Términos de Referencia para la "Contratación de bienes y servicios para la Implantación de Mecanismos de Seguridad y segundo factor transaccional"

Especificaciones técnicas

Los literales detallados a continuación son Requeridos obligatoriamente (u opcional en caso de que así se encuentre explícitamente mencionado) para la implementación de la solución en seguridades y segundo factor transaccional que necesita la Institución.

COMPONENTES	DESCRIPCIÓN
METODOLOGÍAS Y MARCOS DE TRABAJO	La metodología para el desarrollo del core de seguridades debe cumplir con las mejores prácticas de desarrollo como son: desarrollo iterativo, administración de requerimientos, arquitectura basada en componentes, modelamiento visual, aseguramiento y control de calidad y, gestión de cambios.
	El desarrollo o personalización de los componentes informáticos deben utilizar la metodología RUP la misma que debe contemplar iteraciones en cada una de las fases (inicio, elaboración, construcción y transición). Los artefactos referenciales que deberán ser elaborados y entregados por el proveedor, son los que se detallan en los *(Ver ANEXO 1) Entregables Metodología RUP*.
	Los aplicativos especializados a nivel de aplicativos Web a los que se deben integrar esta solución referirse al *ANEXO 8 - CATALOGO DE SISTEMAS ESPECIALIZADOS*
	OPCIONAL Los aplicativos de la intranet a los que se tienen que integrar la solución de manera opcional para realizar el proceso de control de acceso, referirse al *ANEXO 10. LISTA DE APLICATIVOS DE INTRANET PARA INCORPORAR EL CONTROL DE ACCESO.* En caso de que exista la oferta, el proveedor deberá integrar los servicios y aplicativos de escritorio además realizará la transferencia de conocimiento al personal de la institución para que en la fase de acompañamiento de la segunda iteración el área técnica de la institución determine si integra otros aplicativos o servicios. El proveedor deberá realizar el proceso de despliegue a nivel de la intranet, si es necesario que se configuren componentes adicionales en las PC's de los funcionarios del IESS.
	La Administración del Proyecto por parte del proveedor deberá ser gestionada bajo las buenas prácticas de la gestión de proyectos que propone el PMBOK (Project Management Body of Knowledge). Los entregables referenciales de la Gestión del proyecto que deberán ser elaborados por el proveedor, son los que se detallan en los *(VER ANEXO 5) Entregables de Administración de proyectos.*
	Los componentes de seguridad deberán ser entregados junto con la documentación donde se especifique los mecanismos de integración e información técnica necesaria. Artefactos que deberán ser evaluados y aprobados por el área de Arquitectura de la Dirección de Desarrollo Institucional.
	El proveedor deberá entregar los API's (Application Programming Interface), y todos los componentes de la solución de seguridades; junto con la documentación técnica correspondiente que permita el mantenimiento de la aplicación y la integración con otras plataformas que están descritas en la sección de Arquitectura.
	El proveedor debe dotar de un Call-Center que soporte las consultas de los usuarios del internet e intranet sobre el uso de los nuevos mecanismos de seguridad implantados en los sistemas especializados. Las especificaciones base que el proveedor debe tomar en cuenta para el Call center, se encuentran referidas en el *ANEXO 9, CARACTERÍSTICAS BASE PARA UN CALL CENTER*. El detalle de las especificaciones requeridas se encuentra descrito en la

COMPONENTES	DESCRIPCIÓN
	sección de Call-Center.
	El Proveedor es responsable de suministrar, instalar y entregar debidamente funcionando los EQUIPOS Y SISTEMAS INFORMÁTICOS en los ambientes solicitados para la solución (desarrollo, pruebas, producción con alta disponibilidad y contingencia), cumpliendo con la totalidad de las especificaciones técnicas descritas en los pliegos, entrega de la cual se dejará constancia en documento suscrito por las partes y comisión asignada, acta de entrega recepción final de los bienes, a plena satisfacción de la Institución, de conformidad con la oferta y más documentos que forman parte integrante de este contrato. El procedimiento y fechas de entrega del hardware serán planificados en las fases iniciales del proyecto. El INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL: i. No dispone de instalaciones para hacer posible una recepción física de todos los bienes contratados para embodegarlos, debiendo el proveedor solventar esta necesidad, sin perjuicio de la responsabilidad del contratista sobre la seguridad e integridad de los equipos; además de cubrir la logística de entregarlos en cada una de las dependencias; de esta manera el IESS evita incurrir en costos adicionales para la institución, ii. Se informa que la institución carece de personal técnico para atender el proceso logístico en corto tiempo; iii. Se considera esta decisión además por la perdida de las garantías por la manipulación directa. Se realizará la celebración del acta de verificación cuando los dispositivos se encuentren en la bodega del proveedor. Se realizará la celebración del acta entrega-recepción parcial de todos los equipos físicos de la solución; toda vez que el administrador de contrato ha constatado que los equipos se encuentran listos en cada una de las direcciones provinciales.
	En relación a los componentes citados en la sección *ARQUITECTURA Y ESTANDARES* el proveedor deberá entregar al IESS la metodología a utilizar para el despliegue e implantación de la solución, misma que será validada y aprobada por la Institución. El proceso de despliegue estará bajo responsabilidad del proveedor y supervisión del área tecnológica de la DDI.
	El proveedor deberá emitir un plan de mantenimiento preventivo y correctivo a los servidores instalados en los diferentes ambientes de la Institución considerándose por parte del proveedor la ejecución de este plan en al menos cada 6 meses durante la duración del contrato, adicional deberá capacitar a todo el personal de mesa de servicios, funcional y técnico para el uso, instalación, configuración e integración de los componentes de la solución.
	El proveedor deberá contemplar la ejecución de un despliegue piloto (Sistema especializado de funcionarios) de todos los componentes de la solución en ambiente de producción con el objetivo de solventar inconvenientes que se presenten en el uso del sistema y posibilitar un afinamiento de los procesos de seguridad implantados. Con el propósito de disminuir el riesgo de inestabilidad de Core de Seguridades, en caso de no presentarse novedades en el piloto previo a la presentación del informe respectivo, se continuará el despliegue a nivel nacional de todos los sistemas especializados en acuerdo con delegados de las unidades de negocio involucradas.

COMPONENTES	DESCRIPCIÓN
REQUERIMIENTOS FUNCIONALES	La solución tiene como propósito fortalecer los niveles de seguridad en los aplicativos de los servicios especializados del usuario final, para lo que se requiere la incorporación parametrizable de los siguientes componentes:

COMPONENTES	DESCRIPCIÓN
	• Utilización de 6 factores de autenticación para los servicios especializados, como: usuario/clave, preguntas abiertas de desafío, IP Geolocation, Machine FingerPrint, selección de imagen, OTP (One Time Password) con envío de mensajería. • Permitir: o La creación de roles, opciones de menú por sistema, asignación de permisos, registro de regionales y funcionarios o Parametrización de horarios de acceso a los aplicativos. o Parametrización del tamaño mínimo de la clave. o Parametrización de la fortaleza de la clave (cantidad de números, letras o caracteres especiales que deben ser utilizadas). o Parametrización del tiempo de caducidad de claves. o Parametrización del número de intentos fallidos para proceder al bloqueo del usuario. o Parametrización del número de claves históricas para que el usuario no repita una clave ya utilizada anteriormente. o Parametrización de alertas al usuario (días próximos para cambiar su clave, intentos restantes para bloqueo de su cuenta, entre otros). o Mecanismo para dar de baja a un usuario. o Mecanismo para bloqueo de usuarios. o Mecanismo para suspensión de usuarios durante cierto periodo de tiempo. o Administración de calendarios para la definición de días no laborables, feriados, entre otros. o Administración de perfiles de usuarios. o Administración descentralizada de usuarios pertenecientes a una diferente unidad de trabajo. o Mecanismo para el cambio de clave. o Mecanismo para la recuperación de usuario y clave olvidados. o Mecanismo para registro de auditorías. o Mecanismo para la asociación de los factores de autenticación a los usuarios. • Debe permitir la parametrización de niveles de autenticación por sistema especializado y rol del usuario. • Integración del componente de seguridades en todos los sistemas especializados y entrega de mecanismos de integración con plataformas según descritas en el *ANEXO 8: Catalogo de Sistemas Especializados* • El segundo factor de autenticación OTP deberá ser integrado en los sistemas especializados, en todas las transacciones que generen egresos económicos a la institución, además deberá integrase en la actualización de datos personales y financieros del usuario y cambio de la clave en línea, en caso de existir un cambio de definición la institución la confirmará en la etapa inicial del proyecto. • Se contará con un único punto de acceso para los sistemas especializados expuestos a usuarios de internet en plataforma Web. • Registro de información de auditorias. • Generación de información para entes de control.

COMPONENTES	DESCRIPCIÓN
	• Generación de reportes para unidades de negocio • Generar el front de la funcionalidad para la impresión de claves considerando la integración de la verificación biométrica tanto del funcionario como del usuario solicitante. El mecanismo y componentes para la integración de biometría serán facilitados por parte de la Institución. (El proveedor deberá reutilizar los insumos de papel químico existentes para impresión de clave) • Generar interface para registro o actualización de información de usuario, como: correo electrónico, número celular, imagen y preguntas de desafío. • Migración de información del 100% de usuarios, roles, opciones de menú y permisos del sistema de seguridades actual al nuevo esquema de base de datos del sistema de seguridades a implantarse. • El sistema de seguridades deberá permitir verificación con listas de observados a nivel de número de cédula de identidad y de números de IP's no autorizados, antes del acceso a los sistemas especializados. • La longitud de la clave debe ser parametrizable como mínimo de ocho caracteres hasta un máximo de diez y seis caracteres, considerando lo siguientes casos: o Cuando se entregue o actualice la clave o Cuando se implemente el nuevo sistema de seguridades (creación de usuario y clave) • La configuración de la vigencia de la clave debe ser parametrizable, inicialmente se tendrá una vigencia de seis meses para usuarios del internet y una vigencia de tres meses para usuarios de los servicios especializados de funcionarios, en caso de que no la haya cambiado, el sistema le obligará el cambio cuando acceda. • Cuando el usuario requiera cambiar la clave a libre albedrío, esta funcionalidad se lo debe realizará a través del aplicativo una vez que el usuario supere los factores de seguridad solicitados para la solución. • El sistema deberá estar integrado con sistemas de envío de mensajes a correo electrónico o mensajería móvil a fin de dar a conocer las acciones realizadas en el sistema informático e informar el código generado "One Time Password" previo a la confirmación de una transacción económica. • Para los usuarios de los servicios especializados de funcionarios, el core de seguridades generará y enviará la clave de acceso directamente a la dirección de correo electrónico institucional del servidor solicitante, de manera que el administrador no pueda visualizar la clave generada. • El proveedor deberá proponer un plan para realizar la campaña de socialización y concientización hacia el usuario final y disminuir el riesgo de rechazo del despliegue de la solución.
	El proveedor deberá certificar en la solución ofertada, que los niveles de seguridad acogen según corresponda las disposiciones emitidas por la Superintendencia de Bancos y Seguros en la Resolución **JB-2012-2148** del 26 de Abril de 2012.
	La solución debe proponer y especificar los procesos para los siguientes escenarios: • Administración de seguridades a la intranet e internet para cada sistema especializado por unidad de negocio (descentralizada).

