



ESPECIFICACIONES TÉCNICAS: Desarrollo de APP compatible con Android/IOS

1. NOMBRE DEL PROCESO

Desarrollo de APP compatible con Android/IOS

Debe contar con los siguientes módulos:

- ❖ Módulo de Información general de la institución
- ❖ Sistema de Identidad Digital Soberana
- ❖ App de usuario dual
- ❖ Web de Operaciones
- ❖ Arquitectura con CDM Nativo (Ciberseguridad basada en Continuous Diagnostic and Mitigation) y AutoML (Auto Machine Learning)

2. OBJETIVO DE LA CONTRATACIÓN

Viabilizar los procesos internos de Supérate en todo lo que concierne a las familias que son beneficiarias del programa.

3. TIEMPO DE ENTREGA

Cinco (5) días luego de colocada la orden de compra.

4. LUGAR DE ENTREGA DEL SERVICIO

Entrega vía remota.

5. ESPECIFICACIONES TÉCNICAS

Debe contener un sistema de identidad soberano con las características:

- Sistema de identidad Biométrico:
- Garantice un onboarding digital, es decir, sin necesidad de presencia física del cliente en ninguna oficina.
- Que pueda hacer una captura de la biometría de la cara del cliente.
- Que pueda hacer una captura de la Cédula de Identidad y todos los datos de filiación del cliente.
- Que pueda realizar una comparación entre sí las caras de la fotografía del cliente, de la cédula escaneada y de la imagen de la cédula que reside en la JCE.
- Que nos permita tener una validación de vida para verificar que la persona que se está conectando es realmente ella y que no está siendo suplantada por una fotografía en tamaño natural que se esté utilizando para engañar al modelo.

❖ Sistema criptográfico de generación de QR alta seguridad

- Permite establecer un pago seguro entre los teléfonos del comprador y del vendedor, asegurando que las transacciones están garantizadas.
- Generación de Código QR de alta seguridad que permita establecer un pago seguro con establecimientos que puedan hacer uso de una tecnología que permita escanear el mismo y generar un pago a través de dicho Código.

❖ App de usuario dual

- La aplicación se ha desarrollado sobre una plataforma de verificación de debilidades de ciberseguridad que elimina las debilidades conocidas de código.
- El acceso a la aplicación para realizar pagos está controlado por el uso de usuario y contraseña que se entrega a los usuarios en el momento del alta.



❖ La aplicación de comprador permite:

- Conocer en todo momento cuál es tu saldo restante. A diferencia de un sistema basado en tarjeta, en el que el usuario va gastando y no sabe nunca realmente cuál es su saldo.
- Puede revisar todas las compras realizadas hasta la fecha.
- Realiza, leyendo el QR que le presenta el vendedor, la aceptación del pago un click.
- Si hubiera problema de iluminación o de rotura de la cámara del comprador, el pago se puede hacer metiendo el código de seis dígitos de verificación de compra que le dé el vendedor.

❖ Web de Operaciones

★ Reportes

- Se realizan diariamente reportes consolidados de las ventas por cada comercio y de las compras por cada cliente.
- Se realizan diariamente los archivos de contabilidad para la generación de la liquidación nocturna con cada comercio.

❖ Arquitectura de Microservicios Lambda

- La Arquitectura de Microservicios está desarrollada en Python y corre en AWS, con todas las medidas de seguridad nativas de Amazon.
- Tiene cifradas por VPN punto a punto la comunicación entre la Arquitectura y la Web de Operaciones, impidiendo el acceso a la Arquitectura desde este cualquier punto que no esté dentro de la red de Operaciones.
- Verifica la identidad de todas las peticiones que llegan desde el App, asegurando que ningún cliente ni vendedor puede consumir recursos o hacer compras que no sean suyas.
- La arquitectura se nutre de un modelo de datos que se gestiona sobre Elastic.
 - 🚩 Esta característica le permite incorporar de manera nativa funcionalidades de Inteligencia Artificial basada en los modelos de Auto Machine Learning (AutoML) nativos de Elastic.

- Detección de comportamientos anómalos basados en AutoML.
 - ✚ La arquitectura incorpora de manera nativa un conjunto de modelos de Machine Learning preparados para detectar comportamientos anómalos en los patrones de compra y en los patrones de venta. Esto permite anticiparse y/o detectar de manera temprana posibles modelos de fraude que puedan darse alrededor del proceso Supérate.
- Mecanismos de ciberseguridad incorporado en la arquitectura para detectar posibles intrusiones y/o ataques de Ransomware.
 - ✚ Basados en el modelo CDM (Continuos Diagnostic & Mitigation) la plataforma está conectada a un SOC en la nube gestionado por una empresa internacional de servicios de monitorización de ciberseguridad.



Ronald Fernando Lebron Peña

Director de Sistemas y Tecnología de la Información.

