**INGENIERÍA DE SEGURIDAD US**
**E.T.S. Ingeniería Informática. Universidad de Sevilla**
Avda Reina Mercedes s/n. 41012 Sevilla

# PAI-5. MOBIFIRMA. DESARROLLO DE PILOTO PARA COMPRAS CON DISPOSTIVOS MÓVILES PARA UNA CORPORACIÓN HOTELERA INTERNACIONAL

## Introducción

Una gran corporación internacional hotelera le ha planteado a INSEGUS, dentro del **PLAN DE DIGITALIZACIÓN** que tienen establecido, una arquitectura software piloto; entendida ésta como un **mínimo producto viable (MVP**), para dar soporte a dos actividades de interés para la corporación:

1. **Peticiones a través de dispositivos móviles de las compras de recursos hoteleros** por parte de los diferentes centros hoteleros de esta corporación y que se encuentran establecidas en todo el mundo.

Parra llevar a cabo el proyecto debemos tener en cuenta la **"Política de Peticiones Seguras, a ravés dispositivos móviles, de recursos materiales de forma autenticada, confidencial e integra en la corporación para el abastecimiento de los centros hoteleros"** que indica que se debería cumplir lo siguiente:

***"Todos los mensajes desde los dispositivos móviles sobre peticiones de compras de material hostelero deberán ir firmados por el responsable de la petición y transmitirse de forma confidencial e íntegra. Cada mes el Gobierno de la Seguridad de la Información de la corporación debe ser informado de los porcentajes de peticiones verificadas correctamente su firma y de las tendencias con respecto a los dos meses anteriores."***

Por parte del cliente no se confía en la seguridad proporcionada por las tecnologías de seguridad establecidas en **3G-UMTS, 4G-LTE y 5G** por ello nos han pedido mejorar la seguridad de la ***capa de aplicación*** para poder desarrollar y cumplir la Política De Seguridad propuesta.

## Objetivos del proyecto

Por tanto, se propone al Security Team alcanzar los objetivos siguientes:

1. **Arquitectura cliente/servidor *Piloto* para las compras electrónicas en la corporación.** Desarrollar/Desplegar la arquitectura **cliente/servidor** que permita ***mensajería autenticada mediante firma digital*** con dispositivos móviles con el sistema operativo **Android** que permita firmar las peticiones de compra en el cliente y **verifique dicha firma en el servidor. La transmisión por las redes públicas debe ser autenticada, confidencial e íntegra.**
2. **El servidor debe recoger además de las peticiones de compras, la información necesaria para los indicadores exigidos en la Política de Seguridad Corporativa** para que pueda usarse por el Gobierno de la Seguridad de la información de la Corporación respecto a **la incorrecta autenticación de los clientes**.

## Recomendaciones

### Diseño de arquitectura Cliente/Servidor Piloto

Se necesita implementar el servidor y el gestor de bases de datos correspondiente, incluyendo las correspondientes tablas para almacenar todos los certificados digitales de los empleados (*su clave pública)* y las peticiones de material que realiza cada uno. Se supone que la empresa dispone ya una aplicación que es capaz de recoger todos los certificados digitales de los clientes en dicha base de datos (clave pública de cada uno de ellos). La empresa utiliza **SQLite** como sistema de gestión de bases de datos relacional para este sistema, por lo que cualquier cambio con respecto al sistema de gestión de bases de datos debería ser consultado con la empresa para su aprobación. **Hay que procurar el uso de un protocolo que permita la transmisión segura de los pedidos.**

El servidor deberá responder a las peticiones de los empleados con un mensaje en la pantalla de ***Petición OK*** o ***Petición INCORRECTA***. **La petición incorrecta viene determinada por una entrada invalida o por la verificación de la firma inválida**. Se debe evitar en el servidor que se hagan múltiples peticiones (**no más de 3 en 4 horas**) al servidor para evitar los ataques de fuerza bruta.

**Android Studio** es el IDE de desarrollo oficial para desarrollar aplicaciones Android, esta herramienta nos puede servir para construir, testear y depurar aplicaciones para Android. Desde el propio IDE se pueden crear proyectos para Android y ejecutarlos en un emulador que se puede configurar o en el dispositivo móvil conectado al equipo de desarrollo.

