James Lake 201531545 Juan Felipe Sanchez 201618582 4 de Noviembre, 2019

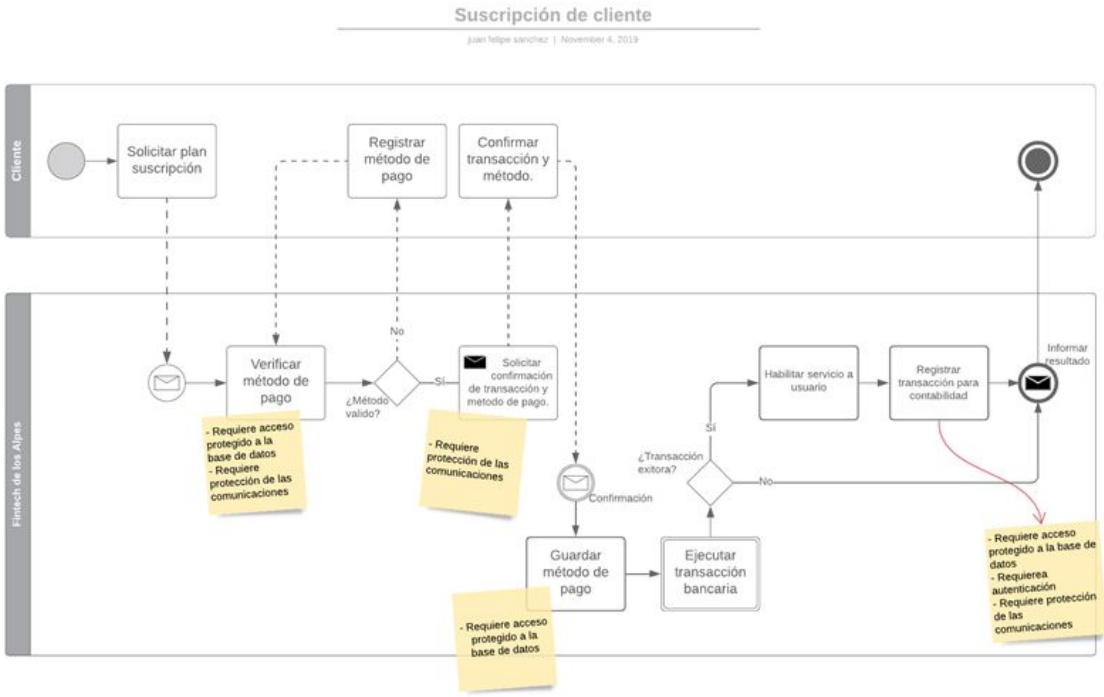
Entrega Caso 1 - Arquitectura de Seguridad

