorizando el bien común sobre intereses comerciales.

7. Innovación Sostenible
Desarrollar soluciones eficientes y escalables que minimicen el consumo de recursos y maximicen su vida útil.

8. Colaboración
Trabajar en equipo, integrando perspectivas multidisciplinarias para resolver problemas complejos.

9. Aprendizaje Continuo
Mantenerse actualizado en avances tecnológicos y éticos para adaptarse a nuevos desafíos.

10. Cumplimiento Legal

Respetar leyes y regulaciones locales e internacionales relacionadas con tecnología, privacidad y derechos digitales.

2. Caso de Estudio: Seguridad y Ética en una Aplicación de Reconocimiento Facial.

Contexto:

Una empresa de tecnología está desarrollando una aplicación de reconocimiento facial para la seguridad de edificios corporativos. La app permitirá a los empleados acceder a sus oficinas sin necesidad de tarjetas o claves, simplemente escaneando su rostro.

Sin embargo, surgen preocupaciones sobre la privacidad de los datos, la precisión del algoritmo y posibles sesgos en el sistema. Además, han ocurrido casos en los que el sistema no reconoce correctamente a personas con ciertos tonos de piel o características faciales.

Resolver

1. Privacidad y Seguridad de los Datos:

¿Cómo garantizar que las imágenes faciales sean almacenadas de manera segura?

Para proteger imágenes faciales, se debe aplicar una estrategia de seguridad en múltiples capas:

- **Cifrado Robusto:** Usar AES-256 tanto en tránsito como en reposo para impedir accesos no autorizados. El cifrado biométrico puede añadir una capa extra de protección al vincular claves con datos biométricos del usuario.

- **Almacenamiento Seguro:** Optar por almacenamiento local en el dispositivo para mayor privacidad o por arquitecturas distribuidas que fragmenten y cifren los datos para mayor resiliencia.

- **Gestión de Claves:** Implementar controles de acceso basados en roles, rotación periódica de claves y usar HSM (Hardware Security Modules) para almacenar claves de forma segura.

- **Anonimización:** Cuando la identificación no sea esencial, aplicar técnicas como pixelación o generación de datos sintéticos para preservar la privacidad.

- **Enfoque Integral:** No depender de una sola medida. Combinar cifrado, control de acceso, almacenamiento adecuado y anonimización según el contexto y sensibilidad de los datos.

¿Qué medidas deben tomarse para evitar el uso indebido o filtraciones de los datos?

Para prevenir el uso indebido o filtraciones de datos faciales, se deben aplicar medidas técnicas, organizacionales y humanas:

- **Control de Acceso:** Usar control de acceso basado en roles (RBAC), autenticación multifactor (MFA) y aplicar el principio de privilegio mínimo para restringir el acceso solo al personal autorizado.

- **Auditorías y Monitorización:** Realizar auditorías de seguridad, pruebas de penetración y monitoreo continuo con sistemas de detección de intrusos para detectar vulnerabilidades y actividades sospechosas.

- **Minimización de Datos:** Recopilar solo los datos necesarios y definir políticas claras de retención y eliminación para reducir el riesgo de filtraciones.

- **Capacitación del Personal:** Formar a los empleados en buenas prácticas de seguridad y manejo de datos biométricos para evitar errores humanos.

- **Prevención de Pérdida de Datos (DLP):** Usar herramientas de DLP para bloquear transferencias no autorizadas de información sensible.

- **Consentimiento y Transparencia:** Informar y obtener el consentimiento explícito de los usuarios, asegurando prácticas claras y transparentes de manejo de datos.

- **Enfoque Integral:** La combinación de tecnología, políticas y cultura organizacional es clave para una defensa efectiva contra amenazas internas y externas.

2. Ética y Sesgo en el Algoritmo:

¿Cómo detectar y mitigar el sesgo en los modelos de inteligencia artificial?

Para detectar y reducir el sesgo en modelos de reconocimiento facial se deben aplicar acciones en todas las etapas del desarrollo:

- **Datos Diversos:** Utilizar conjuntos de datos inclusivos y representativos (tonos de piel, géneros, edades, rasgos faciales) para evitar sesgos desde el entrenamiento.

- **Métricas de Equidad:** Evaluar el modelo con métricas como la paridad demográfica y probabilidades igualadas para detectar disparidades en grupos demográficos.

- **Ajustes Algorítmicos:** Aplicar técnicas como reponderación de datos, ajuste de umbrales o algoritmos sensibles a la equidad para corregir el sesgo durante el aprendizaje.

