PROYECTAMOS SAS

Lineamientos de desarrollo seguro de software (ODK)



Proyectamos Colombia SAS

CONTENIDO

Objetivo 3
Importancia de los lineamientos en el desarrollo de software con ODK 4
Arquitectura empleada 5
Licencias 9
Control de cambios 10

La dirección de PROYECTAMOS SAS, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con se basa en principios y prácticas que aseguran la creación de aplicaciones robustas, eficientes y mantenibles. Estos principios incluyen, entre otros, la modularidad, la reutilización de código, la escalabilidad, la seguridad y la usabilidad. Además, las prácticas ágiles, como el desarrollo iterativo, la integración continua y las pruebas automatizadas, son esenciales para mantener la calidad y la adaptabilidad del software.

En este sentido, uno de los enfoques de mayor aceptación en el campo de la recopilación de datos es el uso de Open Data Kit (ODK). ODK es un conjunto de herramientas de software de código abierto que facilita la recopilación de datos móviles, especialmente en áreas con conectividad limitada o inexistente. ODK ha evolucionado para convertirse en una solución integral para proyectos de recolección de datos en entornos desafiantes, como áreas rurales, comunidades en desarrollo y zonas afectadas por desastres.

Objetivo

Establecer los lineamientos procedimentales basado en las políticas en seguridad de la información y ciberseguridad de acuerdo con los lineamientos de buenas prácticas en seguridad, privacidad para el manejo y protección de la información física y lógica propia y de terceros, con el fin de regular la gestión de la seguridad de la información al interior de la entidad.

Importancia de los lineamientos en el desarrollo de software con ODK

Desarrollar aplicaciones con Open Data Kit (ODK) requiere seguir ciertos lineamientos para asegurar que las soluciones sean efectivas, sostenibles y de alta calidad. La adherencia a estos lineamientos no solo mejora la funcionalidad del software, sino que también asegura su adaptabilidad y durabilidad en diversas condiciones operativas. Estos lineamientos son esenciales para maximizar el impacto positivo de ODK en proyectos de recopilación de datos, especialmente en entornos desafiantes, como lo son:

- Diseño centrado en el usuario: La clave para una implementación exitosa de ODK es entender profundamente las necesidades y contextos de los usuarios finales. Un diseño centrado en el usuario implica crear formularios y aplicaciones que sean intuitivos y fáciles de usar, reduciendo la carga cognitiva y minimizando los errores durante la recolección de datos. Esto incluye utilizar un lenguaje claro, instrucciones precisas y una interfaz de usuario coherente y accesible. Además, implica iterar sobre el diseño basado en la retroalimentación constante de los usuarios, lo que asegura que las soluciones evolucionen de manera efectiva para satisfacer las necesidades cambiantes.

- Modularidad y escalabilidad: La modularidad en el desarrollo de software con ODK implica diseñar componentes que sean independientes y reutilizables. Esto permite realizar actualizaciones y modificaciones sin afectar todo el sistema, facilitando la mejora continua y la adaptación a nuevos requisitos. La escalabilidad es igualmente crucial, ya que asegura que la solución puede manejar un incremento en el volumen de datos y usuarios sin comprometer el rendimiento.

- Manejo eficiente de datos: La integridad y seguridad de los datos son aspectos fundamentales en cualquier proyecto de recolección de datos. Con ODK, es vital implementar prácticas que aseguren la protección de los datos desde la captura hasta el almacenamiento y análisis. Esto incluye el cifrado de datos en tránsito y en reposo, la implementación de controles de acceso adecuados, y el aseguramiento de la integridad de los datos mediante validaciones y pruebas exhaustivas. Además, es importante considerar la privacidad de los participantes y cumplir con las regulaciones locales e internacionales de protección de datos.

- Pruebas exhaustivas: Las pruebas rigurosas son esenciales para identificar y corregir errores antes del despliegue de la aplicación. Esto incluye pruebas unitarias, pruebas de integración, pruebas de aceptación del usuario y pruebas de rendimiento. Las pruebas deben ser continuas y abarcar todos los posibles escenarios de uso para garantizar que la aplicación funcione correctamente en condiciones reales. La implementación de un entorno de pruebas automatizadas puede mejorar la eficiencia y la efectividad del proceso de pruebas, asegurando una mayor cobertura y una detección temprana de problemas.

- Documentación y capacitación: La documentación detallada y la capacitación adecuada son componentes críticos para el éxito de cualquier proyecto de desarrollo de software con ODK. La documentación debe cubrir todos los aspectos del sistema, incluyendo la configuración, uso, mantenimiento y solución de problemas. Una buena documentación facilita la transferencia de conocimientos y asegura que cualquier miembro del equipo pueda entender y trabajar con el sistema. La capacitación de los usuarios finales y administradores es igualmente importante para garantizar que puedan utilizar y mantener la solución de manera efectiva. Esto puede incluir talleres, tutoriales en línea y soporte continuo.