1. Construya la capa contextual:

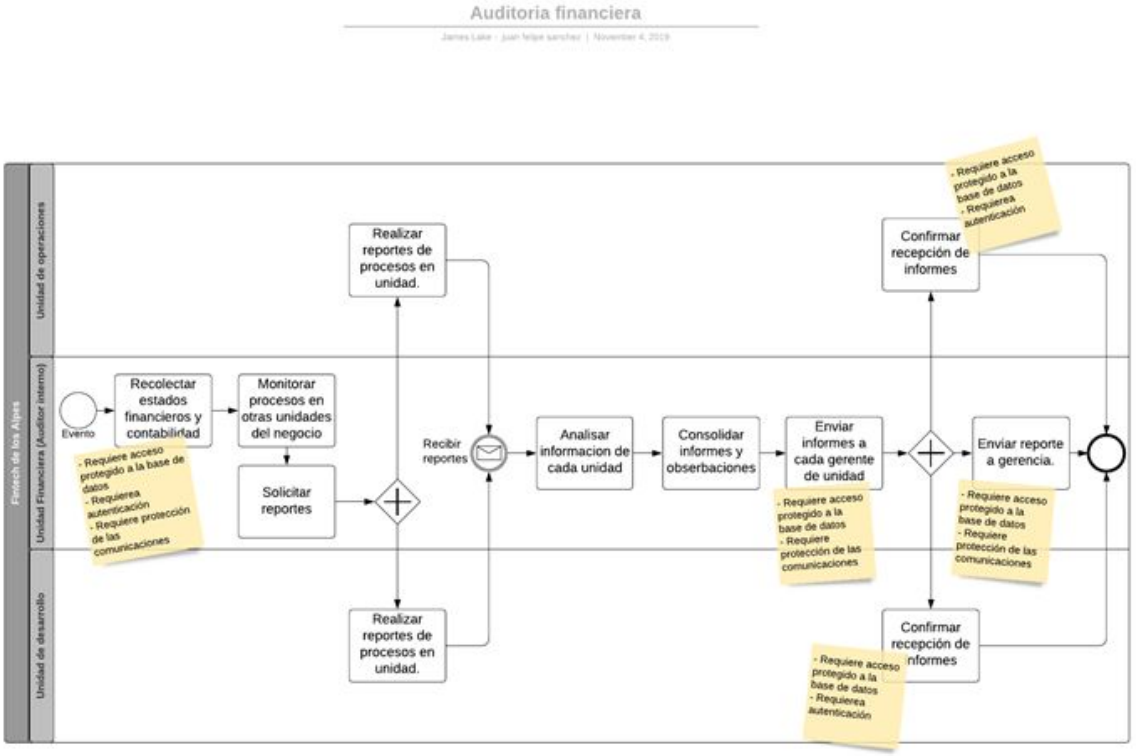
- **Modelo de negocio (motivadores de negocio)**

Motivador	Justificación
Motivador 01: Servicio de pagos con todos los bancos	Fintech debe manejar los pagos de transacciones con todos los bancos para sus apps.
Motivador 02: Investigación y Desarrollo de nuevas apps	Fintech quiere desarrollar nuevas soluciones para el mercado financiero que extiendan su alcance con los clientes. Promover el uso de las apps con nuevas funcionalidades.
Motivador 03: Protección de la marca	Darle seguridad a los clientes que las apps de Fintech valen la pena para que nuevos clientes lleguen por voz a voz. La reputación de la empresa es vital para las métricas.
Motivador 04: Protección de datos de los clientes	Las cuentas de los bancos de los usuarios son información muy sensible, y vital de proteger. Necesidad de cumplir todos los cumplimientos legales.
Motivador 05: Obligaciones Legales	Fintech debe cumplir con lo establecido por la Ley Colombiana: protección de datos personales, manejo de facturas de las compras, historial de transacciones, y demás.

- **Modelos de procesos:**
    - **Suscripción de clientes:** Enlace a diagrama



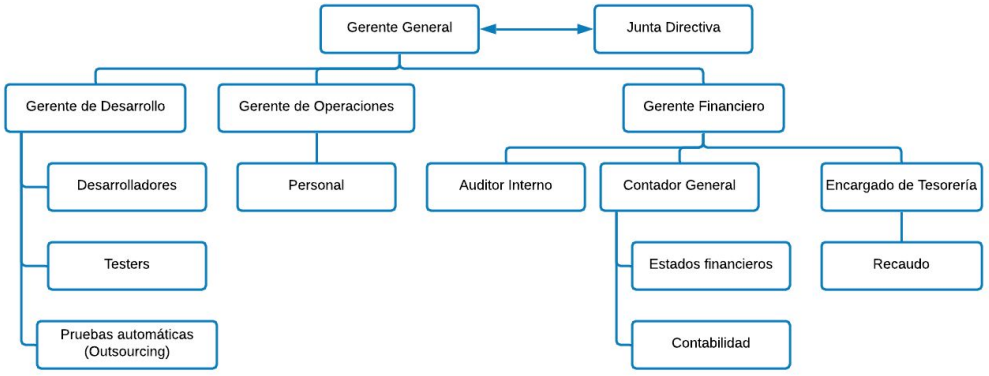
- **Auditoría financiera:** Enlace a diagrama