COMPONENTES	DESCRIPCIÓN
	• Administración de roles de usuarios por unidad de negocio para acceso a los aplicativos de la intranet e internet. • Administración de roles para los siguientes tipos de usuarios: o Afiliado activo o Dependientes o Afiliado voluntario o Jubilado o Cesante o Afiliado que vive en el extranjero o Empleador (posibilidad de manejo de distintos roles / delegación de funciones para este tipo de usuario en el sistema especializado *empleadores* debido a que poseen varias sucursales o delegan funciones a terceros) o Funcionario. • Creación usuarios para los funcionarios en el sistema de seguridades para uso de aplicativos de la intranet por unidad de negocio, regional y oficina. • Inactivación de accesos por unidad de negocio y a nivel institucional según integración dada con el sistema de control de nómina del IESS. Administración de asignaciones de accesos a sistemas especializados para funcionarios por unidad de negocio.
	Se debe generar por parte del proveedor la documentación del procedimiento propuesto para la solicitud, asignaciones, notificación y revocación de accesos para afiliados, empleadores, jubilados y servidores/funcionarios de acuerdo a formato validado con el IESS.
	El proveedor deberá proponer y especificar los procedimientos a seguir para en caso de fraudes, posibilitar el registro en el listado de observados, seguimiento / auditoría para usuarios implicados, de acuerdo a formato validado con el IESS.
	La solución proveída deberá disponer de al menos **diez (10) reportes** para cada tipo de usuario (de la intranet o internet) que permitan dar seguimiento a los fraudes; los formatos serán definidos y validados por la institución.
	El proveedor deberá construir la interfaz de impresión de claves con el nuevo esquema de seguridades e integrar los componentes de verificación biométrica, cuyos componentes y documentación técnica serán provistos por la Institución.
	El proveedor deberá proponer y especificar un procedimiento a seguir para responder ante una contingencia a nivel tecnológico, como podría ser: pérdida de las comunicaciones o en la integración con los sistemas especializados, caída del servidor de seguridades u otros servicios asociados a la solución, falla de los factores de autenticación, entre otros; e implementar mecanismos de restauración en caso de falla de alguno de sus componentes.
	El proveedor deberá sugerir y apoyar en la generación de la normativa necesaria que permita amparar legalmente esta solución informática.
	La solución informática para todos sus mecanismos de seguridades deberá permitir la habilitación o inhabilitación de su funcionalidad por sistema especializado, unidad de negocio, rol y tipo de usuario (de la intranet o internet).

COMPONENTES	DESCRIPCIÓN
	El proveedor deberá incluir el servicio de Call Center para atender la demanda de consultas de los usuarios finales sobre el uso de los nuevos mecanismos de seguridad implantados en los sistemas especializados expuestos al internet e intranet. El Call Center deberá estar a disposición durante un año posterior a la fase de estabilización en ambiente de producción. El proveedor deberá incluir en su oferta el servicio de Call-Center, considerándose para esto lo especificado en la sección "CALL - CENTER".
	El proveedor deberá incluir en su oferta el servicio de envío de mensajes, considerándose para esto lo especificado en la sección "SERVICIO DE ENVIO DE MENSAJES VÍA CELULAR Y CORREO ELECTRÓNICO" El proveedor deberá considerar los mecanismos necesarios para asegurar el envío de los mismos las especificaciones de seguridad serán definidas por la institución en la etapa inicial del proyecto.

COMPONENTES	DESCRIPCIÓN
ARQUITECTURA Y ESTÁNDARES	El proveedor debe desarrollar las interfaces para posibilitar la impresión de claves considerando integración con la verificación biométrica tanto del funcionario en el acceso al sistema, como del usuario solicitante. El mecanismo y componentes para la integración de biometría serán facilitados por parte de la Institución. (El proveedor deberá reutilizar los insumos de papel químico existentes para impresión de clave) El proveedor debe generar las interface para enrolamiento de los datos del usuario, que permitirá según la demanda, registrar o actualizar por parte del usuario final datos como: el correo electrónico, número de celular, preguntas abiertas, imagen y demás información que el IESS a su debido tiempo lo considere.
	La información que se almacenará en la base de datos tales como: clave, número celular, correo electrónico debe estar cifrada con algoritmos aprobados por la institución al inicio del proyecto.
	La solución de autenticación y autorización impactará la Arquitectura de los aplicativos y servicios que actualmente maneja la institución, a continuación se detallan los componentes planteados: • ***Servidor de autenticación:*** *Servidor encargado de manejar las credenciales de autenticación de los usuarios.* • ***Servidor de autorización:*** *Servidor encargado de la autorización de accesos hacia los diferentes aplicativos.* • ***Servidor web:*** *las aplicaciones desarrolladas por el IESS tienen el mecanismo de autenticación y autorización incluida en cada aplicativo por tal motivo para la implementación de la nueva solución de autenticación y autorización se tendrían que hacer los correspondientes cambios en todos los aplicativos web.* • ***Servidor de base de datos:*** *Servidor con la información para la autenticación y autorización que actualmente se utiliza desde los aplicativos web para que se adapten a la nueva plataforma de seguridades.* • ***LDAP:*** *Directorio desde donde se obtendrá los datos pertenecientes a los servidores públicos del IESS.* • ***OSB:*** *Bus de servicios que presentará funcionalidad correspondiente a la autenticación y la autorización para su interoperación con los sistemas que lo requieran.* • ***Servidor de e-mail:*** *Será utilizado para enviar notificaciones vía correo electrónico sobre las alertas identificadas en la autenticación.* • ***Servidor de Repositorio de OTP's****: permite generar un conjunto de códigos*

COMPONENTES	DESCRIPCIÓN
	disponibles para la autentificación del segundo factor transaccional • ***Servicio de envío de mensajes SMS y correo electrónico*** • ***Servicio de Call-Center*** • ***Servidor para SSO*** El esquema de infraestructura planteado, contempla un ambiente de alta disponibilidad que se encontrará físicamente en Quito, sin embargo, se debe considerar un sitio alterno de contingencia en la ciudad de Guayaquil.
	El proveedor deberá implementar para los sistemas especializados un único punto de acceso en el cuál los usuarios se autenticarían una única vez y tendrán a disposición según el rol que tengan asociados, el listado de aplicativos en los cuales no será necesario volverse a logear. Como segundo factor de verificación de una transacción económica a realizarse a través de los sistemas especializados Web se incorporará la generación del OTP y envió del mensaje vía telefonía móvil y correo electrónico.
	El Proveedor para el desarrollo de interfaces para la impresión de claves, registro de información de usuario (preguntas de desafío, imagen, correo electrónico y número celular) deberá cumplir con las siguientes especificaciones de arquitectura de software: • Soporte a JDK 1.5 y superiores • Uso de herramientas de desarrollo para la creación de programas en Java tales como Eclipse 3.4.2 y superiores. • Uso de frameworks JEE 5.0 y superiores así como J2EE1.4, • Uso de contenedores de aplicaciones tales como JBOSS 4.2.3 GA y superiores, • Implementaciones del patrón MVC (Modelo, Vista, Controlador) • Uso del framework JSF 1.2 y superiores para desarrollo de la capa de presentación. • Uso del framework EJB 3.0, desarrollo de los servicios (sesión bean), lógica de negocio. • JPA, desarrollo de la persistencia. • Uso de base de datos Oracle 11g y superior • Soporte de exploradores: Internet Explorer 7 y superior, Firefox 3.5 y superior, Chrome 4.1 y superior, Safari 4.0 y superior y en los navegadores que sean definido por el IESS en la fase de elaboración según la necesidad de cada mantenimiento * Por motivo de mantenimiento en las aplicaciones es necesario el conocimiento de los siguientes APIs y frameworks: Richfaces 3.3.3 o superior, struts 1, css, javascript, ajax, html, xml, xslt, apache ant, spring, hibernate, jpa 1.0 o superior, pl/sql, jasper reports, jax-ws, xsd. Además considerar que para la impresión de claves de usuarios, las opciones implementadas deberán reutilizar el formato de papel químico que la Institución posee.

COMPONENTES	DESCRIPCIÓN
	El Proveedor deberá considerar el desarrollo o personalización de las siguiente interfaces: • Interfaz para registrar preguntas de desafío, selección de imagen, correo electrónico, número de celular y demás información del usuario necesaria para la solución. • Reutilizar la lista de observados que proporcionará la institución para que sea validada previo a transacciones que demanden salida de dinero. • Interfaz para generación de reportes de auditoría para los usuarios de la intranet e internet. • Interface para impresión de claves en la cual se re-utilizará el papel químico existente y se incorporará el componente de verificación biométrica. • Interfaces de administración y subadministración de seguridades a nivel de roles, opciones de menú, habilitación / deshabiltiación de accesos, y demás especificaciones mencionadas en la sección "Requerimientos Funcionales". • Generación de reportes para auditoría El proveedor deberá cumplir con los estándares, mecanismos de arquitectura y mejores prácticas de desarrollo definidos por la Institución (Los documentos de estándares y buenas prácticas serán entregados al proveedor adjudicado) para el desarrollo de los componentes de seguridad, interfaces personalizadas y creación de objetos de base de datos. En caso de que el proveedor recomiende variaciones en la arquitectura de referencia e integración de nuevos mecanismos de arquitectura, que agreguen valor tecnológico a las soluciones informáticas desarrolladas para la institución, estos serán en conjunto con el IESS evaluados para ser incluidos como parte del estándar. (Ver ANEXO 2) Arquitecturas Referenciales.
	Los componentes informáticos Software y Hardware que el proveedor debe proporcionar en la solución de los nuevos mecanismos de seguridad a implantarse en los sistemas especializados Web, referirse al *ANEXO 7 COMPONENTES INFORMÁTICOS DE SOFTWARE Y HARDWARE*
	El diseño gráfico de las interfaces Web / personalización de la solución debe sujetarse a los lineamientos, necesidades funcionales y estándares vigentes en la Institución.
	La solución de seguridades deberá soportar y garantizar configuraciones de alta disponibilidad y balanceo de carga, para lo cual el proveedor deberá establecer una configuración del servidor se seguridades activo-pasivo para el centro de cómputo principal y pasivo para el centro de cómputo alterno de contingencia, mismos que el proveedor deberá proporcionar el licenciamiento correspondiente.

