*Alumno: Gonzalez, Diego Andrés.*
*Legajo: 10413/7*

# Informe buenas prácticas en privacidad para el desarrollo de aplicaciones

En nuestra era digital, la privacidad no es total ni siquiera en nuestro propio hogar, ya que dejamos una huella digital a través de los dispositivos conectados a internet.

Como desarrolladores de software, es nuestra responsabilidad garantizar la privacidad de los datos personales que los usuarios confían a nuestras aplicaciones. Esto implica establecer una política de uso de datos clara y transparente, que permita a los usuarios conocer cómo se tratarán sus datos y generar confianza en el correcto manejo de la información, en cumplimiento con las leyes de protección de datos.

Este informe ofrece recomendaciones clave para desarrollar aplicaciones y establecer políticas de datos que respeten la privacidad y seguridad de los usuarios.

Por lo tanto, dedicar tiempo y esfuerzo a la elaboración de una Política de Privacidad clara, precisa y adaptada a las prácticas específicas de nuestra aplicación es fundamental para garantizar la transparencia y el cumplimiento normativo.

**Palabras claves:** privacidad, protección, seguridad, transparencia, consentimiento.

## Principios de privacidad

**Consentimiento:** El consentimiento del titular para el uso de su información personal es la única manera en la que el tratamiento de datos es lícito, salvo que se trate de alguna excepción prevista por la ley.

**Finalidad:** Los datos que recolectan nuestras aplicaciones solo pueden ser utilizados conforme con la finalidad con la que originalmente se los solicitó.

**Calidad:** Las aplicaciones solamente pueden pedir datos adecuados, pertinentes y no excesivos en relación con la finalidad que motivó su recolección.

**Seguridad:** Evaluar los riesgos de seguridad que la aplicación puede aparejar, teniendo en cuenta la sensibilidad de la información personal que recolecta y almacena.

**Confidencialidad:** Los datos personales que nuestra aplicación toma consentimiento debido al tratamiento que realices son confidenciales.

En el desarrollo de nuestras aplicaciones tanto el administrador como el portal público, lamentablemente no elaboramos políticas formales de privacidad y protección de datos. Nos centramos en el desarrollo de las funcionalidades del sistema y, debido a restricciones de tiempo, no pudimos completar esta tarea. Sin embargo, hemos adherido a principios clave: solo solicitamos datos necesarios para la funcionalidad de la aplicación y los protegemos datos necesarios como contraseñas mediante encriptación. No compartimos información con terceros y, en caso de ser necesario, informaríamos a los usuarios. Reconocemos la importancia de informar a los usuarios sobre el tratamiento de sus datos gracias a la clase que nos dío

Mariano al compartir la guía de buenas prácticas y nos comprometemos a mejorar en este aspecto en el futuro para garantizar el cumplimiento de los principios de privacidad.

## Consideraciones de privacidad aplicada a nuestro desarrollo

Es fundamental integrar la protección de la privacidad en todos los procesos de tu organización. Esto implica el desarrollo de aplicaciones con el principio de "privacidad desde el diseño", donde se prioriza la seguridad y confidencialidad de los datos desde el momento de la concepción.

Una política de privacidad clara y fácilmente accesible para los titulares de datos es esencial. Debe proporcionarse de manera transparente y comprensible, permitiendo a los usuarios tomar decisiones informadas sobre el manejo de su información personal.
Dar a los titulares de datos el control sobre su privacidad es crucial. Deben tener la capacidad de elegir y ajustar la configuración de privacidad según sus preferencias individuales.

Es importante limitar la cantidad de datos que se recopilan y retienen en la aplicación, evitando la recopilación excesiva y el almacenamiento innecesario de información sensible.
La seguridad de los datos personales recopilados debe ser una prioridad, implementando medidas robustas para protegerlos contra accesos no autorizados o violaciones de seguridad.

Designar a un "responsable de privacidad" o a un desarrollador de la aplicación para asumir la responsabilidad del resguardo de los datos personales es una práctica recomendada. Esta persona debe garantizar el cumplimiento de las políticas de privacidad y estar preparada para abordar cualquier problema relacionado con la seguridad de los datos.

