ENUNCIACION DEL REQUERIMIENTO POR PARTE DEL BHU				DETALLE DE COBERTURA POR PARTE DEL OFERENTE		
CARÁCTERISTICA	**ID**	**DESCRIPCION DEL REQUERIMIENTO**	**OBLIGATORIO**	**FORMA DE COBERTURA**	**ANEXO**
INTERFAZ	**1**	La "interfaz" de usuario debe ser 100 % web para todos los tipos de usuarios	**SI**		
ESCALABILIDAD	**2**	La solución debe poder soportar un crecimiento en la cantidad de usuarios y la cantidad de transacciones manteniendo un nivel adecuado de rendimiento y calidad. Deberá soportar 200 usuarios concurrentes y una base de datos del orden de 1.000.000 clientes / prospectos.	**SI**		
RENDIMIENTO	**3**	La solución debe poder asegurar tiempos de respuesta adecuados para su correcto uso en todos los niveles de permisos y usuarios. Se pretende que la solución pueda asegurar un tiempo de respuesta no mayor a 5 segundos para un máximo de hasta 200 usuarios concurrentes, cumpliendo con la infraestructura de software y hardware de base necesaria. Para el caso de operaciones complejas (ej: reportes con gran cantidad de registros), el tiempo de respuesta no deberá ser mayor a 10 segundos. En caso de identificarse excepciones, se requiere especificar para qué casos no se cumplirán los mencionados tiempos de respuesta. El criterio de aceptación final será ajustado y aprobado en el marco de la definición del alcance del proyecto.	**SI**		
CONFIABILIDAD Y ESTABILIDAD	**4**	La solución debe ser estable y la información que maneja confiable. Para esto debe asegurar niveles de integridad, la NO pérdida de información y debe responder de una manera predecible y consistente frente a la ejecución de las funcionalidades que incluye.	**SI**		
USABILIDAD	**5**	La solución debe proveer niveles de usabilidad aceptables (de acuerdo a los estándares ISO/IEC 9241 y siguiendo los estándares definidos por Agesic en https://www.agesic.gub.uy/innovaportal/file/549/1/Capitulo_2_Usabilidad_v1_0.pdf). Debe cumplir con las siguientes características: • El sistema debe contar con manuales de usuario estructurados adecuadamente. • El sistema debe proporcionar mensajes de error que sean informativos y orientados al usuario final. • El sistema debe contar con un módulo de ayuda en línea.	**SI**		
ADAPTABILIDAD	**6**	La solución debe ser de diseño adaptable "responsive", por lo cual las "interfaces" de usuario se deben adaptar a distintos tipos de dispositivos (ejemplos celulares, tabletas, monitores de PC) ofreciendo las mismas funcionalidades de manera automática, sin requerir intervención del usuario.	**SI**		
ACCESIBILIDAD	**7**	Se desea que la solución cumpla nivel de accesibilidad AA y contemple las buenas prácticas del nivel AAA en base a la WCAG 2.0, siguiendo los estándares recomendados por AGESIC en la materia (https://www.agesic.gub.uy/innovaportal/file/549/1/Capitulo_3_Accesibilidad_v1_0.pdf)	**NO**		
EXTENSIBILIDAD Y MODULARIZACIÓN	**8**	La solución debe ser flexible y extensible mediante una arquitectura modular y de capas. Debe ser posible el desarrollo o implementación de módulos independientes para atender las distintas necesidades de negocio, sin interferir en las funciones generales del sistema. A su vez debe poder actualizarse mediante versiones que incorporen nuevas funcionalidades, parches de seguridad, actualizaciones y otras mejoras sin interferir con el correcto y adecuado funcionamiento del sistema.	**SI**		
INTEGRACIÓN	**9**	La solución debe ser capaz de intercambiar datos utilizando los estándares establecidos y debe poder comunicarse mediante los protocolos y formatos que se establezcan. Debe soportar Web Services como método de integración entre las aplicaciones, así como también la posibilidad de carga de información mediante procesos batch. Debe ofrecer Servicios SOAP y REST para integraciones.	**SI**		
IDIOMA	**10**	La solución debe proveer "interfaces" gráficas en idioma español.	**SI**		
RESPALDOS	**11**	La información debe poder ser respaldada y recuperada ante problemas de disponibilidad. Se debe proveer un esquema de respaldos para incluir en los procesos internos de resguardo de información del BHU.	**SI**		