<table>
<tr><th>COMPONENTES</th><th>DESCRIPCIÓN</th></tr>
<tr><td></td><td>
La solución debe integrarse los siguientes sistemas operativos a nivel de cliente:

Windows XP de 32 y 64 bits,
Windows Vista de 32 y 64 bits,
Windows 7 de 32 y 64 bits.

La solución debe ser compatible con los exploradores:

Internet Explorer 6 y superior,
Mozilla Firefox 8 y superior,
Google Chrome 19.0 y superior,
Safari
Opera y
En navegadores que sean definidos por la institución en la fase de ejecución del proyecto.

<u>Integración con los aplicativos de la Institución:</u>
La solución deberá ser integrada a nivel de todos los sistemas especializados desarrollados por el IESS (referirse al listado de aplicativos del ANEXO 8: Catalogo de Sistemas Especializados).
La solución debe presentar un API para:

Impresión de clave
Control de acceso a los sistemas especializados
Construcción de las opciones de menú
Verificación de segundo factor de autenticación OTP antes de una transacción que derive en el pago de una prestación económica
Componente de integración con mensajería celular y correo electrónico

Estos componentes deberán ser factibles su integración con aplicativos web desarrollados bajo el lenguaje de programación java (jdk 1.3 y superior).
La solución debe estar certificada para la integración en los aplicativos Web con las siguientes arquitecturas:
<table>
<tr><th rowspan="2">SERVIDOR DE APLICACIONES</th><th colspan="3">ARQUITECTURA</th></tr>
<tr><th>PERISITENCIA</th><th>NEGOCIO</th><th>WEB</th></tr>
<tr><td>JBoss 4.2.3 y JBoss 5.1 EAP</td><td>JPA</td><td>EJB 3.0</td><td>JSF</td></tr>
<tr><td>JBoss 4.2.3 y JBoss 5.1 EAP</td><td>JPA</td><td>EJB 3.0</td><td>JSF (ADF)</td></tr>
<tr><td>JBoss 5 EAP</td><td>JDBC</td><td>JSP</td><td>JSP</td></tr>
<tr><td>IAS 9i, versión 1.3.22.0.1a</td><td>JDBC</td><td>JSP</td><td>JSP</td></tr>
<tr><td>OAS 10G, 10.1.2.0.2</td><td>JBDC</td><td>EJB 2.1</td><td>cocoon</td></tr>
<tr><td>JBoss 4.2.3</td><td>hibernate</td><td>spring</td><td>struts</td></tr>
<tr><td>JBoss 4.2.3</td><td>hibernate</td><td>spring</td><td>struts</td></tr>
</table>
</td></tr>
</table>

COMPONENTES	DESCRIPCIÓN
	La solución que proporcionará el proveedor deberá además cumplir con las siguientes características: • El código debe pertenecer al proveedor de manera que pueda adaptarse a las necesidades del IESS (en el caso que se requiera validaciones previas contra una base de datos, servicio web, etc.). • El aplicativo debe ser fácilmente integrable a los aplicativos web desarrollados en el IESS. • El aplicativo deberá ser personalizable de manera que se pueda incluir estilos de acuerdo a la imagen institucional. • Debe cumplir normas de seguridad para que no pueda ser utilizado por personas no autorizadas.
	La plataforma debe cumplir con las siguientes características: Acceso: • Único punto de acceso para Internet e intranet, por medio del portal institucional. • (OPCIONAL) Single Sign On (SSO) para Intranet, por medio del sistema operativo. El proveedor deberá incorporar a nivel de intranet; en los sistemas web que hacen uso los usuarios internos del IESS y aplicaciones de escritorio; los componentes para permitir la autenticación y verificación a través de un SSO a nivel de sistema operativo. Autenticación: Se utilizarán los siguientes factores para autenticación: • Usuario y clave: Para las aplicaciones de Internet, la clave se ingresará por medio de un teclado virtual. • IP-geolocation y machine fingerprint. • Selección de imagen: en el caso que exista alguna alerta en los factores de IP-geolocation y machine fingerprint. Aseguramiento de transacciones: Se utilizarán los siguientes factores para aseguramiento de transacciones: • Envío de OTP al teléfono celular y correo electrónico del usuario: para transacciones monetarias y actualización de información del usuario (mail, celular, imagen, preguntas). • Selección de imagen junto a preguntas y respuestas abiertas: se utilizarán para la recuperación de claves o recuperación del identificador de usuario. • (OPCIONAL) Preguntas cerradas: la información se obtendrá de los datos que posee el IESS. Se utilizará este factor en la creación del identificador de usuario en caso de no existir este mecanismo se debe usar las preguntas abiertas. Sistema de Administración de Seguridades: Características mínimas • Administración de usuarios, roles y perfiles. o Funcionalidades adicionales requeridas: bloqueo, suspensiones, bajas, delegación de funciones. • Administración descentralizada de usuarios pertenecientes a una diferente unidad de trabajo. • Administración de calendarios para la definición de días no laborables, feriados, entre otros. • Administración de los permisos hacia los diferentes aplicativos. • Administración de los factores de autenticación (preguntas y respuestas, selección de imagen, tiempo de vigencia del OTP, etc.).

COMPONENTES	DESCRIPCIÓN
	• Parametrización horarios de acceso a los aplicativos. • Parametrización el tamaño mínimo de la clave. • Parametrización la fortaleza de la clave (cantidad de números, letras o caracteres especiales que deben ser utilizadas). • Parametrización el tiempo de caducidad de claves. • Parametrización el número de intentos fallidos para proceder al bloqueo del usuario. • Parametrización el número de claves históricas para que el usuario no repita una clave ya utilizada anteriormente. • Parametrización las alertas al usuario (días próximos para cambiar su clave, intentos restantes para bloqueo de su cuenta, entre otros). • Mecanismo para el cambio de clave. • Mecanismo para la recuperación de claves olvidadas. • Mecanismo para la recuperación de usuario olvidado. • Mecanismo para registro de auditorías (accesos fallidos, accesos exitosos, cambios realizados en las configuraciones).
	Consideraciones • La solución debe incluir el hardware necesario para su implementación, en base a las características técnicas descritas en la sección "Plataforma de Hardware". • Cambio del Login de usuario: actualmente se maneja la cédula para el acceso a las aplicaciones. La cédula debe ser cambiada por un identificador de usuario para el Login de forma que no se afecten a los aplicativos. • Se debe contemplar el proceso de enrolamiento de los factores de seguridad (selección de la imagen, preguntas y respuestas) • En el enrolamiento se debe solicitar el correo electrónico y el celular del usuario, los cuales serán utilizados para el envío del OTP. • El modelo de datos de seguridades que soporta la autorización no está normalizado, por tal motivo se debe contemplar el mejoramiento o creación del modelo de datos de roles y perfiles y su adaptación al core de seguridades. • La exposición de servicios web debe realizarse a través del bus de servicios que el IESS defina.
	Plataforma de Hardware Para la instalación de la solución debe contemplarse las siguientes características de hardware: • Si la solución se despliega sobre una arquitectura JEE: Implementar sobre sistema operativo LINUX 6.X o superior en equipos de arquitectura POWER (IBM 780 o 770) sobre ambientes virtualizados con LPARS. • Si la solución requiere su implementación sobre sistema operativo WINDOWS SERVER: Implementar en equipos de arquitectura BLADE X86-64 sobre ambientes virtual izados con VMware vSphere 5 Enterprise plus. • Para el caso de Windows Server 2008 R2 64 bits debe incluir licencias tipo Datacenter bajo el esquema Microsoft Enterprise Agreement que posee el IESS. • Las subscripciones de Linux RedHat Enterprise 6.x o superior debe incluir los módulos de monitoring y agente para conectarse a RHN que posee el IESS. • El proveedor deberá incluir como parte de la solución la infraestructura necesaria en hardware; el proveedor será responsable del dimensionamiento de: servidores, almacenamiento y licenciamientos de Sistemas Operativos y

COMPONENTES	DESCRIPCIÓN
	software adicional, tomando en cuenta los lineamientos emitidos por el IESS, debe garantizar la funcionalidad requerida del servicio o aplicación a implementar. • La implementación de los ambientes de Producción deben considerarse en un esquema de alta disponibilidad activo-activo y balanceo de carga. • Se debe contemplar la implementación de un esquema de contingencia en el centro de datos alterno del IESS en la ciudad de Guayaquil sin alta disponibilidad. • Se implementarán en el centro de datos principal (Quito) los ambientes de Producción, Pruebas y desarrollo. • Se implementara en el centro de datos alterno solo el ambiente de Producción. • Instalación sobre la base de datos: Oracle 11G release 11.2.0.3 – RAC. El proveedor deberá incluir en su solución los componentes necesarios para establecer una configuración de un ambiente de pruebas y un ambiente de pre-producción.
	Los objetos de datos de la autenticación y autorización se crearán en una instancia de Base de Datos en el ambiente de Producción, en un esquema propio. La integración a nivel de Base de Datos que manejará la solución, se muestra a continuación: **A NIVEL DE LA INTRANET** • LDAP: o Validación de Usuarios y Claves • Seguridades: o Validación de usuario y clave o Validación de políticas de seguridad • Sistemas IESS: o Homologación de Identificación o Validación de Roles o Generación de menús o Actualización de Datos en un repositorio central • Biométrico: o Validación de las listas de observados o Validación de la huella digital para las transacciones **A NIVEL DEL INTERNET** • Seguridades: o Validación de usuario y clave o Validación de políticas de seguridad • Sistemas IESS: o Homologación de Identificación o Validación de Roles o Generación de menús o Actualización de Datos en un repositorio central • Biométrico: o Validación de las listas de observados
	El registro de auditoría debe contener como mínimo la siguiente información: • Autenticación:

