[Seguridad en Dispositivo móviles]

Profesor: Jesús Cabrera
Alumno: Milton Ramiro Avapillo
Año: 2° Año

Índice

1) Introducción.

Se centra en abordar una serie de aspectos críticos con el propósito de garantizar la seguridad y privacidad de los usuarios. Estos aspectos incluyen la implementación de medidas para proteger los datos de los usuarios y el compromiso con la capacitación continua de los empleados en las mejores prácticas de seguridad.

2) Considereaciones generales.

2.1 Objetivos:

- Proteger la Integridad de los datos de los usuarios como datos personales, información de pago y datos de ubicación de usuarios y conductores.
- Garantizar la protegidos de datos contra accesos no autorizados, pérdidas o alteraciones.
- Evitar brechas de datos es un objetivo critico que se busca identificar y mitigar en la infraestructura para prevenir incidentes que puedan comprometer la información de los usuarios.

2.2 Alcance

- Protección de Datos de Usuarios: garantiza la seguridad y la privacidad de la información personal, datos de pago y registros de viaje.
- Seguridad de la Plataforma Tecnológica: se encarga de protegerla contra amenazas como ataques cibernéticos.

- Gestión de Identidad y Acceso: implementar sistema de gestión de identidad y el acceso a la información, solo personal autorizado tiene acceso a la información.

- Gestión de Vulnerabilidades y Parches: Identificar y mitigar vulnerabilidades en el software mediante actualizaciones esporádicas.

2.3 Marco normativo

Reglamentación de la Ley 25.326 (Decreto 1558/2001):
Este decreto reglamenta la Ley de Protección de Datos Personales y establece pautas específicas para el tratamiento de datos personales, incluyendo la seguridad de los datos.

Ley Nº 26.388 - Ley de Delitos Informáticos:
Esta ley aborda aspectos relacionados con la ciberseguridad y establece penas para la comisión de delitos informáticos, como el acceso no autorizado a sistemas informáticos.

Resolución 47/2018 - RGPD (Reglamento General de Protección de Datos):
Aunque no es una ley argentina, es relevante para cualquier entidad que maneje datos personales, ya que regula la protección de datos a nivel de la Unión Europea. Las empresas internacionales, como Uber, que operan en Argentina y tratan datos de ciudadanos de la Unión Europea deben cumplir con esta regulación.

Regulación del Ente Nacional de Comunicaciones (ENACOM):
ENACOM regula aspectos relacionados con las telecomunicaciones y la seguridad de la información en Argentina. Es importante para las empresas que ofrecen servicios en línea, como Uber.

3)Terminos y Definiciones

3.1 Seguridad de la Información

Confidencialidad: es la capacidad de un sistema, ser o aplicación para funcionar de manera continua y segura, sin ningún tipo de interrupción debido a las amenazas cibernéticas o fallos técnicos.

Integridad: se refiere a la confianza en la precisión y consistencia de los datos y sistemas. Asegura que la información no ha sido modificada de manera corrupta.

Disponibilidad: es la capacidad de mantener los sistemas y datos accesibles y operativos cuando se requiere, sin interrupciones no planificadas debido a ataques cibernéticos, fallas técnicas o desastres.

Autenticidad: se refiere a la verificación de un usuario. Se logra mediante la confirmación de la identidad a través de credenciales, como contraseñas o sistemas de autenticación. Esto garantiza que solo usuarios autorizados tengan acceso a información o recursos sensibles, protegiendo contra el acceso no autorizado.

Adaptabilidad: se refiere a la capacidad de una organización o sistema para ajustarse y responder eficazmente a las amenazas y desafíos en constante evolución. Implica la habilidad de detectar, mitigar y recuperarse de ataques.

3.2 Termino y definiciones

Confiabilidad de la información: se refiere a la credibilidad y precisión de los datos o fuentes de información. Se evalúa según la consistencia, exactitud y veracidad de los datos, así como la confiabilidad de la fuente que los proporciona. La información confiable es precisa y puede ser verificada, lo que la hace útil y creíble para la toma de decisiones o la investigación.

Sistema de información: es una estructura organizada que recopila, almacena, procesa y distribuye datos para respaldar la toma de decisiones y las operaciones de una organización. Utiliza hardware, software y personal especializado para gestionar la información de manera eficiente. Los sistemas de información pueden variar en tamaño y complejidad, desde simples hojas de cálculo hasta sistemas empresariales avanzados. Su objetivo principal es proporcionar información precisa y oportuna para ayudar a la organización a alcanzar sus objetivos.

Tecnología de la información: es el uso de computadoras, software, redes y sistemas para almacenar, procesar, transmitir y manipular datos de manera eficiente. Incluye hardware, como computadoras y servidores, y software, como aplicaciones y sistemas operativos. La TI desempeña un papel crucial en la gestión de información, la automatización de procesos, la comunicación y la toma de decisiones en organizaciones y la vida cotidiana.