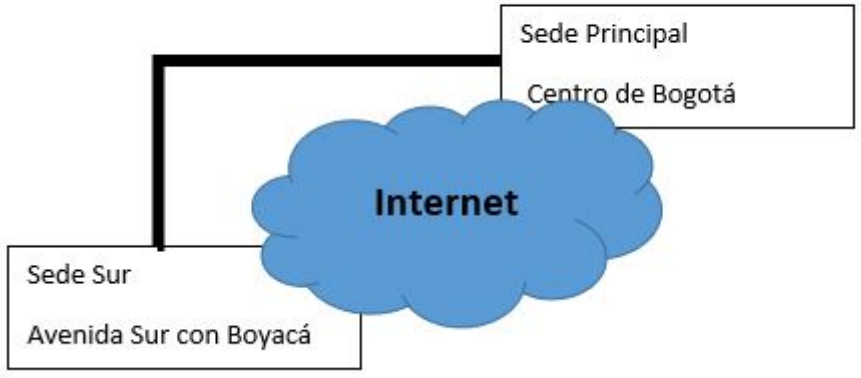
- **Modelo de organización y relaciones (estructura jerárquica):**
    - Enlace a diagrama

ORGANIGRAMA

James Lake - juan felipe sanchez | November 4, 2019



- **Modelo de geografía:**



- **Modelo de tiempo:**
  Tiempo de almacenamiento de transacción
  Tiempo de realización de transacción
  Tiempo de vida de la llaves de cifrado
  Tiempo de respuesta de app
  Tiempo de conexión entre las dos sedes
  Tiempo de autorización y validación de compra.
- **Modelo de riesgos (con base en NIST SP 800-30r1):**
    a. **Amenazas - Adversarios**

Id.	Fuente de amenaza	En el alcance	Capacidad	Intención	Objetivo

FA1	Empleado con privilegios	Si	Alta	Baja	Alto
FA2	Empleado con permisos	Si	Moderada	Baja	Alto
FA3	Atacante Externo	Si	Alta	Alta	Moderado

b. Amenazas - No adversarios

Id.	Fuente de amenaza	En el alcance	Rango
FA4	Accidental: Usuario con privilegios/administrador del sistema	Si	Alto. Si un usuario con privilegios o administrador accidentalmente puede comprometer todo el sistema.
FA5	Estructural: Comunicaciones	Si	Alto. El esquema de comunicaciones contiene información sensible. Cualquier fallo puede ser catastrófico.
FA6	Estructural: Procesamiento	Si	Alto. Un fallo en los servidores de procesamiento puede llevar a que no se puedan prestar lo servicios de las apps.
FA7	Estructural: Almacenamiento	Si	Moderado. Las versiones de desarrollo de las apps nuevas y la información de las transacciones, si no están en la nube, pueden dañarse o perderse de manera irremediable si se presenta un fallo en los servidores de almacenamiento.
FA8	Software: Aplicación misional	Si	Baja. En el caso que el software interno para manejo de transacciones presente irregularidades, puede interrumpir el servicio de la compañía.

FA9	Ambiental: Fallos de infraestructura	Si	Bajo. Las instalaciones y las sedes pueden ser afectadas por fallos estructurales, que perjudiquen las condiciones regulares de trabajo.

c. Eventos de amenaza

Id	Evento de amenaza	Fuente de Amenaza	Relevancia
AM1	Sniffing de la red, servicios y puertos expuestos.	Atacante Interno	Esperado
AM2	Realizar reconocimiento y vigilancia sobre organizaciones específicas	Atacante Externo	Anticipado
AM3	Ataques por Phishing	Atacante Externo	Posible
AM4	Distribución de malware a sistemas de organización internos (virus via email)	Atacante Interno	Posible
AM5	Distribución de malware objetivo para controlar sistemas de información y filtrar información	Atacante interno de confianza	Posible
AM6	Entregar malware al proporcionar medios extraíbles.	Atacante Externo	Posible
AM7	Insertar malware especializado en los sistemas de información de la organización con base en las configuraciones del sistema	Atacante interno con privilegios	Posible
AM8	Aprovechar vulnerabilidades conocidas en sistemas móviles	Atacante Externo	Posible