COMPONENTES	DESCRIPCIÓN
	○ El aplicativo al que ingreso ○ El usuario que ingresó al aplicativo ○ Fecha en la que se ingresó o se intentó ingresar al aplicativo. ○ Tipo de acceso, exitoso o fallido ○ El error presentado en caso de acceso fallido del usuario. ○ La IP desde donde se realizó el ingreso al aplicativo. • Autorización ○ El aplicativo al que ingreso ○ El usuario que ingresó al aplicativo ○ Fecha en la que se ingresó o se intentó ingresar al aplicativo. ○ La IP desde donde se realizó el ingreso al aplicativo. Seguridad (Implementación de protocolo seguro en las aplicaciones). Instalación sobre la base de datos: Oracle 11G release 11.2.0.3 – RAC. La solución debe presentar un mecanismo para el mantenimiento y vaciado de datos históricos, considerando las mejores prácticas de la industria. En caso de requerir campos adicionales la Institución los definirá en la fase de diseño del proyecto.
	Desarrollo de la solución En el desarrollo o mantenimiento de aplicativos para la integración de la solución debe considerarse lo siguiente: • Enmarcarse dentro de la Arquitectura Referencial establecida por la Dirección de Desarrollo Institucional. • Enfocarse en la metodología de desarrollo de software definida por la Dirección de Desarrollo Institucional. • Acoger las definiciones, recomendaciones, lineamientos y mecanismos generados por Arquitectura de TI de la Dirección de Desarrollo Institucional. • Reutilizar el código fuentes y componentes existentes en los sistemas especializados, bases de datos y sistemas legados. • Al inicio de la fase de ejecución, para el caso de nuevas propuestas tecnológicas estas deben ser validadas por el área de Arquitectura y en el caso de requerirlo se solicitará la entrega de una prueba de concepto que valide la propuesta. • Integrarse e interoperar dentro de una Arquitectura Orientada a Servicios • Proveer servicios, conectores y/o adaptadores para funcionar en un esquema de integración • Funcionar y operar de manera nativa sobre la infraestructura especificada. • El proveedor será el responsable de la implementación, pruebas y puesta en marcha de la solución además de la debida transferencia de conocimiento y documentación a las áreas de tecnologías correspondientes del IESS y contar con el aval de las áreas de la Dirección de Desarrollo Institucional que intervienen en el ciclo de vida del desarrollo del software. • El inicio de la fase de ejecución, el proveedor debe realizar un análisis de integración de la solución ofertada con los sistemas existentes en el IESS, conjuntamente con los arquitectos de la institución con la finalidad de revisar su factibilidad.

COMPONENTES	DESCRIPCIÓN
	El proveedor deberá integrar la verificación de transacciones a través de OTP en los siguientes aplicativos: • Fondos de Reversa • Cesantías • Jubilaciones • Subsidios • Actualización de parámetros de seguridad del usuario. • Y demás que confirme la institución al inicio del proyecto.
	El proveedor deberá brindar el servicio de envío de mensajes según se especifica en la sección "**SERVICIO DE ENVIO DE MENSAJES VÍA CELULAR Y CORREO ELECTRÓNICO**".
	El proveedor deberá brindar el servicio de Call-Center según se especifica en la sección "**CALL - CENTER**".

COMPONENTES	DESCRIPCIÓN
NIVELES DE SERVICIO	El proveedor según el *ANEXO 6: "Plan de trabajo estimado referencial"* proporcionará un periodo de estabilización previo a la entrega formal para la iteración 1 no menor a 30 días calendario y para la iteración 2 no menor a 30 días calendario. Por lo tanto la solución de errores y/o defectos imputables al sistema, se realizará sin costo alguno durante el tiempo de estabilización. Finalizada la fase de estabilización de la iteración correspondiente (iteración 1 o iteración 2) el proveedor deberá cumplir lo siguiente: • Acompañará de manera presencial en el proceso de uso y administración de seguridades para cada unidad de negocio, además solventar a nivel de Hardware o Software inconvenientes en el uso de cualquiera de los componentes de la solución e igualmente validará la calidad del proceso de seguridad implantado a nivel de la intranet e internet. La fase de acompañamiento para la iteración 1 no menor a 90 días calendario y para la iteración 2 no menor a 60 días calendario. • Se realizará la entrega recepción de los componentes de la solución implantados, junto con la entrega del informe de aceptación emitido por parte de las áreas involucradas de la DDI-IESS de muto acuerdo con el proveedor. • De la iteración 1 el proveedor brindará un soporte por un lapso de un año para todos los componentes y servicios que intervienen en la solución, tiempo en el cual mantendrá un canal abierto de soporte 24/7 con el área de mesa de servicios del IESS, para solventar de manera conjunta inconvenientes de Hardware o Software. En caso de temas emergentes que defina el área técnica del IESS, el proveedor deberá dirigirse a las instalaciones del IESS para solventar el inconveniente. Para soluciones correctivas el proveedor deberá sujetarse al proceso / metodología para realizar el mantenimiento de aplicaciones que lleva actualmente la institución. El soporte deberá considerar los tiempos indicados en el *ANEXO 3 Tiempo de*

COMPONENTES	DESCRIPCIÓN
	Diagnóstico y Solución a Fallas.
	Para el desarrollo de componentes de seguridades de integración con los sistemas especializados, que serán usados a nivel de intranet e internet, el proceso de modelado de negocio, administración de requerimientos, análisis, diseño, implementación, pruebas, aseguramiento y control de calidad, despliegue, estabilización del sistema, diagnóstico y solución a fallos; así como el servicio de Call-Cener y servicio de envío de mensajes serán medidos en base a los acuerdos del nivel de servicio (SLA) establecidos por la institución
	Los artefactos generados por el proveedor para el desarrollo de componentes de seguridades, así como del desarrollo de componentes de integración con los sistemas especializados, servicio de Call-Center y servicio de mensajería; serán continuamente evaluados por el gerente de proyecto designado por la institución, mismo que al encontrar inconformidades en estándares, funcionalidades y/o acuerdos, solicitará formalmente al proveedor que realice los respectivos ajustes sin que esto incurra en costos adicionales a la institución con una respuesta en un máximo de horas según el nivel de criticidad que esto represente. *(Ver sección de indicadores de niveles de servicio).*
	El proveedor realizará la capacitación necesaria solicitada en la sección de Instalación y Capacitación para todo el personal asignado por la institución, con el objetivo de que conozcan a detalle la estructura técnica, funcional y la administración de la solución informática; de tal forma que esto permita el uso eficaz del software y su posterior mantenimiento de manera escalable
	El proveedor de la solución informática antes de publicar el sistema en ambiente de producción deberá cumplir con todas las políticas, estándares y buenas prácticas definidos por el departamento de aseguramiento y control de calidad de la Institución. Además deberá contar con un plan de despliegue a nivel nacional y plan de contingencia, aprobados por la unidad de negocio que defina el IESS y el departamento de mesa de servicios del IESS.
	El proveedor garantizará la seguridad y confidencialidad de la información proporcionada por el IESS durante el proceso, así como protegerá la propiedad intelectual de la solución de seguridades, de los componentes de integración desarrollados, nueva funcionalidad en sistemas especializados y de los artefactos entregados a la Institución, por lo que, de los mismos queda prohibida la copia, distribución y utilización en otras empresas ya sean estás públicas o privadas dentro y fuera del país. El incumplimiento del mismo desembocara en la Terminación Unilateral del Contrato y ejecución de los procesos legales que de ello se deriven.
	El proveedor al inicio del primer mes de inducción debe presentar en su propuesta los modelos de calidad, los procedimientos asociados al control de cambios y versionamiento de software y herramientas que posee para el desarrollo de este tipo de proyecto; además el perfil del equipo responsable del aseguramiento de la calidad. Vale indicar que los modelos de calidad que hace uso el proveedor pueden sufrir

COMPONENTES	DESCRIPCIÓN
	cambios para satisfacer los niveles de calidad requeridos por el IESS.
	Para el dimensionamiento de la solución deben contemplarse los siguientes valores: - Promedio mensual de nuevos usuarios: 12.850 - Promedio diario de conexiones: 393.600 - Número de usuarios registrados en el LDAP: 10.000 La solución informática deberá permitir un alto nivel de transaccionalidad en las verificaciones de los factores de seguridad, para un manejo de : **Usuarios de la intranet:** 5.000 **Usuarios del internet:** 4'000.000 La concurrencia por segundo que debe soportar el core de seguridades debe ser de al menos 40 transacciones por segundo.

COMPONENTES	DESCRIPCIÓN
	El proveedor deberá presentar los documentos de titularidad del software ofertado. En caso de ser partner de alguna fabrica deberá presenta el documento que le otorgue la representación de la misma, garantía técnica del fabricante y certificado de que es un centro autorizado para proporcionar soporte..
	El proveedor deberá acreditar experiencia de al menos 5 (años) en el mercado, desarrollando e integrando soluciones de mecanismo de Seguridades y segundo factor transaccional con sistemas informáticos para Instituciones del Sector Público o Privado.
	El proveedor deberá contar con una propuesta de plan de trabajo formal para cumplir con la implantación y construcción de la solución informática e integración de la parte de accesos y opciones de menú con los sistemas especializados que la Institución posee. El plan de trabajo deberá ser entregado para la calificación de la oferta y en la etapa inicial del proyecto, además en la etapa inicial será evaluado y aprobado de mutuo acuerdo entre el proveedor y la Institución. *(ANEXO 6 PLAN DE TRABAJO ESTIMADO REFERENCIAL)*
EXPERIENCIA Y CERTIFICACIÓN	El proveedor deberá incluir en su propuesta los perfiles de cada uno de sus recursos que conformarán el equipo base *(Ver ANEXO 4) PERFILES POR ROL*, correspondientes a los roles definidos en la metodología de trabajo. Dichos recursos deberán mantener relación de dependencia laboral con el proveedor. Además el proveedor deberá presentar el Rol de empleados del Sistema de Historia Laboral del IESS, donde conste al menos el equipo base que se asignará a la ejecución del contrato.
	El equipo base asignado *(Ver ANEXO 4) PERFILES POR ROL*, calificado y aprobado en el proceso de selección, deberá tener participación en el 100 % de la duración del contrato en base al plan de trabajo presentado. El IESS se reserva el derecho de solicitar el cambio de personal en caso de requerirlo, por lo que El proveedor estará en la capacidad de reemplazarlo con un recurso asignado, calificado y aprobado que cuente con igual o superior perfil para su rol a desempeñar,