- **Evaluación y Monitoreo Continuo:** Probar regularmente el modelo con datos variados y supervisar su comportamiento en uso real para detectar sesgos emergentes.

- **Supervisión Humana:** Incluir revisión humana en decisiones críticas para identificar sesgos que los sistemas automatizados podrían pasar por alto.

- **Enfoque Integral:** Mitigar el sesgo requiere una estrategia completa desde la recolección de datos hasta la implementación, combinando técnicas técnicas con vigilancia activa.

¿Qué estrategias pueden implementarse para asegurar la equidad en el reconocimiento facial?

Para garantizar que el reconocimiento facial funcione de forma justa para todos los grupos demográficos, se recomienda:

- **Pruebas Rigurosas:** Evaluar el sistema en distintos grupos y condiciones (iluminación, ángulos, etc.) para detectar disparidades en el rendimiento.

- **Ajustes de Umbral:** Adaptar los niveles de confianza del reconocimiento por grupo, con cuidado de no comprometer la seguridad ni la precisión global.

- **Transparencia y Explicabilidad:** Informar a los usuarios sobre las limitaciones del sistema y usar técnicas de IA explicable (XAI) para entender las decisiones del modelo.

- **Retroalimentación del Usuario:** Permitir que las personas reporten errores o sesgos para mejorar continuamente el sistema.

- **Diversidad de Características:** Asegurar que el modelo no dependa solo de rasgos dominantes en ciertos grupos, promoviendo una base más inclusiva.

- **Compromiso con la Equidad:** Lograr justicia en el reconocimiento facial requiere acciones técnicas, políticas inclusivas y una experiencia de usuario justa para todos.

3. Alternativas Tecnológicas y de Implementación:

¿Existen métodos alternativos para mejorar la seguridad sin comprometer la privacidad?

Sí, existen varias alternativas al reconocimiento facial que refuerzan la seguridad sin invadir la privacidad:

- **Autenticación Multifactor (MFA):** Combinar biometría (como huellas o iris) con factores adicionales (PIN, tarjetas, apps) para mejorar la seguridad sin depender solo del rostro.

- **Tarjetas de Proximidad o Llaveros:** Son opciones menos intrusivas que pueden reforzarse con códigos PIN, siendo prácticas y respetuosas con la privacidad.

- **Biometría del Comportamiento:** Analiza patrones únicos (como escritura o forma de andar) para una autenticación continua y menos invasiva.

- **Tokens o Contraseñas de Un Solo Uso (OTP):** Proveen seguridad sólida sin necesidad de datos biométricos, usando dispositivos del usuario para generar códigos.

- **Enfoque por Capas:** Combinar varios métodos reduce los riesgos de privacidad y ofrece más flexibilidad y control al usuario.

¿Cómo podrían integrar múltiples factores de autenticación sin afectar la usabilidad?

Para que la seguridad no se vuelva una barrera, es clave diseñar un sistema de autenticación que sea fuerte pero también fácil de usar:

- **Interfaz Intuitiva:** Crear un diseño claro que guíe al usuario durante la autenticación sin complicaciones, incluso cuando hay múltiples factores.

- **Autenticación Contextual:** Ajustar el nivel de autenticación según el riesgo: menos exigente para accesos comunes y más riguroso para zonas críticas.

- **Autenticación Escalada:** Pedir factores extra solo cuando sea estrictamente necesario (por ejemplo, al acceder a datos confidenciales).

- **Flexibilidad para el Usuario:** Permitir que cada usuario elija los métodos de autenticación que prefiera, facilitando la adopción.

- **Inicio de Sesión Único (SSO):** Usar SSO para evitar múltiples inicios de sesión, haciendo el acceso más fluido sin perder seguridad.

- **Insight:** El éxito de la autenticación multifactor (MFA) depende de su capacidad para ser segura sin interrumpir demasiado al usuario. El enfoque debe ser inteligente, adaptativo y centrado en la experiencia.

4. Cumplimiento Legal y Normativo:

¿Qué regulaciones sobre protección de datos deben considerarse al implementar esta tecnología?

- **Reglamento General de Protección de Datos (RGPD)**

Aplica en la Unión Europea y es una referencia global.
Exige consentimiento explícito para procesar datos biométricos (como rostros).
Impone principios como minimización de datos, limitación de la finalidad, y transparencia.

- **Leyes Locales en Ecuador (Ambato, Tungurahua)**

Es vital revisar la Ley Orgánica de Protección de Datos Personales de Ecuador, en vigencia desde 2021.
Esta ley regula el tratamiento de datos personales, incluidos los biométricos, y exige bases legales claras, medidas de seguridad, y derechos de los titulares como el acceso, rectificación y oposición.

