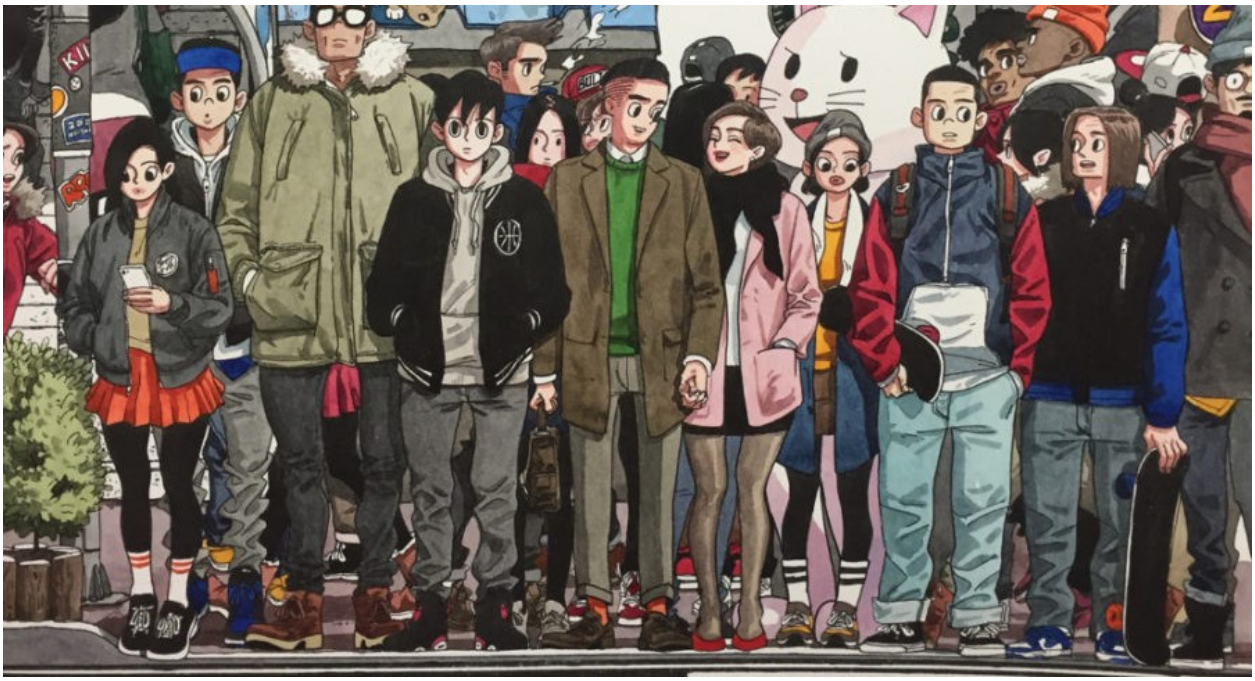
Documento de protección de datos personales

Creado por	Josue Hernandez Chavez
Fecha de creación	@October 6, 2023 5:52 PM
Etiquetas	DMI



Documento de protección de datos personales.

Introducción:

Este documento sirve como un pilar fundamental para la protección de la privacidad y los derechos de los individuos en un mundo donde la información personal es altamente valorada y vulnerable. El documento de seguridad de datos personales es esencial para proteger la privacidad de los usuarios, cumplir con las leyes aplicables,

ganar la confianza del usuario y salvaguardar la reputación de una organización. Su correcta implementación y actualización continua son críticas en el panorama digital actual.

Importante:

Este documento es únicamente de carácter **interno** debido al contenido de suma delicadeza del mismo, por lo que **queda estrictamente prohibido su publicación o filtración fuera de la empresa sin la aprobación del responsable correspondiente**. Si se viola dicha afirmación se procederá legalmente contra el infractor.

Medidas de seguridad

Cifrado

La información sensible como la contraseña para el inicio de sesión se guardara de forma encriptada y mediante el uso de una llave privada. Esta información pasa por un método de cifrado en cuanto llega al servidor. Posteriormente se envía a la base de datos donde permanecerá en este estado hasta que el usuario retire dicha información.

Firewall

En el servidor se establecerán políticas CORS para impedir que cualquier solicitud de origen diferente al establecido pueda ser procesada. Esto con el fin de proteger la integridad de los datos y el correcto funcionamiento del servicio.

Control de acceso

Referente al acceso al servicio y a la información se implementaran JsonWebTokens, los cuales se acoplaran en cualquier petición al servidor para que se tenga un mejor control de acceso. Estos tokens tendrán vigencia de un máximo de 3 inicios de sesión o no mas de 2 semanas. Para el acceso al administrador. se configuró una ruta especifica para su acceso además de estrategias de seguridad mas rigurosas como duración de sesión, o información se inicio fuera de la base de datos.

Detección y respuesta ante incidentes

En el caso de que se registren múltiples inicios de sesión fallidos por parte del administrador, el servicio bloqueara temporalmente todos los intentos posteriores. El

usuario no tendrá este nivel de seguridad hasta que el servicio implemente compras o apartados.

Protección de contraseñas

Para que un usuario pueda registrarse deberá proporcionar una contraseña con las siguientes características;

- Mínima longitud de 8 caracteres.
- Contener al menos una letra mayúscula.
- Contener al menos una letra minúscula.
- Contener algún símbolo especial.

En cuanto llega al servidor, este utiliza la llave privada establecida para comparar el texto recibido y el almacenado.

Almacenamiento de datos

La información recopilada será almacenada en un cluster de base de datos remoto a cargo de MongoDB Inc. el cual será configurado para la generación automática mensual de un respaldo de la información.

Terceros y proveedores de servicios.

La empresa Pastylla Store se compromete a no compartir la información recopilada por los usuarios que no sea con los fines establecidos en la política de privacidad. Implícitamente, se asegura de que dicha información no será compartida con ninguna otra persona que no sea la propietaria de la misma.

Acceso a datos por empleados

Los empleados de la empresa Pastylla Store tienen acceso completo a la información almacenada en la base de datos, sin embargo no a las llaves privadas para el cifrado o descifrado de claves o tokens. Solo se les tiene permitido su uso para los fines establecidos en la política de privacidad.

Confidencialidad del personal

Ningún empleado puede acceder a la información de los usuarios desde cualquier equipo que no sea proporcionado por el administrador del servicio. Además, debe tener autorización del administrador para realizar cualquier manipulación de dicha información. Si se viola dicha afirmación se procederá legalmente contra el infractor.

Conclusión

En un mundo cada vez más digitalizado, la privacidad y la seguridad de datos se han convertido en pilares fundamentales para establecer una relación de confianza entre las aplicaciones móviles y sus usuarios. La política de privacidad y seguridad de datos de nuestra aplicación móvil no es solo un conjunto de palabras y compromisos; es un contrato implícito con aquellos que confían en nosotros para proteger sus datos personales.