COMPONENTES	DESCRIPCIÓN
	de tal forma que el desarrollo del proyecto no sea afectado.
	El proveedor garantizará que el personal asignado a la ejecución del proyecto cuente con el perfil solicitado por el IESS, para de esta manera asegurar que posean los suficientes conocimientos, experiencia y competencias para desempeñar el rol que se le está encargando; los recursos asignados, calificados y aprobados en el proceso no podrán ser reemplazados intempestivamente por parte del proveedor durante la ejecución del proyecto, a menos que existan razones que justifiquen el hecho, en cuyo caso el personal de reemplazo deberá mantener el perfil acorde al rol a desempeñar, además de contar con la aprobación por parte del IESS.
	El IESS se reserva el derecho de evaluar al personal asignado cuando crea necesario. Las políticas de validación y puntaje mínimo, serán notificadas el momento de la evaluación, los resultados obtenidos de no estar acordes a las necesidades del IESS, permitirán disponer de la remoción del recurso y su respectivo e inmediato reemplazo, con un recurso asignado y calificado que cuente con igual o superior perfil para su rol a desempeñar, de tal forma que el desarrollo del proyecto no sea afectado. Una vez que el proveedor sea adjudicado podrá adherir talento humano que crea conveniente para sus equipos de trabajo según los perfiles definidos *(Ver ANEXO 4) PERFILES POR ROL* en caso de que alguno de los perfiles no cumpla con los requisitos establecidos, deberá someterse a la evaluación técnica correspondiente por parte del IESS, y al menos deberá alcanzar un puntaje del 75%.
	El proveedor designará un Gerente de Proyecto y un equipo técnico idóneo (Propuesto en el Plan de trabajo), mismos que serán evaluados y aprobados por el IESS acorde a su perfil y rol a desempeñar, mismos que se encargará del proceso de desarrollo e implantación de la solución informática, en conjunto con un Gerente de Proyecto asignado por el IESS el cual actuará como contraparte.
	El proveedor deberá entregar como parte de su expediente, información sobre sus casos de éxito con lecciones aprendidas, mismos que serán avalados con los respectivos certificados de las empresas en las cuales fueron ejecutados en los 5 (cinco) últimos años, proyectos para la Implantación del mecanismo de Seguridades y segundo factor transaccional o con características similares en lo referente a la arquitectura utilizada por el IESS. Certificado de que el producto ofertado cumple con estándares de seguridades de la resolución JB-2012-2148 de la Superintendencia de Bancos asociados a la solución a implantar. Certificado/s de ser proveedor habilitado para el servicio de mensajería móvil a través de las operadoras de telefonía móvil habilitadas en el país Certificado de estar habilitado para el servicio envío de correo electrónico (Mailing) Certificado en Gestión de Calidad para Mensajería Celular y Correo Electrónico

COMPONENTES	DESCRIPCIÓN
	Si los productos ofertados a más de lo especificado en la sección *ARQUITECTURA Y ESTANDARES,* necesitan de software y/o hardware adicional para el correcto funcionamiento y no están especificados en los solicitados, los costos de licenciamiento, capacitación en administración e implementación estarán a cargo de proveedor, con las mismas condiciones de garantía, mantenimiento y soporte solicitados para el resto de licencias, los mismos que deberán ser especificados como parte de la oferta.
	El proveedor deberá considerar en su propuesta las características detalladas de los componentes de seguridades y factores de autenticación que requiere la Institución, así como la especificación en la infraestructura mínima necesaria para garantizar el correcto funcionamiento de la solución.
	El proveedor generará el plan de soporte técnico (mínimo 3 niveles) y de operaciones, el cual será previamente aprobado por la Institución y se aplicará durante el período de estabilización, acompañamiento de la iteración 1 y 2.
	El proveedor deberá contar con un equipo base conformado por: Líder de proyecto, analista de procesos y de sistemas, arquitecto de software y de base de datos, desarrollador java senior, tester, soporte, capacitador, supervisor del servicio de Call-Center, supervisor del servicio de envío de mensajes, teleoperadores y los especialistas de plataforma. *(Ver ANEXO 4) PERFILES POR ROL*
RECURSOS	El proveedor deberá considerar la disponibilidad de un especialista en la plataforma para el core de seguridades, el servicio de mensajería y call-center con el propósito de transferir el conocimiento necesario al área técnica para el uso, instalación, configuración del core de seguridades en todos sus componentes, y solventar imprevistos que se presenten. La disponibilidad por parte del proveedor de un especialista además permitirá la transferencia del conocimiento al área técnica del IESS sobre el software base necesario para soportar la solución en seguridades a implementarse.
	El personal del proveedor se someterá a talleres de introducción e inducción de conocimientos fundamentales sobre los procesos a nivel de negocio, estándares tecnológicos, la estructura organizacional de las unidades de negocio y área de desarrollo tecnológico, metodología y flujo de trabajo con áreas de apoyo tecnológico y buenas prácticas que maneja la Institución, el proveedor no facturará el valor de los talleres impartidos por parte del IESS el cual tendrá una duración aproximada de 1(un) mes. Esto con el fin de minimizar la curva de aprendizaje sobre la lógica del negocio y el desarrollo de la parte técnica en lo referente a estándares y buenas prácticas que la institución maneja. El proveedor una vez finalizado este primer mes de inducción, generará un cronograma de actividades a ser validado por las áreas involucradas de la institución, para: • Especificación referencial del proceso y normativa que deberá seguir esta solución informática en seguridades. El levantamiento de dichos procesos deberá realizar el proveedor con apoyo de los funcionarios asignados por las

COMPONENTES	DESCRIPCIÓN
	unidades de negocio correspondientes según el cronograma antes mencionado. • Desarrollo o integración de sus componentes con los sistemas especializados para usuarios de la intranet e internet, iteración 1 e iteración 2.
	En el caso que el proveedor requiera inducciones (posteriores al 1er mes de talleres de introducción e inducción) sobre algunas de las herramientas o procesos manejados por partes del IESS se las gestionará con las áreas técnicas o de negocio responsables, cuyo proceso será de mutuo acuerdo sin que el proveedor genere factura de cobro.

COMPONENTES	DESCRIPCIÓN
INSTALACIÓN Y CAPACITACIÓN	El despliegue de la solución deberá cumplir con el cronograma de trabajo establecido al inicio del proyecto entre la Institución y el proveedor, y no deberá exceder la fecha límite a no ser que existan razones que así lo justifiquen y hayan sido previamente analizadas por ambas partes y sujetas al control de cambios correspondiente y aprobación correspondiente por parte del IESS.
	La solución informática por cada iteración será configurada en ambiente de pruebas del IESS y probada por parte del proveedor y las áreas técnicas y funcionales de la Institución, previa al despliegue de la misma en ambientes de producción, con la emisión de informes de aprobación correspondiente según los modelos de calidad que defina la institución.
	La solución informática será configurada e instalada de manera que la información, los componentes y los aplicativos estén centralizados en el Data Center principal del IESS con esquemas de alta disponibilidad y balanceo de carga, además la solución deberá configurarse e instalarse en el centro alterno de contingencia en un esquema pasivo. En caso de requerir instalación de componentes adicionales para el buen funcionamiento de la solución a más de los mencionados en la sección *Arquitectura y Estándares* (del presente documento) en los servidores de aplicación que alojan los sistemas especializados, será responsabilidad del proveedor incluir las licencias, realizar las instalaciones y configuraciones necesarias sin incurrir en costos adicionales para la institución. Además la solución informática deberá ser configurada para los ambientes de pruebas de: desarrollo y pre-producción; mismos para los que el proveedor deberá proporcionar el licenciamiento correspondiente para habilitar estos ambientes.
	La solución informática a desplegarse en producción deberá contar con la capacitación de acuerdo al perfil de usuario designado por el IESS: funcionales y técnicos de las direcciones provinciales, sin que esto incurra en costos adicionales para la institución, además de esto la logística de dichas capacitaciones deberá ser responsabilidad del proveedor y planificada previamente con el administrador del contrato que designe la Institución. Por cada capacitación el proveedor deberá efectuar encuestas de satisfacción de los

<table>
<tr><th>COMPONENTES</th><th>DESCRIPCIÓN</th></tr>
<tr><td></td><td>asistentes.</td></tr>
<tr><td></td><td>El proveedor deberá incluir la entrega de una capacitación sin incurrir en costos adicionales para el IESS sobre los temas, componentes e implementaciones que hayan formado parte del desarrollo, dirigida al personal técnico del área de desarrollo.</td></tr>
<tr><td></td><td>Todas las capacitaciones deben ser dictadas antes de la puesta en producción de la solución y de la firma del acta de entrega recepción. Las capacitaciones se dictarán de forma presencial a las personas que designe la Institución y por instructores a cargo del proveedor certificados en las herramientas.

Los cursos serán dictados en idioma español en la ciudad de Quito en las oficinas del Oferente que deberá contar con un espacio y equipos adecuados y suficientes (un equipo por cada persona a capacitarse). La logística y planificación estará a cargo del proveedor de mutuo acuerdo con la Institución.</td></tr>
<tr><td></td><td>El proveedor deberá considerar las siguientes capacitaciones:
<table>
<tr><th>Tipo</th><th>Curso</th><th>Tiempo</th><th>Personas</th></tr>
<tr><td rowspan="4">Mecanismos de Seguridad</td><td>Capacitación para usuarios funcionales administradores de las unidades de negocio o direcciones provinciales</td><td>24 horas por cada grupo de 25 personas</td><td>50</td></tr>
<tr><td>Capacitación para técnicos administradores para mantenimiento de hardware y software</td><td>20 horas</td><td>10</td></tr>
<tr><td>Capacitación a técnicos (mesa de servicios) sobre Administración, configuración y uso de todos los componentes del sistema de seguridades</td><td>24 Horas</td><td>15</td></tr>
<tr><td>Capacitación a técnicos de desarrollo para futuros mantenimientos del software e integración con otras plataformas sobre :
• Componentes que conforman el sistema de seguridades para acceso, mecanismos de autenticación y autorización a los sistemas especializados.
• Componentes de seguridad integrados a los sistemas especializados
• Sobre la configuración, integración de los componentes del servicio de SMS y mailing (OTP) con los sistemas especializados involucrados en la solución.</td><td>24 Horas por cada grupo de 20 personas</td><td>40</td></tr>
<tr><td rowspan="3">Servicio de Call-Center</td><td>Capacitación dirigida a técnicos administradores de los servicios que intervengan en la interconexión con el Call-Center así como sobre la administración de la base de conocimiento</td><td>20 horas</td><td>10</td></tr>
<tr><td>Capacitación dirigida a técnicos Supervisores sobre el proceso operativo del Call-Center, base de conocimiento y uso del sistema de seguimiento y monitoreo.</td><td>20 horas</td><td>5</td></tr>
<tr><td>Capacitación a técnicos de mesa de servicios sobre las herramientas que permita la gestión de tickets, actualización de la base de conocimiento y demás componentes de este servicio</td><td>24 horas</td><td>10</td></tr>
<tr><td>Servicio de envió de mensajería vía</td><td>Capacitación dirigida a técnicos administradores de los servicios que intervengan en la integración del sistema de seguridades con el servicio de envío de mailing.</td><td>20 horas</td><td>10</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>COMPONENTES</th><th colspan="4">DESCRIPCIÓN</th></tr>
<tr><td></td><td colspan="4">
<table>
<tr><td>SMS y correo electrónico</td><td>Capacitación dirigida a técnicos Supervisores sobre el uso del sistema de seguimiento y monitoreo del servicio de mailing.</td><td>20 horas</td><td>5</td></tr>
<tr><td></td><td>Capacitación a técnicos de mesa de servicios sobre las herramientas de integración del core de seguridades con el servicio de mailing vía SMS y correo electrónico.</td><td>24 horas</td><td>10</td></tr>
</table>
El proveedor deberá considerar en caso de que no se mencione alguna capacitación de un componente o producto que conforma la solución, este deberá estar acompañado por una capacitación técnica administrativa y una funcional de un mínimo de 25 horas para 20 participantes
En todas las capacitaciones se debe además cubrir los temas de: resumen de procesos involucrados y normativa de la solución.
Los cursos serán dictados en fechas y horas a convenir. No se aceptará una carga horaria de más de cuatro (4) horas diarias. En caso de requerir un horario extendido de ocho (8) horas diarias para las capacitaciones deberá ser acordado entre las partes.
Cada capacitación deberá contar con un temario y cronograma entregado por el proveedor y la respectiva aprobación por parte del área de control de calidad del IESS y Administrador de contrato, además de estar acorde al manual de usuario, el cual será parte de los entregables. La logística de esta capacitación será responsabilidad del proveedor.
Se debe entregar un manual por participante para cada una de las capacitaciones y un manual adicional para la biblioteca del IESS.
El proveedor deberá emitir un certificado personal de aprobación acorde a la capacitación con la especificación de: fechas, número de horas y tema impartido.
</td></tr>
</table>