AM9	Comprometer sistemas de información críticos	Atacante interno	Posible
AM10	Mal manejo de información crítica o sensible por usuarios autorizados.	Atacante Interno	Posible
AM11	Configuración incorrecta de sistemas de información	Estructural	Posible
AM12	Desastres Naturales en sedes	Ambiental	Posible

d. Vulnerabilidades

Id	Vulnerabilidad
V1	Políticas de seguridad no definen el manejo seguro de la información.
V2	Las comunicaciones entre las sedes viajan a través de la internet y no un canal dedicado
V3	No se conoce una definición sobre usuarios privilegiados, y quién maneja qué riesgos.
V4	La compañía no cuenta con un plan de continuidad de la operación de TI.
V5	Irregularidades en los servicios de electricidad.
V6	Manejo de información sensible sin especificar la fortaleza de los protocolos de cifrado.

e. Condiciones de Predisposición

Id	Condición de predisposición	Condición

C1	Información: Información controlada identificable y no clasificada	Moderada
C2	Técnico: Soluciones de colaboraciones (código)	Bajo
C3	Operacional: Sitio Fijo	Alto

f. Impactos Adversos

Tipo de Impacto	Impacto	Máximo Impacto
Daño a las operaciones	Inhabilidad de desarrollar funciones empresariales o misionales	Alto
	Daños dado a no cumplimiento	Alto
	Costos financieros o relacionales	Moderado
Daños a los Activos	Daño a sistemas de información o redes	Alto
	Daño a las sedes físicas	Alto
Daño a los individuos	Pérdida de información sensible	Muy Alto
	Robo de identidad	Muy Alto
Daño a otras organizaciones	Daños dado a no cumplimiento	Muy Alto

g. Riesgos - Adversarios

Id	Amenaza	Fuente	Relevancia	Probabilidad	Vulnerabilidades	Criticidad	Probabilidad de	Probabilidad	Nivel de	Riesgo

				de Ataque			ataques exitosos	General	Impacto	
R1	AM1	FA1, 2, 3	Esperado	Alta	Bajo	Bajo	Mod.	Bajo	Mod.	Bajo
R2	AM2	FA3	Anticipado	Mod.	Mod.	Mod.	Alto	Mod.	Mod.	Moderado
R3	AM3	FA3	Posible	Alta	Alta	Mod.	Alta	Alta	Mod.	Alto
R4	AM4	FA1, 2, 3	Posible	Baja	Alta	Alta	Alta	Mod.	Muy Alto	Moderado
R5	AM5	FA1, 2	Posible	Baja	Mod.	Mod.	Alta	Mod.	Bajo	Bajo
R6	AM6	FA3	Posible	Alta	Alta	Alta	Muy Alta	Alta	Alto	Alto
R7	AM7	FA1	Posible	Mod.	Mod.	Alta	Mod.	Mod.	Mod.	Moderado
R8	AM8	FA3	Posible	Mod.	Muy Alto	Alta	Alta	Alta	Alto	Alto
R9	AM9	FA1	Posible	Mod.	Mod.	Alta	Alta	Alta	Mod.	Moderado

h. Riesgos - No adversarios

Id	Amenaza	Fuente	Rango de	Probabilidad de	Vulnerabilidades y Condicion	Criticidad	Probabilidad que	Probabilidad	Nivel de	Riesgo