En nuestra aplicación, hemos designado al superadmin como el único responsable de la privacidad del lado del administrador. Sin embargo, esto limita el derecho del usuario a controlar y modificar sus propios datos. Esta decisión fue tomada debido a restricciones de tiempo durante el desarrollo inicial, donde priorizamos la gestión eficiente de los datos sensibles. Nos comprometemos a agregar la funcionalidad que permita a los usuarios tener control total sobre sus datos en futuras actualizaciones, reconociendo la importancia de cumplir con este derecho fundamental.

## Política de privacidad

En el proceso de desarrollo de nuestra aplicación, un aspecto crítico es la creación de una Política de Privacidad que detalle con claridad qué tipo de información se recopila, cómo se utiliza y con quién se comparte. Esta política debe ser redactada de manera simple y preferiblemente estandarizada, facilitando así su lectura y comprensión por los usuarios cuyos datos se recaban.

Es esencial que la Política de Privacidad refleje de manera precisa el tratamiento de datos llevado a cabo por nuestra aplicación. Se desaconseja el "cortar y pegar" de políticas genéricas de otras aplicaciones o desarrolladores, ya que esto puede ocasionar problemas tanto con los clientes como con los titulares de los datos de nuestra aplicación, e incluso con las autoridades regulatorias.

El incumplimiento de este principio puede conllevar inconvenientes significativos, incluyendo la pérdida de confianza por parte de los usuarios, la exposición a demandas legales por parte de los titulares de datos y la posibilidad de enfrentar sanciones por parte de las entidades reguladoras pertinentes.

## Control de la información personal por parte de sus titulares

Es esencial otorgar a los usuarios de aplicaciones y a los dueños de datos el control absoluto sobre su información personal, especialmente en casos que involucren datos delicados o íntimos, o cuando se utilicen con propósitos fuera de lo común. Debe ser sencillo para los usuarios acceder a sus datos almacenados, permitiendo la corrección de información errónea o desactualizada, y la eliminación de datos cuando sea necesario.

El consentimiento del titular de los datos debe obtenerse en todo momento para el uso de su información personal. Por ejemplo, si inicialmente se solicita un dato para un propósito específico y posteriormente se desea utilizar para una nueva funcionalidad en la aplicación, o si surge un uso no previsto inicialmente, es imperativo solicitar nuevamente el consentimiento del usuario en el momento en que vuelva a interactuar con la aplicación. Este enfoque garantiza la transparencia y el respeto por la privacidad del usuario en todo momento.

## Uso de aplicaciones por niños

Debemos limitar al mínimo esencial tanto la variedad como la cantidad de datos que recolectamos de nuestros usuarios, aplicando medidas de seguridad estrictas para salvaguardar la información necesaria. Es crucial abstenerse de compartir datos personales de menores con terceros. Además, es fundamental ofrecer orientación adaptada al nivel de comprensión de los menores sobre el manejo adecuado de sus datos y alertar sobre los peligros asociados con un uso inapropiado. Siempre que corresponda, se debe obtener el consentimiento de los padres o tutores, e implementar sistemas de protección que mantengan a estos informados sobre el uso de los datos personales de los menores.

En nuestra aplicación, asumimos que los usuarios serán mayores de edad y no implementamos restricciones a la hora del registro. Sin embargo, esta omisión podría resultar en la inscripción de menores que sin el tratamiento adecuado de datos puede conllevar a un error potencialmente grave. Será un tema a tener en cuenta en futuras actualizaciones para garantizar el cumplimiento legal.

## Términos y condiciones - Nociones básicas

Los términos y condiciones son cláusulas legales que delinean el uso y acceso a la información de una página web o aplicación. Estas condiciones especifican cómo el propietario del sitio o la aplicación manejará tanto tus datos personales como los datos que generes durante su uso.

Se trata de condiciones unilaterales que debes aceptar para poder acceder y utilizar los servicios ofrecidos por la página web o aplicación, conformando así un contrato de adhesión.

Al aceptar los términos y condiciones, otorgas tu consentimiento para que la empresa pueda almacenar, procesar, analizar o utilizar tus datos con diversos fines, según lo estipulado en dichos términos y condiciones.

## La información que debe incluirse en los términos y condiciones de una página web abarca diversos aspectos:

**Datos de identificación:** Se deben proporcionar los datos del profesional o la empresa propietaria de la página web.

**Derechos de propiedad intelectual e industrial:** Debe indicarse quién es el titular de los elementos de la página web y qué tipo de licencias de uso se otorgan a los usuarios.