COMPONENTES	DESCRIPCIÓN
CALL - CENTER	Es importante puntualizar que el servicio de CALL-CENTER, fue dimensionado de manera referencial, y su capacidad definitiva se establecerá conforme a las necesidades de la prestación de servicios a sus asegurados. Como estimado se deberá atender 100.000 llamadas mensuales por el lapso de un (1) año a partir de la puesta en producción de la solución. El proveedor previo al inicio de este servicio deberá notificar la cantidad de tele-operadores con los que cuenta para cubrir esta demanda. El proveedor deberá considerar en la etapa de negociación del proceso de compra que la disminución de su oferta económica, no debe afectar a la cantidad mínima requerida (100.000 llamadas mensuales) de llamadas anuales.
	El proveedor será responsable de capacitar al personal del CALL-CENTER en el uso de los nuevos componentes de seguridad incorporados en los sistemas especializados, necesario para la prestación del servicio de soporte de primer nivel. EL proveedor deberá emitir un certificado de que todo el personal del CALL-CENTER se encuentra capacitado en el uso de los nuevos componentes de seguridad incorporados en los sistemas especializados expuestos al internet. Además deberá entregar el material necesario al personal del CALLCENTER que permita brindar un servicio de calidad, considerando la entrega de un ejemplar del material usada para la capacitación para incorporarlo a la biblioteca de la Institución.
	El proveedor debe considerar la asignación de las personas necesarias para trabajar como tele-operadores con el perfil pertinente y experiencia en atención al público. Estas personas tendrán que haber sido previamente entrenadas por el Proveedor, sin perjuicio de la inducción al material y procedimientos operativos del IESS. La fase de capacitación al personal de CALL-CENTER a cargo del proveedor, no podrá exceder los 30 días calendario, considerándose que esta fase deberá finalizar antes de la puesta en producción del sistema de seguridades en su iteración 1 (*ANEXO 6. Plan de Trabajo Referencial*). Las capacitaciones al personal del CALL-CENTER contendrá entre otros temas, los siguientes: • Detalles técnicos y de usabilidad del sistema, • Arboles de voz, • Implementación de los guiones, • Procesos lógicos, • Detalles de los informes, • Reportes gráficos y estadísticos del sistema y, • Requerimientos de software a cargo del Proveedor • Servicio de atención al cliente. Cada uno de los documentos generados en la fase de capacitación a personal de CALL-CENTER, se convertirán en "Anexos Técnicos del Contrato" y serán de estricto cumplimiento para el Proveedor.
	El servicio de Call-Center deberá pasar la fase de pruebas de funcionamiento según los procedimientos definidos con el área de control de calidad de la institución y deberá iniciar dicho servicio luego de la puesta en producción de la iteración 1 del presente proyecto (Implantación de mecanismos de seguridad y segundo factor). Fecha desde la cual se tomará como inicio para la contabilización de las llamadas para el pago de este

COMPONENTES	DESCRIPCIÓN
	servicio.
	Previo a la finalización del contrato el proveedor deberá realizar la transferencia del conocimiento a un grupo de personal que designe la Institución sobre la operación, procedimiento, información generada del CALL-CENTER.
	Bajo acuerdo de confidencialidad, el IESS se encargará de proveer el acceso de consulta a la información de las Bases de Datos necesarias para la prestación del servicio de CALL-CENTER. La veracidad de la información suministrada es de competencia del IESS. El proveedor deberá generar una interface básica o disponer de un servidor de integración para el acceso de consultas a la información de la base de datos que ponga a disposición la Institución; la información a proporcionar será: • Cédula de ciudadanía, RUC • Apellidos y Nombres, • Fecha de nacimiento • Tipo de afiliado: Afiliado activo, Afiliado voluntario, Pensionista, Cesante, Empleador, etc. • Nombre de Empleador actual. En caso de requerirse campos adicionales serán confirmados en el inicio del proyecto.
	El proveedor deberá contratar un enlace dedicado para acceso a las herramientas y base de datos de la institución.
	El proveedor deberá especificar el proceso (a validarse en conjunto con el personal de aseguramiento de calidad y mesa de servicios de la institución) a seguir para la atención de consultas realizadas por parte del usuario final y en caso de requerirse, escalamiento a un segundo nivel de soporte que será de responsabilidad de la institución a través del área de mesa de servicios.
	El proveedor deberá disponer de una herramienta de tickets para registrar la información de cada evento que ingrese al servicio de Call-Center.
	Por cada evento que atienda el personal de CallCenter deberá registrar la siguiente información mínima: • Consulta realizada por el cliente • Respuesta generada, obtenida del banco de preguntas frecuentes dentro de la base de conocimientos • Respuesta no generada del banco de preguntas frecuente • Resultado indicado por el cliente. • Notificación realizada a segundo nivel de soporte (en caso de requerirse) • Resultado emitido por el segundo nivel de soporte. • Catalogar la llamada si corresponde a soporte del core de seguridades o a otro módulo de negocio Toda la información generada de este proceso será de propiedad intelectual del IESS, quien solicitará periódicamente la entrega de las bases de datos obtenidas para realizar un seguimiento del servicio brindado al usuario final.

COMPONENTES	DESCRIPCIÓN
	El proveedor deberá proporcionar la información levantada en el formato que solicite la institución para que esta pueda ser integrada con la herramienta de tickets. Dicha información deberá ser proporcionada de forma diaria o en el período que se establezca en la fase inicial del proyecto
	El IESS NO proporcionará equipos, servicios, suministros, insumos, movilización, viáticos que no se encuentren mencionados expresamente en las presentes Especificaciones técnicas de la sección CALL - CENTER.
	El proveedor en conjunto con la Institución generará un banco de preguntas frecuentes, información que será socializada con el personal del CALL – CENTER con el propósito de contar con una fuente de conocimiento ante las consultas de los usuarios finales relacionadas al uso de los componentes implantados de seguridad en los sistemas especializados de la institución. El proveedor deberá frecuentemente proponer la actualización de la base de conocimiento en acuerdo con la institución, con el objeto de mejorar la calidad de servicio de CALL-CENTER, cada actualización del FAQ será con previa aprobación del IESS.
	El proveedor deberá disponer de una oficina independiente, en la que un funcionario de la Institución desempeñara las funciones de supervisor, a través de quien la contraparte del proveedor administrativa del Call-Center, canalizará los informes, validará el escalamiento al siguiente nivel de soporte (a cargo del área de mesa de servicio de la institución), y demás temas relacionados con el aseguramiento de la calidad de servicio brindado. El proveedor facilitará los accesos necesarios y la interface requerida para que el supervisor del IESS pueda verificar y hacer seguimiento de la calidad de servicio brindado al usuario final.
	El proyecto ha sido definido para brindar una cobertura a nivel nacional de atención de llamadas entrantes de consultas (sobre los nuevos componentes de seguridad incorporados en los sistemas especializados) en la modalidad 24x7x365 (veinte y cuatro horas diarias, siete días de la semana durante un año). Las llamadas entrantes serán atendidas por medio de asistencia telefónica por un tele-operador. El Proveedor proveerá al IESS un plan de continuidad de operaciones para eventos de emergencias con el fin de asegurar que el Servicio sea completamente funcional en la modalidad 24X7X365(veinte y cuatro horas, 7 días por semana durante 365 días al año).
	La planificación, administración y control del servicio de CALL-CENTER se llevará a cabo bajo la responsabilidad del proveedor con la supervisión del IESS.
	El proveedor deberá contratar un 1800 o Línea telefónica. Además de E1's necesarios para garantizar la calidad del servicio. El número de enlaces de comunicación E1's contratados debe ser equivalente al número estimado de llamadas diarias a ser cubiertas por el servicio de Call-Center.
	De requerirse por parte del proveedor realizar mantenimientos a la plataforma del servicio de Call-Center, se podrán realizar 3 eventos máximos al año, considerando para esto un horario 19:00 hasta 5:00am con una duración máxima de 3 horas por evento. Estas actividades deberán ser notificadas con 72 horas de anticipación, y previa a su ejecución deberán ser previamente autorizadas por la institución.
	Ajustes al Esquema de Atención y a la Capacidad El esquema inicial de atención, se modificará en relación al volumen real de llamadas recibidas. Para el efecto, el proveedor deberá brindar de manera oportuna (en 24 horas)

<table>
<tr><th>COMPONENTES</th><th>DESCRIPCIÓN</th></tr>
<tr><td></td><td>
la información y asesoría necesarias para que el Administrador del Contrato autorice/decida los ajustes/modificaciones pertinentes durante la primera semana de iniciado el servicio.
El Proveedor:

Analizará permanentemente la demanda, y sugerirá al IESS ajustes en los horarios de atención, así como aumentar o disminuir tele-operadores
Informará en un plazo de 24 horas calendario en el caso de que el Proveedor detecte que el nivel de servicio real está fuera de los límites establecidos, y sugerirá soluciones.
Entregará reportes semanales de actividad del servicio en general, y de los tele-operadores
Debe tener la capacidad de ajustar y distribuir el número de estaciones y líneas telefónicas necesarias para la atención y calidad del servicio, conforme el flujo de demanda entrante proyectada.