3.3 Evaluación de riesgos.

Amenazas: Uber observa situaciones o eventos que podrían ser peligrosos para su información, como ataques informáticos, brechas de seguridad, desastres naturales u otros problemas que podrían dañar su tecnología y datos.

Vulnerabilidades: Estas debilidades podrían ser, por ejemplo por espiritualizaciones, formas ineficientes de mantener segura la información o sistemas.

3.4 Administración de riesgos

Se verifica la identidad de los usuarios que intentan acceder a su información, mediante la implementación de medidas de

seguridad para proteger los datos. Esto se hace para mantener la información de los usuarios segura de manera efectiva y eficiente.

3.5 Incidentes de seguridad

Son problemas o situaciones en las que pueden ocurrir en los servidores de la organización. Incluye ataques como hackers, problemas de seguridad de la información o situaciones similares que pueden dañar la seguridad de la empresa.

3.6 Propietarios de la información

Son unidades académicas responsables que recopilan información, con competencia jurídica para administrar y disponer de su contenido.

4) Seguridad del Personal

4.1_ Seguridad en la definición de puestos de trabajo y asignación de recursos.

Se garantizar que los empleados tengan acceso a los recursos necesarios para llevar a cabo sus tareas de manera segura. Esto implica considerar aspectos como la formación necesaria, y la provisión de equipo.

4.2_ Capacitación de los Usuarios.

El objetivo principal de es garantizar que los usuarios sean capaces de operar estas el sistema de manera competente, lo que mejora la productividad y minimiza la posibilidad de errores.

4.3_ Respuesta a incidentes o anomalías en materias de seguridad.

Acciones tomadas para abordar y solucionar situaciones anómalas o eventos de seguridad, como violaciones de datos o intrusiones. Implica detectar, evaluar, mitigar y aprender de estos incidentes para prevenir futuros problemas y proteger la seguridad de la información y sistemas.

5) Control de Acceso

5.1_ Responsabilidad del usuario.

Los usuarios debe crear contraseñas seguras y únicas para su cuanta, implica la utilización de letras, números, símbolos y caracteres especiales así como realizar el cambio de las contraseñas periódicamente

5.2_ Monitoreo del acceso y uso del sistema.

Autenticación y Autorización: Implementación de sistemas seguros de autenticación para permitir el acceso solo a personas autorizadas mediante credenciales como nombres de usuario y contraseñas.

Registro de Acceso: Llevar un registro detallado de intentos de acceso, incluyendo información sobre quién, cuándo y desde dónde intenta acceder.

Auditorías y Supervisión Continua: Realizar auditorías periódicas para revisar quién ha accedido a los sistemas y qué actividades han realizado, lo que permite detectar y responder a actividades inusuales.

Control de Permisos: Administrar permisos de acceso, asignando a cada usuario un conjunto específico de privilegios que determina qué partes del sistema pueden utilizar y qué acciones pueden llevar a cabo.

Acceso Basado en Roles: Emplear un enfoque de acceso basado en roles para asignar permisos según las responsabilidades laborales de los usuarios, garantizando que solo accedan a la información necesaria.

Detección de Intrusiones: Utilizar sistemas de detección de intrusiones para identificar comportamientos anómalos en el acceso y uso de los sistemas y tomar medidas contra actividades sospechosas.

Formación y Concientisación: Proporcionar formación a los empleados sobre políticas de seguridad y mejores prácticas para el acceso y uso de sistemas.

Cumplimiento Normativo: Asegurar el cumplimiento de regulaciones de privacidad y seguridad de datos, lo que puede requerir un monitoreo riguroso del acceso y uso del sistema para demostrar el cumplimiento.

5.3_ Cumplimiento de requisitos legales

Regulaciones de Privacidad de Datos: Leyes de privacidad que regulan la recopilación, almacenamiento y uso de datos personales de usuarios y conductores de acuerdo a las normativas aplicables.

Seguridad de la Información: Cumplir con los estándares y regulaciones de seguridad de la información para proteger los datos y el sistema de amenazas y riesgos de seguridad.

Cumplimiento Fiscal y Laboral: Adherencia a leyes fiscales y laborales, incluyendo impuestos y regulaciones laborales para conductores y empleados.

Licencias y Permisos: Asegurar que los conductores tengan las licencias y permisos necesarios para operar legalmente en las áreas donde prestan servicios.