Arquitectura empleada

La arquitectura del aplicativo de captura ODK basa sus procesos en el diagrama de flujo de información utilizado por los modelos de información y herramientas de Open Data Kit (ODK). ODK es una suite de código abierto para recolección de datos que incluye herramientas para crear y distribuir formularios, recolectar y almacenar datos en campo y finalmente transmitirlos y acopiarlos en un servidor central para su procesamiento y análisis, en tiempo real cuando existe conectividad, o de manera asincrónica de ser necesario.



Fuente: elaboración propia

El anterior gráfico describe el flujo de información que realiza ODK en la integración de sus diferentes plataformas. Consiste en tres aplicaciones separadas que funcionan ensambladas para cada parte del proceso de diseño y recolección:

1.1. ODK Build

ODK Build es una herramienta para la creación de formularios de datos, definiendo reglas de validación y lógica básica. Los formularios pueden ser en formato .xml o .xlsx (XForm), que contiene:

- El cuestionario.
- Opciones de respuesta.
- Reglas de validación.

Son simples para comenzar, pero permiten la creación de formularios complejos por parte de alguien familiarizado con la sintaxis y el lenguaje propio de programación con una funcionalidad compleja como la lógica de omisión de manera coherente en una serie de plataformas de recopilación de datos móviles y web. Parte del protocolo de seguridad de la información es la codificación de las opciones de respuesta para ser leída posteriormente por el analista por documentos soporte necesarios para ello.

1.1 Reglas de Validación y Lógica

- Validación de Entradas: Implementar validaciones robustas para asegurar que las entradas de los usuarios cumplan con los formatos esperados.
- Lógica de Omisión: Utilizar lógica de omisión para asegurar que solo se muestren preguntas relevantes, reduciendo la exposición de datos sensibles.
- Codificación y Decodificación: Implementar la codificación de las opciones de respuesta para ser leídas posteriormente por el analista de datos.

1.2. ODK Central Server

ODK Central Server es la aplicación en el servidor que recibe e integra los datos recopilados en campo. Administra cuentas y permisos de usuarios, almacenas definiciones de formularios y permite la recopilación de datos.

1.2.1 Gestión de Seguridad en el Servidor

Gestión de Usuarios y Permisos: Crear tipos de registro y perfiles de usuario con permisos específicos (lectura, escritura, modificación, eliminación).

Cifrado de Datos: Todos los datos almacenados deben estar cifrados usando algoritmos fuertes como AES-256.

Autenticación y Autorización: Implementar autenticación multifactor (MFA) y controles de acceso basados en roles (RBAC).

Auditoría y Monitoreo: Registrar y monitorear todas las actividades en el servidor para detectar y responder a actividades sospechosas.

Manejo de Claves: Uso de claves privadas para desencriptar las instancias de datos recibidas en el servidor, garantizando que solo personal autorizado pueda acceder a los datos sensibles.

1.3. ODK Collect

ODK Collect es una aplicación Android de código abierto que reemplaza los formularios en papel. Soporta varios tipos de preguntas y está diseñado para funcionar sin conectividad de red.

1.3.1. Seguridad en la Captura de Datos

Configuración Segura del Dispositivo: La configuración del dispositivo móvil se realiza mediante código QR para asegurar la privacidad en la transferencia de datos.

Cifrado de Formularios: Utilizar cifrado de bloque de transmisión AES Cipher Feedback (CFB) de 256 bits para los datos del formulario y archivos adjuntos.

Generación de Claves: En el momento de finalización de los formularios, se genera una clave aleatoria de cifrado/descifrado de 256 bits mediante un generador de números aleatorios (Secure Random).

Eliminación Segura: Una vez cifrados, eliminar todos los datos de texto sin formato y archivos adjuntos que se usaron en el proceso de cifrado.

2. Seguridad de la Información

2.1. Creación de Formularios

Validación de Entradas: Validaciones robustas para asegurar que las entradas de los usuarios cumplan con los formatos esperados.

Lógica de Omisión: Utilización de lógica de omisión para mostrar solo preguntas relevantes y reducir la exposición de datos sensibles.

Codificación y Decodificación: Implementación de codificación para las opciones de respuesta para ser leídas posteriormente por el analista.

2.2. Seguridad en el Servidor Central

Gestión de Usuarios y Permisos: Crear tipos de registro y perfiles de usuario con permisos específicos (lectura, escritura, modificación, eliminación).

Cifrado de Datos: Cifrar todos los datos almacenados utilizando algoritmos fuertes como AES-256.

Autenticación y Autorización: Implementar autenticación multifactor (MFA) y controles de acceso basados en roles (RBAC).

Auditoría y Monitoreo: Registrar y monitorear todas las actividades en el servidor para detectar y responder a actividades sospechosas.

Manejo de Claves: Uso de claves privadas para desencriptar las instancias de datos recibidas en el servidor.