<h2>Componentes Tecnológicos y Funcionales</h2>
El Proveedor debe garantizar la disponibilidad de la infraestructura tecnológica necesaria, esto es: personal profesional, personal operativo, equipos y software para la prestación del servicio detallado de CALL-CENTER, de acuerdo con las especificaciones establecidas por el IESS detalladas en el presente documento.
En particular, el servicio de CALL-CENTER a proporcionar debe estar soportado por los elementos de hardware y software, que están considerados en la sección ANEXO 9 COMPONENTES PRINCIPALES CALLCENTER.

Elementos de Continuidad Operacional:

El Proveedor debe tener los siguientes elementos que garanticen una continuidad del servicio:

Redundancia en:

<table>
<tr><th>Descripción</th><th>Mandatorio</th></tr>
<tr><td>El enlace entre el CALL CENTER y el IESS, incluido redundancia en canales.</td><td>SI</td></tr>
<tr><td>Redundancia en los equipos activos y aplicaciones que se utilizarán en el Call Center.</td><td>SI</td></tr>
<tr><td>Troncales telefónicas (en caso de falla en canales principales)</td><td>SI</td></tr>
<tr><td>El Sistema Eléctrico por medio de un generador de energía (deberá contar con red eléctrica exclusiva, constituida para cubrir las necesidades del Call Center en caso de fallo en la electricidad o apagón).</td><td>SI</td></tr>
<tr><td>UPS para el centro de cómputo</td><td>SI</td></tr>
<tr><td>UPS para estaciones de trabajo</td><td>SI</td></tr>
<tr><td>Sistema de enfriamiento del centro de cómputo.</td><td>SI</td></tr>
</table>

Otros:

<table>
<tr><th>Descripción</th><th>Mandatorio</th></tr>
<tr><td>Herramienta(s) de respaldo y recuperación de la(s) Base(s) de Datos así como toda la información administrada por el Call Center.</td><td>SI</td></tr>
<tr><td>Contingencia del 50% del Sistema Telefónico mediante líneas análogas</td><td>SI</td></tr>
</table>
</td></tr>
</table>

COMPONENTES	DESCRIPCIÓN

Estaciones de Trabajo de Tele-operadores

- Los Tele-operadores en su turno respectivo deben laborar en estaciones de trabajo que cuenten con los siguientes elementos independientes (no compartidos):

Descripción	Mandatorio
Cubículo Independiente	SI
Diadema y filtro	SI
Enlace telefónico	SI
Equipo de Cómputo	SI
Acceso a Internet	NO

- Otros:

Descripción	Mandatorio
El CPU deberá tener deshabilitado el CD, Diskette, y todos los puertos USB	SI

Estadísticas y Reportes

El Proveedor debe estar en capacidad de generar reportes y consultas que deberá ser puestas a consideración del supervisor del IESS, relacionadas con el desempeño del servicio brindado por el CALL CENTER, que permitan analizar como mínimo la siguiente información:

1) Comparativo de Llamadas por día.
2) Comparativo de Llamadas por horario
3) Llamadas contestadas.
4) Llamadas perdidas y abandonadas.
5) Usuarios atendidos por puesto de trabajo, por tele-operador, por horario, por día.
6) Indicadores de niveles de servicio (90/10, porcentaje de llamadas perdidas)
7) Registro de preguntas más frecuentes
8) Motivos de llamadas.
9) Llamadas de quejas y reclamos.
10) Llamadas fueras del ámbito del alcance del servicio.
11) Promedio de llamadas vs accesos de consultas a la base de datos de la Institución.
12) Número de llamadas vs número de tickets (herramienta de registro de eventos atendidos por el Call-Center).
13) Porcentaje de casos correctamente categorizados o derivados
14) Porcentaje de casos pendientes de resolución
15) Porcentaje de llamadas resueltas en el primer contacto.
16) Porcentaje de satisfacción del cliente final
17) Porcentaje de requerimientos resueltos dentro de un especifico período de tiempo

COMPONENTES	DESCRIPCIÓN
	18) Porcentaje de casos escalados 19) Tiempo de espera de llamadas El IESS podrá solicitar otro tipo de consultas, informes y/o reportes según sus necesidades y de común acuerdo con el Proveedor. Los reportes serán dirigidos a los responsables designados en base a un formato y períodos acordados No obstante lo anterior, esta información será entregada conjuntamente con la factura correspondiente, sin perjuicio de que el IESS solicite estos reportes en un período de tiempo menor. El IESS podrá verificar en cualquier momento la calidad del servicio; para esto, El Proveedor deberá remitir estadísticas de gestión y cobertura de llamadas entrantes, de acuerdo con lo especificado en los términos de servicio. Adicionalmente el Proveedor dará acceso al IESS a su sistema tecnológico e instalaciones para la verificación de la atención al usuario final y obtención de información estadística relacionada con el servicio. Las partes desarrollarán procedimientos que aseguren la coordinación del envío de información y estadísticas entre el Proveedor y el IESS, sustentados por la documentación correspondiente.
	En la etapa inicial de la puesta en producción del servicio de Call-Center se deberá entregar al Supervisor del IESS informes de seguimiento diario hasta su estabilización del servicio, con el objeto de tomar correctivos en caso de necesitarse y garantizar la calidad en el servicio.
	El proveedor deberá presentar en su oferta el costo por llamada, se manejara dos precios: el precio total por llamada si corresponde a soporte en el uso de los componentes de seguridad (lo cual demandará un tiempo considerable de atención al usuario final), y un segundo precio equivalente al 30% del costo ofertado por llamada si la misma es de otro tipo.
	Otras Responsabilidades del Proveedor Adjudicado sobre el servicio de CALL-CENTER • **Enlaces:-** El Proveedor será responsable de la contratación y pago de los enlaces de datos necesarios entre las instalaciones del Proveedor y las instalaciones del IESS ubicadas en la ciudad de Quito, en la Veracruz y Av. NNUU, edificio de Riesgos del Trabajo, estos enlaces deberán tener redundancia como parte del aseguramiento de la disponibilidad del servicio, y el Proveedor será responsable de ampliarlo para no superar el 90% de saturación. • **Niveles de servicio.-** El PROVEEDOR ADJUDICADO debe priorizar el cumplimiento de los niveles de servicio establecidos en los Pliegos. • **Facilidades para supervisión.-** El IESS podrá supervisar físicamente y sin previo aviso las instalaciones donde se lleva a cabo la prestación del servicio, para lo cual deberá contar con las autorizaciones respectivas de ingreso. • **Coordinación**: Una vez iniciado el servicio de CALL-CENTER, el Proveedor deberá reunirse con el ADMINISTRADOR DEL CONTRATO para aspectos de coordinación periódica del servicio. Estas reuniones se mantendrán en los momentos que requiera el IESS en coordinación con el proveedor. • **Auditoría**: El PROVEEDOR debe aplicar auditoría de la calidad del desempeño de los tele-operadores, a cuyos resultados deberá tener acceso al IESS. En la propuesta, el PROVEEDOR debe hacer explícito el mecanismo que utilizará para auditar el

COMPONENTES	DESCRIPCIÓN
	trabajo de sus Tele-operadores en el CallCenter. Este mecanismo es diferente de las auditorías del contrato que realice el IESS • **Grabación**: Es obligatoria la grabación digitalizada del 100% de las llamadas. El registro de la grabación deberá incluir como mínimo la siguiente información: cuando se realizó la llamada (fecha/hora/minuto), persona que llamó y el tele-operador que la atendió. El Proveedor debe mantener las grabaciones por un período mínimo de seis (6) meses posteriores a la finalización de la llamada, período al final del cual deberán ser entregadas al IESS. De requerir el IESS una grabación que se encuentre aun en custodia del proveedor, esta deberá ser provista 24 horas luego de haberse presentado la petición. El Proveedor debe documentar el mecanismo con el que se identificará el registro o grabación de cada llamada y el procedimiento que se utilizará para ubicar a un usuario en particular. Adicionalmente, se debe identificar el tipo de medio que se utilizará para almacenar las grabaciones, así como el tipo de medio que se utilizará para entregar las grabaciones al IESS.
	El IESS no adquirirá obligación alguna de carácter laboral con el PROVEEDOR, ni con los empleados que el PROVEEDOR vinculare de cualquier forma para la ejecución del contrato.
	Con el objeto de garantizar la calidad de servicio de Call-Center, el IESS podrá solicitar por escrito posiciones fijas adicionales, con quince (15) días calendario de anticipación del inicio del servicio de las nuevas posiciones, manteniendo para el efecto los mismos costos.
	El personal para atención del CALLCENTER tendrá al menos los perfiles de: Teleoperador y Supervisor, mismos que se encuentran detallados en el *ANEXO 4. PERFILES POR ROL*

COMPONENTES	DESCRIPCIÓN
SERVICIO DE ENVIO DE MENSAJES VÍA CELULAR Y CORREO ELECTRÓNICO	Este servicio permitirá: - Enviar un mensaje a un número de celular o dirección de correo electrónico determinados. El estimado del número de mensajes que se esperan enviar en un año es de: 2’500.000 vía telefonía celular y 2’500.000 vía correo electrónico.
	Sobre el servicio de envío de mensajes vía correo electrónico; Si durante la ejecución del proyecto, en caso de que la Institución confirme disponer del servidor para soportar este servicio, el proveedor deberá realizar la transferencia de conocimientos necesaria al personal técnico de la institución para configurar el envío del OTP vía correo electrónico a través del servidor que estaría a cargo de la institución. Con lo cual se suspenderá el pago de este servicio, sin que esto signifique incumplimiento por parte del proveedor.
	Las configuraciones de parámetros de envío del servicio de correo electrónico serán definidas al inicio de la ejecución del proyecto.
	Para mensajes a ser enviados a través de telefonía móvil, se manejará una cadena alfanumérica de hasta 150 caracteres (sin espacios) de 7 bits, y cuyo encapsulado incluye una serie de parámetros. PARAMETROS DE LOS SMS vía telefonía móvil: Cuando un usuario recibe un SMS, se incluirán con su payload (carga útil o cuerpo del mensaje) al menos los siguientes parámetros: • Fecha de envío (también conocida como timestamp); • Número de teléfono del remitente y del destinatario;

