PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

088-2025-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aéreadel Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y lasempresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°088	Fecha: 12-03-2025
		Página: 4 de 6

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Riesgos a la privacidad al crear tu imagen al estilo de Studio Ghibli		
Tipo de Ataque	Fuga de Información	Abreviatura	FugaInfo
Medios de propagación	Red, Internet, Redes sociales		
Código de familia	K	Código de Sub familia	K02
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

1. ANTECEDENTES:

La última actualización del chatbot de ChatGPT ha permitido a los usuarios replicar sus imágenes generadas al estilo de Studio Ghibli. Sin embargo, en ocasiones, sumarse a una tendencia puede desencadenar fraudes o suplantación de identidad, si la tecnología se ve comprometida o simplemente si para usarla aceptas condiciones privacidad desfavorables.

2. DETALLES:

A diferencia de otras plataformas que recolectan imágenes desde internet, el uso de generadores por medio de IA implica una cesión voluntaria y explícita de los datos por parte del usuario.

Esto tiene implicaciones directas en términos legales y técnicos. Bajo el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, el consentimiento explícito permite a empresas como OpenAI almacenar y procesar esta información con más libertad

Al tratarse de plataformas que procesan información biométrica, los datos recopilados van más allá de un simple archivo JPG.

Entre los riesgos de usar ChtaGPT para convertir tus fotos al estilo Ghibli más relevantes se encuentran:

- Reconocimiento facial: uso de los rasgos únicos del rostro para identificar personas de forma automatizada.
- Análisis emocional: detección de expresiones faciales para inferir emociones o estados de ánimo.
- Perfiles digitales: construcción de patrones de comportamiento a partir de las imágenes entregadas.
- Rastreo en línea: asociación de la identidad visual con perfiles en otras plataformas o redes sociales.
- Uso en deepfakes: posible incorporación del rostro del usuario en videos generados artificialmente.

Por otro lado, el funcionamiento de los modelos de IA depende mayoritariamente del acceso a grandes volúmenes de datos (con los que se entrenan y de los cuales se sirven), muchos de los cuales contienen información personal, sensible y confidencial.

Las diversas fuentes para recolectar información y así entrenar a los modelos de IA pueden provenir de información pública o de fuentes abiertas, información solicitada a los usuarios (quienes la consienten, como lo es en este caso con la tendencia de las imágenes generadas al estilo Studio Ghibli) y también de redes sociales y, más recientemente, de información recopilada por dispositivos IoT.

Dada la gran cantidad de datos, está claro que, si estos no son tratados y almacenados de forma segura, pueden quedar expuestos y sujetos a posibles accesos indebidos, filtraciones o incluso robos de información.

Unirse a esta tendencia además del entusiasmo puede traer riesgos de la privacidad si no se toman las debidas precauciones.

3. RECOMENDACIONES:

- Preferir plataformas con estándares de seguridad claros, buscar servicios que tengan políticas transparentes y cumplan con certificaciones en protección de datos.
- Limitar permisos y accesos innecesarios, no autorizar a estas plataformas acceder a tu galería completa o a tu cámara si no es indispensable.
- Revisar las políticas de privacidad del sitio o aplicación, sobre cómo funcionan los modelos de IA y cómo tratan la información, para saber si es fiable subir o no información personal o confidencial.
- Revisar si la información que se sube al sitio o aplicación está protegida por alguna ley, de tal manera que cumplan con regulaciones internacionales y nacionales pertinentes, así como con los principios éticos de transparencia, explicabilidad, equidad y responsabilidad.
- Evitar subir imágenes sensibles o de terceros, en especial cuando se trata de menores de edad o personas que no han dado su consentimiento.
- Usar aplicaciones web o móviles de fuentes oficiales.

Fuente de Información:	• hxxps://www.welivesecurity.com/es/privacidad/riesgos-crear-tu-imagen-estilo-studio-ghibli/ • hxxps://www.excelsior.com.mx/hacker/cuales-son-los-riesgos-de-usar-chtagpt-para-convertir-tus-fotos-al-estilo-ghibli/1708032

Índice alfabético