			Efectos	Ocurrencia	es de Predisposición		resulte en impacto adverso	General	Impacto	
R10	AM10	FA4	Alto	Mod.	Mod.	Alta	Alta	Alta	Alta	Alto
R11	AM11	FA5, 6, 7, 8	Mod.	Mod.	Mod.	Alta	Mod.	Mod.	Mod.	Moderado
R12	AM12	FA9	Mod.	Bajo	Bajo	Alta	Alta	Mod.	Mod.	Bajo

2. Construya la capa conceptual:

- **Perfil de atributos (SABSA)**

- **Objetivos de control (Propios y/o COBIT):**

Base de la definición	**Id.**	**Objetivo**
Atributo: privacidad, compliant, regulado, legal	OBJ1	Establecer procedimientos para proteger la información de los clientes, en cualquiera de los estados de acuerdo con la legislación Colombiana.
Atributo: integridad	OBJ2	Todos los sistemas y aplicaciones de la organización deben implementar técnicas para cumplir con los estándares de integridad.
Atributo: Disponible	OBJ3	Definir e implementar estrategias para prevenir fallas en equipos por flujo de energía irregular.
Atributo: Disponible	OBJ4	Definir e implementar estrategias para responder ante fallas en equipos por flujo de energía irregular.
Atributo: Disponible	OBJ5	Establecer acuerdos de niveles de servicio con proveedores externos de servicios y con la unidad operacional para responder a la disponibilidad mínima esperada.

Análisis de riesgos: R-8	OBJ6	Definir e implementar estrategias para prevenir ataques a través de dispositivos móviles de usuarios.
Análisis de riesgos: R-6	OBJ7	Definir e implementar estrategias al interior de la organización para evitar la entrada de malware a través medios extraíbles.

- **Estado actual:**

Base de la definición	**Id.**	**Objetivo**	**Estado**
Atributo: privacidad, compliant, regulado, legal	OBJ1	Establecer procedimientos para proteger la información de los clientes, en cualquiera de los estados de acuerdo con la legislación Colombiana.	No se cumple (Se cumple solo parcialmente)
Atributo: integridad	OBJ2	Todos los sistemas y aplicaciones de la Organización deben implementar técnicas para cumplir con los estándares de integridad.	No se cumple (Se cumple solo parcialmente)
Análisis de riesgos: R-XX mala energía en la zona.	OBJ3	Definir e implementar estrategias para prevenir fallas en equipos.	No se cumple
Análisis de riesgos: R-XX mala energía en la zona.	OBJ4	Definir e implementar estrategias para responder ante fallas en equipos.	No se cumple
Atributo: Disponible	OBJ5	Establecer acuerdos de niveles de servicio con proveedores externos de servicios y con la unidad operacional para responder a la disponibilidad mínima esperada.	Si Se cumple
Análisis de riesgos: R-08	OBJ6	Definir e implementar estrategias para prevenir ataques a través de dispositivos móviles de usuarios.	No se cumple
Análisis de riesgos: R-6	OBJ7	Definir e implementar estrategias al interior de la organización para evitar la entrada de malware a través medios extraíbles.	No se cumple

- **Modelo de dominios:**

Dominio	**Descripción**

Unidad de Desarrollo	Esta unidad tiene acceso a información de los recursos tecnológicos y procesos internos de la unidad.
Unidad de manejo operacional	Esta unidad tiene acceso a información administrativa como información de empleados, clientes, estados de procesos y recursos tecnológicos.
Unidad de manejo financiero	Esta unidad tiene acceso la información financiera y de contratos.
Sede principal	En esta sede maneja información de todas las unidades de negocio.
Sede al sur de la ciudad	Esta sede tiene acceso principalmente a la información que maneja la unidad de desarrollo.
Servidor local	En este servidor se maneja toda la información persistente de la empresa (financiera, administrativa y operacional)
Clientes	El cliente consume servicio de la aplicación por suscripción.