2.3. Seguridad en la Captura de Datos (ODK Collect)

Configuración Segura del Dispositivo: La configuración del dispositivo móvil se realiza mediante código QR para asegurar la privacidad en la transferencia de datos.

Cifrado de Formularios: Utilizar cifrado de bloque de transmisión AES Cipher Feedback (CFB) de 256 bits para los datos del formulario y archivos adjuntos.

Generación de Claves: En el momento de finalización de los formularios, se genera una clave aleatoria de cifrado/descifrado de 256 bits mediante un generador de números aleatorios (Secure Random).

Eliminación Segura: Una vez cifrados, eliminar todos los datos de texto sin formato y archivos adjuntos que se usaron en el proceso de cifrado.

3. Mejores Prácticas de Seguridad

3.1. Desarrollo Seguro

Control de Versiones: Utilizar sistemas de control de versiones (e.g., Git) y revisar el código regularmente.

Pruebas de Seguridad: Realizar pruebas de penetración y análisis de vulnerabilidades regularmente.

Capacitación en Seguridad: Capacitar a los desarrolladores en las mejores prácticas de seguridad de software.

3.1.1. Gestión del Código Fuente

Revisiones de Código: Implementar revisiones de código periódicas y auditorías para asegurar la calidad y seguridad del código.

Integración Continua (CI/CD): Utilizar pipelines de CI/CD para automatizar pruebas y despliegues, asegurando que el código pase por evaluaciones de seguridad antes de ser desplegado.

3.1.2. Análisis de Vulnerabilidades

Escaneo de Seguridad: Utilizar herramientas de escaneo de seguridad estático (SAST) y dinámico (DAST) para identificar y corregir vulnerabilidades en el código.

Pruebas de Penetración: Realizar pruebas de penetración periódicas para identificar posibles vectores de ataque y corregir vulnerabilidades.

3.2. Operaciones Seguras

Actualizaciones Regulares: Mantener el software y las dependencias actualizadas con los últimos parches de seguridad.

Copia de Seguridad: Implementar un plan de copias de seguridad regular y asegurar que las copias estén cifradas.

Respuesta a Incidentes: Establecer un plan de respuesta a incidentes y realizar simulaciones regulares para asegurar su efectividad.

3.2.1. Monitorización y Alertas

Sistemas de Monitorización: Implementar sistemas de monitorización para detectar actividades inusuales y posibles incidentes de seguridad.

Alertas de Seguridad: Configurar alertas para notificar a los administradores sobre eventos sospechosos o vulnerabilidades detectadas.

3.2.2. Gestión de Incidentes

Plan de Respuesta a Incidentes: Crear y mantener un plan de respuesta a incidentes que incluya la identificación, contención, erradicación y recuperación ante incidentes de seguridad.

Simulaciones y Ejercicios: Realizar simulaciones y ejercicios de respuesta a incidentes para preparar al equipo ante situaciones de seguridad.

Según la documentación oficial de ODK, en el apartado 34.1; la cual puede consultarse en: https://docs.getodk.org; donde se habla específicamente de la forma de licenciamiento, se manifiesta que el software ODK se publica bajo la licencia Apache 2, que denomina código abierto a un modelo de producción descentralizada que permite que cualquier persona modifique y comparta tecnología porque su diseño es accesible de manera pública.

La licencia Apache es permisiva ya que no exige que las obras derivadas (versiones modificadas) del software se distribuyan usando la misma licencia (a diferencia de las licencias copyleft). Requiere la aplicación de la misma licencia a todas las partes no modificadas y en cada archivo de licencia, así como los derechos de autor, patentes, marcas, y las comunicaciones originales de atribución de código redistribuido se deben mantener (con exclusión de avisos que no pertenezcan a ninguna parte de los trabajos derivados) y, en cada cambio de la licencia de archivo, se debe añadir la notificación que indica que se han realizado cambios a ese archivo. Para la consulta de licencia puede visitarse el siguiente link:

https://www.apache.org/licenses/LICENSE-2.0

Todas las demás herramientas que intervienen en la adaptación y personalización de las herramientas de captura (por ejemplo, el sitio web de ODK) están liberados bajo la Licencia Internacional Creative Commons Atribución 4.0., de tal forma que todos los instaladores, programas, código fuente y documentación se proporcionan sin garantía o condiciones, y sin ninguna obligación de responsabilidad. Es decir, se es libre de:

- Compartir: copiar y redistribuir el material en cualquier medio o formato para cualquier propósito, incluso comercialmente.

- Adaptar: remezclar, transformar y construir a partir del material para cualquier propósito, incluso comercialmente.

El software ODK se publica bajo la licencia Apache 2.0. Como cualquier otra de las licencias de software libre, la Licencia Apache permite al usuario del software la libertad de usarlo para cualquier propósito, distribuirlo, modificarlo, y distribuir versiones modificadas de ese software.

Control de cambios

Última revisión: abril 2024

- Junio 2023
- junio 2022
- junio 2021

Creado en julio 2020