ARQUITECTURA	**12**	La aplicación debe tener una Arquitectura WEB en capas (presentación, negocio y datos). Se preferirá que esté basada en componentes distribuidos y SOA (Service Oriented Architecture).	**SI**		
PLATAFORMA	**13**	La solución debe funcionar con Internet Explorer 11 y versiones posteriores y sobre Sistema Operativo Windows 7 en adelante en las estaciones de trabajo de los usuarios. El backend del software ofrecido debe poder ejecutar sobre ambientes Microsoft con las siguientes características: Servidor de Aplicación - IIS **(Internet Information Service 7.5)** Framework **Microsoft .NET 4.0 o superior** Windows Server **2008 o superior** Ambientes virtuales **VmWare 6.5**	**SI**		
BASE DE DATOS	**14**	La persistencia de la aplicación deberá basarse en el motor relacional SQL Server en Cluster 2014 (64 bits), prefiriéndose la utilización del set de caracteres (collation) Modern_Spanish_CI_AS, case insensitive, for use with the iso_1 multilingual character set.	**SI**		
SEGURIDAD (GENERAL)	**15.1**	La solución debe cumplir con buenas prácticas en materia de seguridad. En particular se requiere que cumpla con: • El Manual de políticas de Seguridad de la Información del BHU. • Medidas de seguridad en relación al Top 10 de OWASP (incluir detalle sobre forma de cobertura) • La seguridad de la aplicación debe controlarse en la capa de presentación y de negocio.	**SI**		
	15.2	Se desea la solución cumpla con: • Los estándares de calidad en la materia ISO/IEC 270XX y con las exigencias de la ISO 27002:2013. • Los estándares definidos por Agesic respecto a la seguridad de los sitios web según: https://www.agesic.gub.uy/innovaportal/file/549/1/Capitulo_5_Seeuridad_v1_0.odt.	**NO**		
SEGURIDAD (AUTENTICACIÓN)	**16**	La conexión a la base de datos debe soportar Windows Autentication con el usuario de LDAP configurado como cuenta de servicio. La seguridad de accesos del aplicativo debe estar integrada al Active Directory del BHU. Con respecto a este punto cabe aclarar que se espera que el Sistema tome las definiciones de usuario y clave de LDAP, apontando por fuera la definición de roles y perfiles. Se prefiere que el sistema solicite usuario y contraseña al ingresar para autenticar al usuario. La aplicación deberá bloquear o cerrar las sesiones de los usuarios por inactividad, siendo el tiempo de inactividad parametrizable a criterio del Banco. Se valora que además se puedan limitar las conexiones de un mismo usuario a n activas concurrentes.	**SI**		
SEGURIDAD (CIFRADO)	**17**	De tráficos: A los efectos de garantizar la confidencialidad e integridad de la información de carácter privado, la aplicación deberá soportar el cifrado de tráficos mediante la utilización del protocolo TLS-HTTPS.	**SI**		
SEGURIDAD (INTERFACES CON SERVICIOS WEB)	**18**	Deberá soportar el cifrado de los datos considerados como críticos mediante la utilización de algoritmos de cifrado robustos, como la utilización de XMLEncryption. Se utilizará autenticación por usuario-clave o por certificado para el llamado de servicios Web.	**SI**		
SEGURIDAD (CONTROLES DE SEGURIDAD)	**19**	• **Sincronización** - Todos los sistemas que integren la solución deberán soportar la sincronización de hora a través de NTP. • **Controles de virus** - Todos los sistemas deberán soportar el software de control de virus de uso corporativo (Kaspersky , Symantec). • **Filtrado** - Todos los sistemas que integren la solución deberán soportar filtrado de tráficos con criterios restrictivos (firewalling). • La solución a implantar deberá ser compatible con la utilización de Reverse Proxy.	**SI**		
SEGURIDAD (AUTORIZACIÓN)	**20**	• La administración de la aplicación deberá soportar la agrupación de usuarios por grupos y perfiles, así como la administración centralizada de perfiles y políticas. • Deberá existir un rol específico para la administración de usuarios y otro para la administración de perfiles.	**SI**		