Por lo general una aplicación Android usa una ***Activity*** como medio por el cual un usuario de dispositivo móvil interactúa con la aplicación. Las ***Activities*** se encargan entre otras cosas de crear una ventana donde el desarrollador puede plasmar el diseño y el control de la interfaz de usuario y además constituyen la parte lógica de la aplicación.

La empresa cliente nos ha solicitado desarrollar una aplicación cliente para dispositivos Android que permita a través de la correspondiente interfaz (ver mockup en la imagen anterior) realizar **pedidos de material hotelero y que éste pueda ser firmado por el correspondiente peticionario, además de facilitar al receptor del pedido (servidor/responsable de compras) los medios correspondientes para que pueda verificar la autenticidad del mensaje enviado.**

En los campos de texto al lado de cada artículo se espera un número entero positivo comprendido entre 0 y 300. Se debe realizar una **validación de todos los parámetros de entrada que escogen los empleados en la interfaz.**

El Gobierno de la Seguridad de la Información de la Corporación necesita conocer si las medidas impulsadas por la Dirección se están llevando a cabo. Parar ello se ha propuesto los siguientes **indicadores la ratio de los pedidos recibidos por el servidor cuya firma ha sido verificada correctamente/peticiones realizadas y la tendencia mensual respecto a los dos meses anteriores,** para medir la tendencia se usa los siguientes criterios:

- Si la ratio de los dos meses anteriores es menor o una es menor y otra igual al actual **TENDENCIA POSITIVA**
- Si alguna de las ratios de los dos meses anteriores es mayor al actual **TENDENCIA NEGATIVA**
- Si las ratios de los dos meses anteriores es igual al actual **TENDENCIA NULA**

Todo ello se **recogerá en un fichero de texto donde en cada línea aparecerá el nombre del mes y año, el valor de la ratio mensual y un carácter (+, -, 0) para representar la tendencia (las dos primeras tendencias serán 0), que podrá ser consultado por el Gobierno de la Seguridad de la información (la aplicación de consulta de los informes ya está implementada por tanto no es necesaria su implementación).**

**NOTA de INSEGUS: Es muy importante que la aplicación cliente no pueda realizar cualquier tipo de ataque son la aplicación servidora, por tanto, es necesario la validación de todas las entradas, suplantación de la identidad de los empleados y evitar los ataques de DoS sobre ella.**

## Normas del entregable

- Cada grupo debe entregar a través de la Plataforma de Enseñanza Virtual y en la **actividad** preparada para ello un archivo zip, nombrado ***PAI5-SecurityTeamX*.zip**, que deberá contener al menos los ficheros siguientes:
  - ✓ **Documento en formato pdf que contenga un informe/resumen del proyecto** con los detalles más importantes de las decisiones, soluciones adoptadas y/o implementaciones desarrolladas, así como el resultado y análisis de las pruebas realizadas (máximo 10 páginas).
  - ✓ **Código fuente de las implementaciones y logs de las pruebas, así como los scripts y/o configuraciones para poner en marcha el proyecto.**
- Los proyectos entregados fuera del plazo establecidos serán considerados inadecuados por el cliente y por tanto entrarán en penalización por cada día de retraso entrega de 5% del total, hasta agotarse los puntos.
- **El cliente no se aceptará envíos realizados por email, ni mensajes internos de la enseñanza virtual, ni correo interno de la enseñanza virtual.**

## Métricas de valoración

Para facilitar el desarrollo de los equipos de trabajo el cliente ha decidido listar las métricas que se tendrán en cuenta para valorar los entregables de cada grupo de trabajo:

- **Resumen (30%)**
    - Tamaño del informe
    - Calidad del resumen aportado
    - Calidad de pruebas presentadas y resultados
- **Solución aportada (70%)**
    - Cumplimiento de requisitos establecidos
    - Calidad del código entregado
    - Complejidad de la solución
    - Respuesta al conjunto de preguntas planteadas
    - Pruebas realizadas