**Pasos para contratar:** Se deben detallar los pasos necesarios para adquirir productos o servicios, así como los derechos y obligaciones del usuario.

**Producto o servicio:** Debe especificarse claramente qué producto o servicio se ofrece para contratar a través de la web.

**Precios, duración y formas de pago:** Se debe informar sobre los precios, impuestos, cargos adicionales, duración del contrato, formas y condiciones de pago, así como las consecuencias por mora o incumplimiento.

**Reglas de conducta:** Si es necesario registrarse, se deben establecer las condiciones de uso, derechos y responsabilidades del usuario.

**Responsabilidades:** Deben detallarse las responsabilidades asumidas y las limitaciones de responsabilidad.

**Garantías:** Se deben proporcionar las garantías asociadas a la adquisición de productos o servicios.

**Legislación aplicable y resolución de conflictos:** Se debe indicar la legislación aplicable y el sistema de resolución de conflictos.

**Otros aspectos:** Se deben incluir condiciones específicas para ofertas y promociones, así como detalles sobre servicios de post-venta, si se ofrecen.

Es crucial que los términos y condiciones estén redactados en un lenguaje claro por varias razones:

**Cumplimiento legal:** La normativa requiere que los usuarios estén plenamente informados sobre las condiciones de contratación de un producto o servicio.

**Prevención de sanciones:** Una redacción incompleta o inadecuada puede resultar en sanciones por parte de entidades gubernamentales.

**Comprensión del usuario:** Es fundamental que las condiciones sean comprensibles para los usuarios, evitando ambigüedades, para que puedan conocer y entender las reglas a las que están sujetos.

**Transparencia y confianza:** Una redacción clara y transparente en los términos y condiciones contribuye a generar confianza en la empresa y en sus servicios, fortaleciendo así la relación con los usuarios.

La falta de una política de privacidad en nuestra aplicación resalta algunas deficiencias importantes que deberían haberse comunicado al usuario. Por ejemplo, no se especifica el procedimiento paso a paso para contratar servicios, lo cual sería especialmente útil en el caso de contratar un servicio en CIDEPINT. Además, no se establecen reglas de conducta al contratar un servicio ni se detallan las responsabilidades, garantías o procedimientos para la resolución de conflictos, entre otros aspectos importantes. Reconocemos la importancia de abordar estas cuestiones para brindar una experiencia transparente y segura a los usuarios.

## Registro y Autenticación con redes sociales

**Pérdida de control sobre datos personales:** El servicio puede acceder a datos del perfil social del usuario, cediendo parte de su privacidad.

**Uso no consentido de datos:** Los datos obtenidos de la red social pueden emplearse para fines distintos a los autorizados por el usuario, comprometiendo su privacidad.

**Mayor exposición a seguimiento:** Las redes sociales pueden acceder a más información sobre el comportamiento en Internet, facilitando el seguimiento y perfilado del usuario.

**Riesgo ante brechas de seguridad:** En caso de una vulneración, la contraseña del usuario no se ve afectada, pero su información del perfil social, incluyendo intereses y perfiles publicitarios, puede estar en riesgo.

**Amplificación del riesgo:** Si se pierde el control sobre la cuenta de la red social, también se pierde el control sobre otros servicios vinculados, lo que podría comprometer aún más la seguridad y privacidad del usuario.

Es esencial brindar garantías adecuadas para evitar la pérdida de control sobre los datos personales, ya que esto podría derivar en un mal uso de la información, como el seguimiento o perfilado no deseado de las personas.

## Conclusión

En resumen, adoptar buenas prácticas en privacidad durante el desarrollo de aplicaciones es fundamental para proteger los datos personales de los usuarios y garantizar su confianza. Esto implica implementar medidas de seguridad robustas, establecer políticas de privacidad transparentes y accesibles, permitir a los usuarios controlar sus datos, limitar la recopilación de información, y cumplir con las regulaciones legales pertinentes. Al priorizar la privacidad desde el diseño y mantener un enfoque proactivo en la protección de los datos, los desarrolladores pueden construir aplicaciones que no solo sean funcionales y atractivas, sino también éticas y respetuosas de la privacidad de los usuarios.