SEGURIDAD (USUARIOS)	**21**	• **Privilegiados**: Sera deseable la posibilidad de delegar privilegios (inclusive asociados al superusuario) y la restricción de privilegios (inclusive los del superusuario). Ante esta situación el Sistema debe guardar la información que refleje en forma clara la operativa realizada. En este caso el log de seguridad debe minimamente guardar: usuario que delega, a quien se delega, motivo de la delegación y operaciones realizadas. • **Hardcode**: No deberá utilizarse usuarios o perfiles en forma de "hardcode" dentro de la aplicación (ejemplo: SA para definir la conexión del motor de base de datos).	**SI**		
AUDITORÍA Y LOGS	**22**	• La aplicación deberá implementar un mecanismo propio de auditoría, que se utilizará de forma adicional a la auditoría de la base de datos. • Se requiere disponibilidad online de los últimos registros debiendo ser parametrizable la cantidad de días accesibles en esta modalidad. Se deberán registrar y almacenar en la base de datos todas las actividades consideradas como críticas realizadas dentro del sistema, sean accesos exitosos o fallidos, consultas, transacciones, tareas de administración de usuarios y parámetros o cambios sobre información sensible y/o crítica del sistema. La lista total incluye, pero no necesariamente se limita a este detalle. La información registrada deberá permitir la trazabilidad de todas las actividades, esto implica que se deberá conservar el histórico de las modificaciones y eliminaciones realizadas. Deberá quedar identificado en todos los casos el usuario que realiza la transacción, fecha y hora, equipo. • Se deberán proporcionar funcionalidades para respaldo y depuración de los registros mencionados que contemplen el llenado de logs. • Se deberán incluir funcionalidades de búsqueda y reporte amigable por todos los campos y por sus posibles combinaciones. • La aplicación deberá generar logs de registración del funcionamiento correcto e incorrecto de todas las funcionalidades, con información relevante y clara que permita ser utilizada para analizar situaciones anómalas. Se deberán almacenar en formatos compatibles con las bases de datos relacionales del Banco. Debe proveer además un log de contingencia en caso que no se tenga acceso a la Base de Datos.	**SI**		
CORREO ELECTRÓNICO	**23**	La aplicación debe poder integrarse con Exchange mediante SMTP autenticado admitiendo SSL o TLS. En el caso de envió de correo masivo debe poder hacerlo mediante procesos batch fuera de hora y/o integrarse con alguna herramienta para tal fin.	**SI**		
CONFIGURACIÓN DE AMBIENTE	**24**	Toda configuración de ambiente a saber, conexiones a la base de datos, URL de Web Services y demás deben residir en forma externa a la aplicación y deben proveerse procedimientos de cambios de los mismos.	**SI**		
OTROS ATRIBUTOS DEL SISTEMA	**25**	• **Balanceo**: El Sistema debe soportar mecanismos de balanceo de carga con más de un servidor atendiendo solicitudes. • **Asincronismo**: Aquellos procesos que requieran gran poder de procesamiento o consuman intensamente recursos provistos por los sistemas core del Banco deberán implementarse como asincrónicos. Se recomienda el uso de colas de mensajes para implementar este tipo de funcionalidades. • Cuando se soliciten datos deberá hacer paginado a nivel del motor de Base de Datos.	**SI**		
DOCUMENTACIÓN	**26**	Se deberá proporcionar documentación en relación a las siguientes áreas: • Arquitectura de la aplicación y esquemas de implantación • Requerimientos (hardware, software, ancho de banda, espacio en disco, etc.) • Manual de procedimientos • Manual de usuarios • Diccionario de datos en la base de datos (ej: "Knowledge Base de Genexus", "comments" a nivel de base de datos o equivalente) • Diagrama del Modelo Entidad Relación, en formato "Microsoft Visio". • El sistema en su totalidad deberá estar en idioma español. Se deberá entregar documentación como manuales de usuario, requerimientos funcionales, así como todas las instancias de capacitación en idioma español. Se aceptará en forma excepcional documentación en inglés para el resto de los ítems solicitados.	**SI**		