# EXAME DE PROFICIÊNCIA EM LÍNGUA ESPANHOLA

Cole aqui o Código Identificador

## Orientações:

1. **No ato da realização da prova, o candidato deverá apresentar à banca examinadora documento oficial de identificação com foto.**

2. **A prova deve ser respondida em língua portuguesa e com caneta esferográfica de tinta azul ou preta.**

3. **A única identificação na prova deverá ser o código identificador presente na capa deste caderno, o qual deverá ser copiado em todas as páginas subsequentes. Também é necessário que o candidato tome nota do referido código para fins de consulta de seu desempenho, quando da divulgação dos resultados.**

4. **Será considerada anulada a avaliação do candidato que utilizar outros meios de identificação (assinatura, rubrica, carimbo etc.).**

5. **Somente serão consideradas válidas as respostas presentes nas folhas timbradas que respeitarem os limites de espaço especificados.**

6. **É permitido o uso do dicionário durante a realização da prova. Não é permitida, porém, a utilização de qualquer outro material de consulta, bem como de aparelhos eletrônicos (tradutores, calculadoras, celulares, etc.). Também não é permitido o empréstimo de nenhum tipo de material após o início da prova.**

7. **A prova terá duração máxima de 3 (três) horas, com início às 14 horas e término às 17 horas.**

8. **A presente prova de proficiência procura aferir o desempenho de leitura instrumental em Língua Espanhola, não tendo como objetivo testar conhecimentos específicos na área de Letras.**

---

**TEXTO I**

---

# USO ÉTICO DEL RECONOCIMIENTO FACIAL: BALANCE ENTRE TECNOLOGÍA Y PRIVACIDAD

## Garantizar el uso ético de la tecnología de reconocimiento facial

Con unos 700 millones de cámaras de vídeo en funcionamiento en todo el mundo, la privacidad y las consideraciones éticas son primordiales en el uso de la tecnología de reconocimiento facial. A continuación, se exponen algunas consideraciones para garantizar su aplicación conforme a los requisitos.

Los sistemas de reconocimiento facial éticos deben dar prioridad al consentimiento del usuario y a la privacidad. Los datos no deben recopilarse ni compartirse sin permiso explícito, y las listas de vigilancia deben ser creadas por el usuario sin utilizar fuentes de terceros como las redes sociales. El cifrado de datos y el almacenamiento de vectores matemáticos en lugar de imágenes son esenciales para un tratamiento seguro de los datos. Las organizaciones también deben notificar claramente a las personas cuyas imágenes se analizan y obtener su consentimiento, garantizando el cumplimiento de normativas como el RPGD y otras leyes locales.

Abordar el sesgo es crucial para mejorar la precisión de la tecnología de reconocimiento facial. La utilización de conjuntos de datos diversos y amplios que incluyan diversos datos demográficos puede reducir significativamente el sesgo. Es necesaria una junta interna de revisión ética para evaluar los usos potenciales de la tecnología, garantizando un despliegue ético, especialmente en áreas sensibles como las aplicaciones policiales y gubernamentales. Además, las listas de vigilancia deben crearse a partir de cero en función de las necesidades específicas, utilizando imágenes de alta calidad e identificadores anónimos para mejorar la precisión y proteger al mismo tiempo la privacidad.

Las opciones avanzadas de privacidad y un rendimiento sólido en condiciones reales son vitales. Funciones como el desenfoque facial y el descarte de detecciones que no figuren en la lista de vigilancia protegen la identidad de los transeúntes, mientras que la tecnología debe destacar en entornos difíciles, como con poca luz o grandes multitudes, utilizando algoritmos avanzados. El reconocimiento de objetos basado en la ropa o las características corporales puede ayudar en las investigaciones sin utilizar los rasgos faciales, manteniendo la privacidad. Las políticas de uso ético claramente definidas, los roles de usuario personalizables y los permisos ayudan a evitar el uso indebido, garantizando que la tecnología se utilice de forma legal y ética.

## Priorizar la privacidad y el juicio humano en el reconocimiento facial

Para utilizar éticamente la tecnología de reconocimiento facial, es esencial respetar los derechos de las personas, incluido su derecho a la intimidad, y garantizar que no se tomen decisiones autónomas sin supervisión humana. En el ámbito de la seguridad pública y la aplicación de la ley, los gobiernos deben colaborar con las autoridades para desarrollar políticas de uso aceptable que protejan los derechos de los ciudadanos y, al mismo tiempo, permitan adoptar medidas de seguridad.

En cualquier situación, el reconocimiento facial debe utilizarse como apoyo y no como sustituto del juicio humano. Por ejemplo, en la aplicación de la ley, los algoritmos de reconocimiento facial pueden generar rápidamente un conjunto de posibles coincidencias para su posterior análisis

humano, pero la decisión final debe tomarla siempre una persona. Así se garantiza que la tecnología sirva como herramienta para reducir posibles resultados, en lugar de tomar decisiones autónomas definitivas.