- **Tiempos y plazos:**
    - **Tiempo de almacenamiento de datos de cliente inactivo. Debido a las responsabilidades legales de quien recolecta y mantiene datos de los clientes, si un cliente ya no es activo, es mejor eliminar el registro y reducir la responsabilidad. Se entiende por inactivo al cliente que no cuenta con una suscripción activa tras un tiempo de expiración de un año.**
    - **Tiempo de inactividad de una sesión iniciada antes de ser bloqueada. Para impedir un futuro acceso al sistema por un usuario no autorizado se bloquea la sesión de cada usuario después de [10 min] de inactividad o al recibir una solicitud de un usuario.**
    - **Tiempo de vida de las llaves de cifrado. El tiempo de vida para las llaves simétricas de sesión: una sesión, Públicas/privadas: 1 año [NIST SP 800-57].**
    - **Tiempo de consolidación de datos del día. Los datos sobre los que trabaja cada unidad en la segunda sede debe consolidarse en batch al final del día y debe terminar antes del inicio de operación al día siguiente. El tiempo de respuesta debe ser menor a 8 horas.**
    -
- **Modelo de entidades y confianza:**

Entidades	
Roles	Gerente general

	Gerente de Desarrollo
	Gerente de Operaciones
	Gerente financiero
	Desarrolladores
	Administrador de servicios y aplicaciones
	Auditor financiero
	Contador General
	Tesorero
	Personal unidad operacional
	Cliente registrado
Aplicaciones	Aplicación para manejo de personal operativo
	Aplicación de manejo de estados financieros y contabilidad
	Servidor de procesamiento de transacciones
	Aplicación para manejo de equipo de desarrollo
	Aplicación para manejo de equipo de investigación

Relaciones
El gerente general puede leer/generar reportes consolidados en las aplicaciones para manejo de personal, de desarrollo, de investigación y de contabilidad. (U)
El gerente de desarrollo puede leer y generar reportes consolidados en las aplicaciones para manejo de personal, de equipo de desarrollo y de investigación. (U)
El gerente operativo puede leer/generar reportes consolidados de las aplicaciones para manejo de personal. (U)
El gerente financiero puede leer/generar reportes consolidados en las aplicaciones para manejo de personal, de desarrollo, de investigación y de contabilidad. (U)
El desarrollador puede leer y actualizar la información (manejada por su equipo) en la aplicación de manejo de equipos de desarrollo y de investigación. (B)
El auditor financiero puede leer y generar reportes en las aplicaciones para manejo de personal, de desarrollo de investigación y de contabilidad. (U)

El contador general puede leer y generar reportes consolidados de las aplicaciones para manejo de estados financieros y contabilidad. (U)
El tesorero puede leer y actualizar la información de las aplicaciones para manejo de contabilidad. (B)
Cualquier empleado de la unidad operacional puede leer y actualizar la información (que corresponde a sus funciones y sucursal) en la aplicación de manejo de personal operativo. (B)
El usuario cliente del servicio de suscripciones de app puede leer y actualizar sus datos registrados, consultar planes de suscripción y administrar renovaciones automáticas sobre sus planes. (B)
El administrador de aplicaciones y servicios puede leer y actualizar la configuración de las aplicaciones y los servidores. (B)

Confianza	
A. Sin confianza	La consulta de planes de suscripción en la aplicación no requieren ningún tipo de autenticación.
B. Nivel medio de confianza	Todos los empleados de la organización requieren autenticación para acceso a las aplicaciones y servicios. Las aplicaciones deberán correr con identificadores establecidos y deberán autenticarse para ganar acceso a otras aplicaciones y servicios.
C. Nivel alto de confianza	Administradores de aplicaciones y servicios. Los administradores asumen rol de confianza para todos los usuarios de la organización

- **Estrategia de seguridad y arquitectura:**

Estrategia	**Parte**	**Descripción**
Manejo de incidentes en capas	Servicios de prevención	
	Servicios de detección y notificación	
	Servicios de contención	

	Servicios de recuperación	
	Servicios de restauración	