Ejemplos de Regulaciones Internacionales

BIPA (Illinois, EE. UU.): Una de las leyes más estrictas sobre privacidad biométrica. Requiere consentimiento informado por escrito, avisos sobre uso y limitaciones en la retención de datos.
China: Tiene regulaciones específicas para tecnologías de reconocimiento facial, enfocadas en el consentimiento informado, uso limitado y supervisión estatal.

- **Insight**

El cumplimiento legal no es opcional: ignorarlo puede resultar en sanciones severas y pérdida de confianza pública.
El procesamiento de datos biométricos requiere un enfoque ético, legal y transparente desde la fase de diseño del sistema.

¿Cómo se podría garantizar que la aplicación cumpla con normas como GDPR o leyes locales de privacidad?

1. **Evaluación de Impacto en la Protección de Datos (EIPD)**
   - Realizar una EIPD exhaustiva antes de implementar el sistema para identificar y mitigar riesgos de privacidad.

- La EIPD proporciona una evaluación de riesgos que ayuda a implementar medidas de protección adecuadas desde el principio.

2. Base Legal para el Procesamiento de Datos

- Consentimiento explícito: Obtener el consentimiento explícito y libre de los usuarios para el procesamiento de datos biométricos, lo cual es esencial según el GDPR.

- El consentimiento debe ser específico, informado e inequívoco.

3. Transparencia e Información

- Proporcionar información clara sobre la recopilación, almacenamiento y uso de los datos faciales.

- Asegurar que las personas sean informadas sobre cómo se procesan sus datos, lo que se conoce como el derecho a la información.

4. Derechos del Interesado

- Implementar procedimientos que faciliten el ejercicio de los derechos de los interesados, como el derecho a acceder, rectificar, borrar y restringir el procesamiento de sus datos personales.

5. Medidas de Seguridad

- Implementar medidas de seguridad adecuadas (técnicas y organizativas) para garantizar la protección de los datos personales, tal como exige el Artículo 32 del GDPR.

- Asegurar que los datos se mantengan seguros durante todo su ciclo de vida.

6. Privacidad desde el Diseño y por Defecto

- Adoptar un enfoque de privacidad desde el diseño y por defecto, integrando consideraciones de privacidad en todas las etapas de desarrollo.

- Asegurar que se procesen solo los datos estrictamente necesarios.

7. Documentación de Políticas

- Desarrollar políticas y procedimientos claros para la recopilación, procesamiento y protección de datos biométricos.

- Mantener estas políticas actualizadas y accesibles para asegurar la transparencia y el cumplimiento.

8. Delegado de Protección de Datos (DPD)

- Designar un DPD si las leyes lo exigen, para supervisar y garantizar el cumplimiento continuo de la normativa de protección de datos.

- El DPD puede proporcionar orientación y liderar las actividades de cumplimiento.

9. Auditorías y Revisiones Periódicas

- Realizar auditorías y revisiones periódicas del sistema y de las políticas de protección de datos.

- Las revisiones periódicas aseguran que se cumplan las normativas y se adapten a cualquier cambio legislativo.

Insight

El cumplimiento con las regulaciones de protección de datos no es un proceso estático, sino proactivo y continuo. Una EIPD detallada, junto con un enfoque sólido de transparencia, consentimiento válido y medidas de seguridad, forman la base para un sistema que proteja tanto la privacidad de los usuarios como los datos sensibles. Además, garantizar la privacidad desde el diseño y contar con un Delegado de Protección de Datos facilitará la implementación y el mantenimiento de prácticas de privacidad robustas.

3. Conclusión

La implementación de tecnologías como el reconocimiento facial en seguridad corporativa requiere un enfoque balanceado entre seguridad, conveniencia y preocupaciones éticas. Es crucial que los ingenieros de software comprendan y respeten principios éticos, abordando riesgos de privacidad y sesgo en los algoritmos. Para garantizar la seguridad, se deben aplicar cifrado robusto, almacenamiento seguro, control de acceso y auditorías periódicas, mientras se minimiza la recopilación de datos. La autenticación multifactor y alternativas tecnológicas, como el uso de modalidades biométricas diversas, pueden mejorar la seguridad sin comprometer la privacidad. Además, el cumplimiento con regulaciones como el RGPD exige medidas como la evaluación de impacto de datos, transparencia, y protección adecuada de la información. En última instancia, los ingenieros deben integrar consideraciones éticas y legales en el desarrollo de estas tecnologías, priorizando la equidad y la privacidad.