Además, la transparencia y el consentimiento del usuario son primordiales. Las organizaciones deben comunicar claramente cómo se recopilan, utilizan y protegen los datos de reconocimiento facial. Esta transparencia fomenta la confianza del público y garantiza el cumplimiento de las normas legales.

En conclusión, la tecnología de reconocimiento facial encierra un inmenso potencial para mejorar la seguridad y la comodidad en diversos sectores, pero su despliegue ético es crucial. Al adherirse a los principios de transparencia, consentimiento informado y mejora continua, las organizaciones pueden garantizar el uso responsable de esta tecnología. Configurar adecuadamente los umbrales en función de casos de uso específicos, emplear diversos conjuntos de datos para mitigar los sesgos y aplicar medidas sólidas de privacidad de los datos son pasos esenciales.

Texto adaptado de: Intelion, 18 jun. 2024. Disponível em: https://intelion.isid.com/es/uso-etico-del-reconocimiento-facial-balance-entre-tecnologia-y-privacidad/. Acesso em: 22 mai. 2025.

**QUESTÃO 01:** Com base no TEXTO 01, no que se refere à garantia do uso ético da tecnologia de reconhecimento facial, assinale a alternativa falsa.

a) O reconhecimento facial ético exige garantir a privacidade e o consentimento explícito por meio de práticas seguras de gestão de dados.

b) Reduzir o viés algorítmico e contar com uma revisão ética são fundamentais para um uso responsável e preciso dessa tecnologia, especialmente em contextos sensíveis.

c) É fundamental integrar mecanismos de proteção da privacidade com sistemas de alto desempenho tecnológico, às vezes sustentados em diretrizes éticas que previnam usos indevidos.

d) É indispensável combinar opções avançadas de privacidade com alto desempenho técnico, sempre respaldado por políticas de uso ético que evitem possíveis abusos.

**QUESTÃO 02:** Ainda referente ao TEXTO 01, assinale a alternativa que representa a ideia central da parte que trata da priorização da privacidade e do julgamento humano no reconhecimento facial.

a) Para que o reconhecimento facial seja utilizado de forma ética, é fundamental proteger a privacidade, assegurar que as decisões estejam sob responsabilidade humana e promover total transparência no tratamento dos dados.

b) O uso ético do reconhecimento facial exige priorizar a privacidade, garantir a supervisão humana nas decisões e assegurar opacidade sobre o uso dos dados, para que a tecnologia funcione como apoio e não em substituição do julgamento humano.

c) O uso do reconhecimento facial pode prescindir do julgamento humano, considerando que os algoritmos seriam suficientemente precisos para tomar decisões finais de forma autônoma, até mesmo em contextos sensíveis como a segurança pública.

d) Para garantir maior eficiência nos processos, não é necessário informar aos usuários como seus dados de reconhecimento facial serão coletados e utilizados, desde que as instituições cumpram os protocolos de segurança internos.

**QUESTÃO 03:** Leia atentamente as afirmações a seguir e marque (V) para verdadeiro ou (F) para falso, de acordo com o TEXTO 01.

(  ) Com cerca de 700 milhões de câmeras de vídeo em operação de alguns países do mundo, considerações de privacidade e ética são fundamentais no uso da tecnologia de reconhecimento facial.

(  ) Um conselho interno de revisão ética é necessário para avaliar usos possíveis da tecnologia, garantindo a ablação ética, especialmente em áreas sensíveis, como as aplicações policiais e governamentais.

(  ) No campo da segurança pública e da aplicação da lei, é essencial que os governos trabalhem em conjunto com as autoridades para criar diretrizes de uso que salvaguardem os direitos dos cidadãos e, simultaneamente, permitam a implementação de medidas de segurança.

(  ) As organizações devem comunicar claramente como os dados de reconhecimento facial são coletados, usados e protegidos. Essa transparência promove a confiança pública e garante a conformidade com os padrões legais.

**QUESTÃO 04:** Com base no TEXTO 01, traduza ao português o seguinte fragmento: “Abordar el sesgo es crucial para mejorar la precisión de la tecnología de reconocimiento facial. La utilización de conjuntos de datos diversos y amplios que incluyan diversos datos demográficos puede reducir significativamente el sesgo. Es necesaria una junta interna de revisión ética para evaluar los usos potenciales de la tecnología, garantizando un despliegue ético, especialmente en áreas sensibles (…)”.

**QUESTÃO 05:** Com base no TEXTO I, traduza ao português, ainda, o seguinte fragmento: “La tecnología de reconocimiento facial encierra un inmenso potencial para mejorar la seguridad y la comodidad en diversos sectores, pero su despliegue ético es crucial. Al adherirse a los principios de transparencia, consentimiento informado y mejora continua, las organizaciones pueden garantizar el uso responsable de esta tecnología. Configurar adecuadamente los umbrales en función de casos de uso específicos, emplear diversos conjuntos de datos para mitigar los sesgos y aplicar medidas sólidas de privacidad de los datos son pasos esenciales”.