ESPECIFICACIONES TÉCNICAS
PROYECTO IMPLEMENTACIÓN
DE SOFTWARE ANTIFRAUDE – PROYECTO VISA

1. DESCRIPCIÓN DE LA SOLUCIÓN TECNOLÓGICA

Caja Municipal de Ahorro y Crédito de Trujillo S.A., requiere implementar en la Institución un software antifraude, que permita:

- Detectar posible riesgos de fraude en medios de pago con tarjetas de débito.
- Predecir en forma oportuna la ocurrencia de eventos relacionados con fraudes.
- Detectar patrones ocultos en comportamientos de fraude
- Capacidad de alertar a un grupo de funcionarios, en base al nivel de severidad de la alerta.
- Utilizar información relacionada al comportamiento del cliente o tarjetahabiente (total, por país, por tipo de establecimiento y por código de establecimiento)

2. ESPECIFICACIONES TÉCNICAS

I. ASPECTO FUNCIONALES

El software Antifraude debe contar con la siguiente funcionalidad:

- El software debe realizar el procedimiento de consolidación de información automático.
- El software deber realizar análisis de datos en forma rápida y eficiente, incluyendo datos transaccionales en archivos de todos los tamaños, al 100 por ciento
- El software deber permitir detectar posible riesgos de fraude en medios de pago con tarjetas de debito de cualquier marca compartida.
- El software deber permitir alertar transacciones aprobadas iguales o menores a $X o U$Y (detectar pruebas con tarjetas activas)
- El software deber permitir alertar transacciones configurando límites y condiciones sobre las variables de la transacción: modo de entrada, código de respuesta, código único del comercio, etc. (relacionar las variables que permite filtrar).
- El software deber permitir alertar transacciones en comercios cargados previamente como negativos (por identificación única del comercio)
- El software deber permitir alertar compras inusuales, o retiros de dinero en cualquiera de los canales que la Caja Trujillo tenga según el comportamiento histórico del tarjeta-habiente
- El software debe predecir en forma oportuna la ocurrencia de eventos relacionados con fraudes, de acuerdo a reglas modificables o definidas por el usuario.
- Detectar patrones ocultos en comportamientos de fraude por tarjeta-habiente y la emisión de alertas en base al nivel de severidad
- El software debe permitir una diversidad de medios para enviar alertas
- El software debe contar con mecanismos de defensa capaces de tomar acciones tal como realizar bloqueos preventivos en tarjeta de débito, bloquear una cuenta. Capacidad de actuar en tiempo real.
- Generar reportes y listados tales como:
  - Número de transacciones realizadas en cierto período de tiempo por cliente, tarjeta, tarjeta y tipo de establecimiento, tarjeta y establecimiento, tarjeta y país, etc.
  - Montos acumulados de las transacciones realizadas en cierto período de tiempo por cliente, tarjeta, tarjeta y tipo de establecimiento, tarjeta y establecimiento, tarjeta y país, etc.

  - Tiempo en segundos de las últimas transacciones por cliente, tarjeta, tarjeta y tipo de establecimiento, tarjeta y establecimiento, tarjeta y país, etc.
  - Detalle de la última transacción por cliente, tarjeta, tarjeta y tipo de establecimiento, tarjeta y establecimiento, tarjeta y país, etc.

- El software debe permitir realizar la parametrización y definición de reglas altamente flexibles.
- El software debe incluir la funcionalidad del uso de técnicas de Workflow para seguimiento a casos

II. ASPECTOS OPERATIVOS

- Administración de casos para resolver investigaciones
- El software debe realizar análisis basado en reglas de negocio
- El software debe estar basado en técnicas de inteligencia artificial (Reglas adaptativas y secuenciales)
- El software debe ser adaptable y escalable a las necesidades actuales y futuras de CMACT
- El software debe contar con seguridad por perfiles de usuario.
- El software debe permitir realizar auditorías que guarde y permita evaluar los accesos al sistema, transacciones realizadas, actualizaciones con fecha, hora y usuario.
- El postor debe entregar manuales técnicos y de usuarios en forma impresa y digital. La versión debe ser en español. Así mismo debe contar con una ayuda en línea y manuales de autoaprendizaje en español.
- El postor debe proporcionar una guía con las principales reglas y parámetros para ajustar el modelo de detección de fraudes.

III.ASPECTOS TÉCNICOS

- La solución debe poder ser instalada en una plataforma de Windows 2000, XP, Vista y 2003
- Arquitectura Web ó cliente servidor
- La solución debe permitir la integración con la base de datos SQL Server 2000, 2005 de la institución.
- La solución debe ser adaptable al esquema tecnológico de CMAC-T

IV.ASPECTOS SOBRE EL PROVEEDOR

- Conocimiento del Sector financiero peruano e internacional
- El proveedor debe sustentar la implementación del software en al menos 5 empresas financieras peruanas.
- Conocimiento de antifraude en tarjetas.

V. ASPECTOS SOBRE EL SERVICIO

- Uso del software por tiempo indefinido. Es postor es el responsable de instalar debidamente los programas aplicativos de la solución en los equipos de la Caja Trujillo y de instalar las Interfaces necesarias para la interconexión entre los equipos del Software y el equipo a monitorearse tanto en el ambientes de desarrollo como el producción.
- La metodología de implementación debe estar debidamente comprobada.
- El postor debe entregar un cronograma con las actividades de la implementación.
- El equipo de proyecto por parte del postor deberá ser partícipe de las pruebas en el ambiente de desarrollo previas a la puesta en marcha.
- Tiempo de implementación debe ser menor o igual a 90 días calendario en CMAC-T
- El periodo de garantía debe ser mayor o igual a 120 días, posterior a la puesta en producción del producto
- Se debe capacitar a dos personas como mínimo del Dpto. de Tecnología de Información de CMAC-T, en el uso de la herramienta y 2 personas de la parte operativa.
- Experiencia del personal del proveedor para implementar el software bajo una metodología.
- Facilidad de mantenimiento del software por módulos.
- Durante el proceso de implementación el postor debe designar a un Gerente de Proyecto quien realizará al menos 3 visitas para el seguimiento de las actividades programadas en el cronograma.

- Soporte post implementación. En el caso de consultas se debe considerar el siguiente horario :
  - Lunes a Viernes de 9am - 6pm

- Servicio de mantenimiento de versiones el cual debe permitir tener el derecho a actualizaciones y nuevas versiones del software que el proveedor ponga a disposición de los clientes. Así como la absolución de dudas hasta por 4 veces al mes en el siguiente horario: L- V 9am – 6 pm – Horario Perú. El servicio también debe considerar la reparación de fallas en el software contratado. El periodo de vigencia mínima debe ser de 4 años y se debe iniciar posterior a la finalización del periodo de garantía.

- El postor debe ofrecer servicios de valor agregado tales como:

  - Acceso a información referente a fraudes de tarjeta de débitos y crédito
  - Descuentos especiales en licencias de nuevos productos del mismo proveedor.
  - Inscripción a un mínimo de dos personas de la Caja Trujillo en eventos relacionados con el Control y Gestión de Fraude en Tarjeta de Débito y Crédito.