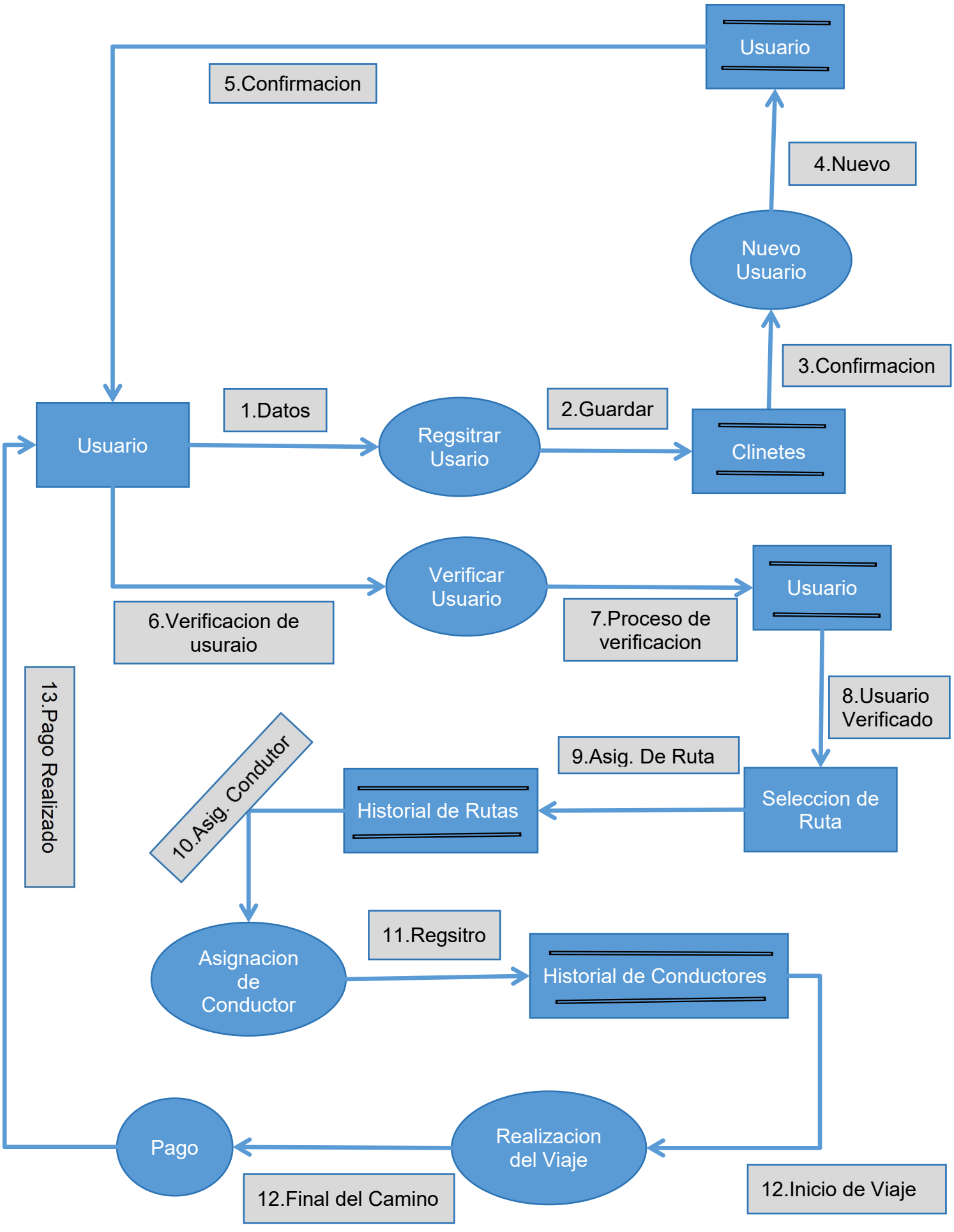
Derechos de los Trabajadores: Cumplir con regulaciones laborales relacionadas con la remuneración, beneficios y otros derechos de los trabajadores.

Antidiscriminación y Accesibilidad: Cumplimiento de leyes que prohíben la discriminación y garantizan la accesibilidad para personas con discapacidades.

Seguridad Vehicular: Cumplir con las regulaciones de seguridad del vehículo para garantizar los estándares de seguridad.

Licencias de Operación: Asegurar que la empresa cuente con las licencias necesarias para operar servicios de transporte en las áreas geográficas donde está presente.

DFD (Diagrama de Flujo)



Glosario

Esporádicas: Ocurren de vez en cuando, pero no con regularidad.

Antidiscriminación: Acciones o medidas que buscan prevenir o detener la discriminación, trato injusto o prejuicios hacia ciertas personas o grupos.

Hackers: Personas que pueden acceder a sistemas informáticos de manera no autorizada, ya sea con fines buenos o maliciosos.

Cibernéticos: Relacionados con la tecnología y sistemas de información en línea.

Mitigar: Reducir o minimizar los riesgos o problemas.