



CRITERIOS

que debe cumplir una Aplicación Móvil Institucional (AMI)
para su publicación en las Tiendas de APPS Google Play y App Store de la UNAM.

24 de noviembre de 2021
Versión 4.3

Dirección de Sistemas y Servicios Institucionales
Acervos Digitales
Tiendas de APPS

https://www.apps.unam.mx/pdf/DGTIC_Lineamientos/DGTIC_Lineamientos.html



1. VERSIÓN DEL DOCUMENTO.

El presente documento entra en vigencia a partir del 24 de noviembre del 2021 y es la versión 4.3.

2. CRITERIOS QUE DEBE CUMPLIR UNA APLICACIÓN MÓVIL INSTITUCIONAL (AMI) PARA SU PUBLICACIÓN EN LAS TIENDAS DE APPS GOOGLE PLAY Y APP STORE DE LA UNAM.

Como parte de los Lineamientos para el desarrollo y publicación de aplicaciones móviles institucionales (AMI), los criterios que debe cumplir una AMI para su publicación en las Tiendas de Apps Google Play y App Store de la UNAM son los siguientes:

1. FACILIDAD DE APRENDIZAJE: Es la facilidad con la que los usuarios alcanzan objetivos específicos desde la primera vez que utilizan la aplicación.

2. MEMORIA: Es la facilidad para memorizar la forma de utilizar la aplicación. Se considera también la facilidad con la que los usuarios vuelven a utilizar la aplicación después de un tiempo.

3. ERRORES: Se refiere a los errores encontrados a la aplicación y la gravedad de éstos. **La aplicación debe de producir la menor cantidad de errores posibles.** Es importante que el desarrollador los corrija de forma rápida. Se consideran errores:

- a) La carencia de la pantalla de bienvenida con el escudo de la UNAM.
- b) Que el escudo de la UNAM no se despliegue por un mínimo de 2.5 segundos en la pantalla de bienvenida.
- c) Carencia de la sección de “Acerca de...” en algún apartado del aplicativo.
- d) La carencia de la liga a la política de privacidad.
- e) Que haya secciones anunciadas como “Próximamente disponibles” o incompletas.
- f) Fallas que impidan el funcionamiento total del aplicativo o de cualquiera de sus secciones.

g) La aparición de mensajes de error durante el uso del aplicativo que no puedan solucionarse.

h) Carencia de un manejo apropiado de los mensajes de error que dificulte conocer el estado de operación del aplicativo.

4. CONTENIDO: Realizar una adecuada distribución de los contenidos, manejo de colores y formatos para presentar la información al usuario final, así como que no haya faltas de ortografía, errores de redacción o un uso inapropiado del idioma. P. ej. (mensajes combinados en español con el inglés). Este punto también considera un correcto funcionamiento del diseño responsivo del aplicativo, que permita que el aplicativo despliegue la información correctamente en todo tipo y tamaño de dispositivos móviles en los modos horizontal y vertical.

5. ACCESIBILIDAD: Consideraciones tenidas en cuenta en el desarrollo de las apps por las posibles limitaciones físicas, visuales, auditivas o de otra índole de los usuarios finales tales como:

- a) Manejo de tamaños de las fuentes adecuadas.
- b) Tamaño de los objetivos táctiles adecuados.
- c) Bajo contraste o mal uso del color que dificulten la lectura de los elementos visuales de la app.
- d) Correcto uso de etiquetas de contenido.

6. ASPECTOS DE SEGURIDAD: En lo referente a los aspectos de seguridad se verifica lo siguiente:

a) Uso adecuado de los permisos solicitados por el aplicativo para acceder a los recursos internos del dispositivo móvil e información del usuario final, esto en relación con la funcionalidad esperada de la AMI. **La app deberá solicitar autorización al usuario final para hacer uso de su información sensible por medio de mensajes emergentes e informar para que utilizará la información que pueda recabar.**

b) En medida de los recursos y capacidades UNAM-CERT, pruebas de seguridad a las apps y a los servicios empleados por las apps. Las pruebas consisten en la identificación y análisis de vulnerabilidades, que bajo ciertas condiciones podrían ser aprovechadas para provocar alguna afectación en la confidencialidad, integridad o disponibilidad de los activos de información.

c) La disponibilidad en el aplicativo de los mecanismos mínimos necesarios para garantizar la seguridad de la información y de la infraestructura de cómputo y telecomunicaciones de la UNAM durante la operación del aplicativo.

Sugerencias para el manejo de la seguridad de la información:

En el caso de aplicativos que realicen un manejo de información confidencial, se sugiere implementar el uso de técnicas de anonimización de datos.

Anonimización de los datos.

- Proceso de eliminar las referencias cualquier identificación personal de un conjunto de datos.
- Este proceso se aplica sobre un conjunto de datos para conservar la privacidad de los individuos a los que se hace referencia.
- Es necesario aplicar este proceso cuando se quieren hacer públicos datos con identificadores como nombres, direcciones o códigos postales.
- En general, se debe intentar eliminar cualquier información que pueda identificar al individuo.

Tipos de anonimización.

- Eliminación de datos.
- Cifrado de los datos sensibles: depende del uso de una buena clave para el cifrado y el coste del proceso.

- Enmascaramiento de los datos sensibles: se pretende mantener la estructura de la fuente de datos original. Los tipos se conservan, sus valores no.

Recordar que la anonimización no asegura la protección.

- La anonimización no proporciona protección absoluta.
- Cualquier conjunto de datos suficientemente extenso puede ser desanonimizado usando información del contexto.
- Con datos sensibles, como la salud, se sugiere limitar los campos más sensibles respecto a la privacidad y aplicar las técnicas más complejas de anonimización.

7. CONTEXTO: Conjunto de circunstancias o factores relacionados al entorno de la aplicación que puedan interferir su adecuado uso.

8. RESPUESTA EMOCIONAL: Cómo se siente el usuario al terminar de usar la aplicación (Feliz, satisfecho, bajo tensión, molesto, inconforme, etc.).