COMPONENTES	DESCRIPCIÓN
	• Número del SMSC que ha originado el mensaje; De este modo se asegura el correcto procesamiento del mensaje en el SMSC y a lo largo de toda la cadena.
	Los tipos de mensajes a remitirse a través de este servicio (vía telefonía móvil y/correo electrónico) corresponden a: • Envió de código OTP para la verificación de una transacción económica o de actualización de datos críticos del usuario. • Envió de notificaciones sobre transacciones realizadas. Una vez estabilizada esta operación se prevé brindar funcionalidad adicional sobre los servicios que la Institución entrega a sus asegurados.
	Previo al inicio del servicio de envío de mensajes vía SMS o correo electrónico, se requiere un período preparatorio, el cual tendrá una duración máxima de 30 días calendario y debe cumplirse antes de la salida a producción, tiempo en el cual el proveedor configurará la plataforma necesaria integrada a la plataforma del IESS para brindar este servicio con calidad y menores tiempos de respuesta. El servicio de envío de mensajes (vía telefonía móvil o correo electrónico) deberá pasar la fase de pruebas de funcionamiento según los procedimientos definidos con el área de control de calidad de la institución y deberá iniciar luego de la puesta en producción de la iteración 1 del presente proyecto (Implantación de mecanismos de seguridad y segundo factor). Fecha desde la cual se tomará como inicio para la contabilización de los mensajes para el pago de este servicio.
	En la fase preparatoria el proveedor deberá capacitar al personal que brinde el servicio de envío de mensajes, reuniones en las que se tratará entre otros temas, los siguientes: • Detalles técnicos del sistema • Detalle de los informes • Reportes gráficos y estadísticos del sistema • Requerimientos de software El proveedor en acuerdo con el IESS desarrollará procedimientos que aseguren la coordinación del envío de información y estadísticas, sustentados en la documentación correspondiente. Cada uno de los documentos generados en la fase preparatoria, se convertirán en "Anexos técnicos del contrato" y serán de estricto cumplimiento para el proveedor.
	Disponer de un acceso para un funcionario de la Institución con el propósito de para realizar un seguimiento y medir la calidad de servicio de mensajería brindado.
	Una vez que se encuentre el servicio de envío de mensajes operativo, se solicitará conforme a condiciones que establezca la institución, la entrega por parte del Proveedor de informes diarios y consolidado mensual que se detallan a continuación: • Informe del total de mensajes enviados, con un desglose por operadora • Informe de los números de teléfonos a los que se envió los mensajes, según el medio de envío • Informe del nivel de servicio y disponibilidad del servicio. En caso de existir un cambio en la periodicidad de envío de estos informes será notificado por la institución.
	El proveedor deberá presentar en su oferta la tasa de despacho de mensajes en telefonía móvil, la misma que no deberá ser menos a 10 transacciones por segundo.

<table>
<tr><th>COMPONENTES</th><th>DESCRIPCIÓN</th></tr>
<tr><td></td><td>
Para él envió de mensajes vía correo electrónico se manejará la misma tasa de despacho de mensajes (10 transacciones por segundo).

El Proveedor deberá presentar en su oferta para el servicio de envío de mensajes vía telefonía celular, los costos finales que utiliza según los rangos (número de mensajes enviados) por operadora, tomando como referencia la siguiente tabla, con un mínimo de 2’500.000 mensajes.

Tabla de mensajes BULK (mensajes masivos)*

<table>
<tr><th colspan="3">Movistar</th></tr>
<tr><th>Desde</th><th>Hasta</th><th>Precio x Mensaje</th></tr>
<tr><td>1</td><td>100,000</td><td rowspan="11"></td></tr>
<tr><td>100,001</td><td>150,000</td></tr>
<tr><td>150,001</td><td>250,000</td></tr>
<tr><td>250,001</td><td>500,000</td></tr>
<tr><td>500,001</td><td>750,000</td></tr>
<tr><td>750,001</td><td>1,000,000</td></tr>
<tr><td>1,000,001</td><td>1,500,000</td></tr>
<tr><td>1,500,001</td><td>3,000,000</td></tr>
<tr><td>3,000,001</td><td>5,000,000</td></tr>
<tr><td>5,000,001</td><td>10,000,000</td></tr>
<tr><td>10,000,001</td><td>adelante</td></tr>
</table>
<table>
<tr><th colspan="3">Claro</th></tr>
<tr><th>Desde</th><th>Hasta</th><th>Precio x Mensaje</th></tr>
<tr><td>1</td><td>250,000</td><td rowspan="7"></td></tr>
<tr><td>250,001</td><td>500,000</td></tr>
<tr><td>500,001</td><td>750,000</td></tr>
<tr><td>750,001</td><td>1,000,000</td></tr>
<tr><td>1,000,001</td><td>1,500,000</td></tr>
<tr><td>1,500,001</td><td>2,000,000</td></tr>
<tr><td>2,000,001</td><td>en adelante</td></tr>
</table>
<table>
<tr><th colspan="3">CNT</th></tr>
<tr><th>Desde</th><th>Hasta</th><th>Precio x Mensaje</th></tr>
<tr><td>-</td><td>10,000</td><td rowspan="7"></td></tr>
<tr><td>10,001</td><td>20,000</td></tr>
<tr><td>20,001</td><td>30,000</td></tr>
<tr><td>30,001</td><td>40,000</td></tr>
<tr><td>40,001</td><td>50,000</td></tr>
<tr><td>50,001</td><td>100,000</td></tr>
<tr><td>100,001</td><td>300,000</td></tr>
</table>

Además deberá incluir en su oferta los costos de envío de mensajes a correo electrónico según los rangos que utilice con un mínimo de 2’500.000 correos electrónicos enviados.
El proveedor deberá considerar en la etapa de negociación del proceso de compra que la disminución de su oferta económica, no debe afectar a la cantidad mínima requerida (2’500.000 SMS y 2’500.000 correos electrónicos) de mensajes para este servicio.
</td></tr>
<tr><td></td><td>
Considerar un código corto de 3 o 4 dígitos a definirse en conjunto con la institución, único número a ser utilizado para el envío de mensajes al celular para todas las operadoras de telefonía móvil, que permitirá a los usuarios finales identificar que el SMS corresponde al generado por el sistema de seguridades del IESS.
El proveedor deberá contemplar la adquisición del código corto considerando los costos de inscripción y renovación para todas las operadoras celulares que intervengan.
</td></tr>
<tr><td></td><td>
El proveedor del servicio de envío de mensajes a telefonía móvil deberá contar con la capacidad de interconexión con todas las Operadoras que se encuentran funcionando en el mercado nacional.
</td></tr>
<tr><td></td><td>
El/los formatos de mensajes y el mecanismo de envío, serán definidos en conjunto con el área técnica de la institución al inicio de la ejecución del proyecto.
</td></tr>
<tr><td></td><td>
El proveedor deberá especificar y desarrollar el mecanismo de integración requerido a nivel de los sistemas especializados (en los que se incluya el segundo factor de verificación OTP) para el envío de mensajes; haciendo uso de la infraestructura que ponga a disposición el proveedor en el servicio de envío de mensajes.
</td></tr>
<tr><td></td><td>
De requerirse por parte del proveedor realizar mantenimientos a la plataforma de envío de mensajes, se podrán realizar 3 eventos máximos al año, considerando para esto un horario 19:00 hasta 5:00am con una duración máxima de 3 horas por evento. Estas actividades deberán ser notificadas con 72 horas de anticipación, y previa a su ejecución deberán ser previamente autorizadas por la institución.
</td></tr>
<tr><td></td><td>
Responsabilidad del proveedor

El proveedor en deberá considerar para el primer logueo del usuario:

Registro inicial de teléfonos celulares a los afiliados
Registro inicial de direcciones de correo electrónico

Responsabilidad del IESS

El IESS se compromete a lo siguiente:

Bajo acuerdo de confidencialidad el IESS se encargará de proveer la información

</td></tr>
</table>

COMPONENTES	DESCRIPCIÓN
	de la base de datos según se acuerde, necesaria para la prestación del servicio por parte del proveedor. La veracidad de la información suministrada en este punto es de competencia del IESS. • El IESS no proporcionará equipos, servicio, suministros, insumos, movilización, viáticos, que no se encuentren mencionados expresamente en esta sección.
	El IESS realizará visitas de inspección al Proveedor para determinar el cumplimiento de aspectos técnicos relacionados con la capacidad actual y potencial en infraestructura técnica y física.
	El proveedor en la plataforma para envío de mensajes vía telefonía celular o correo electrónico, debe considerar los siguientes factores: **Alta disponibilidad** • Plataforma completamente redundante • Seguridad del más alto nivel • Alta capacidad de carga • Eliminación de riesgo de puntos fallidos • Comunicación rápida **Seguridad Operacional** • No almacenamiento de información confidencial • Todas las comunicaciones encriptadas y por canal seguro • La infraestructura con la que cuenta el proveedor proporciona los niveles de seguridad necesarios para evitar fugas de información. **Políticas de Seguridad** • Seguridad Física • Seguridad de la Red • Seguridad del Host / Servers • Seguridad de la aplicación • Encriptación de datos **Cumplimiento de Seguridad** • Legislación Sanbanes-Oaxly sobre seguridad tecnológica – Sección 302 & 404 • ISO 17799 / BS 7799 / IEC 27001 / Seguridad física y digital • Fortalecimiento de Servidor – bajo las recomendaciones de la National Security Agency (NSA) **Proyecciones de Seguridad** • Obtención de Certificación PCI DSS • VISA Verified Compliance **Rendimiento de la plataforma dentro de la solución a implantarse en la institución:**

COMPONENTES	DESCRIPCIÓN
	• Uso de matrices de prioridad para diferenciar mensajes de alta prioridad vs mensajes de menor urgencia, con el objeto de manejar las colas de mejor manera. • Tasa estimada de envío por Operadora: 10 mensajes por segundo. Esta tasa estimada depende de: o El SMSC de Operadora o Número de conexiones a la Operadora.
	La Oferta técnica debe garantizar que el Proveedor será el responsable exclusivo de la calidad, oportunidad y cumplimiento de los diferentes componentes del servicio a prestar. El servicio de envío de mensajes será prestado de acuerdo con el detalle de las especificaciones técnicas contenidas en la presente sección.
	El proveedor deberá contar con un Software especializado y valido, actualizado permanentemente y que permita dar atención a los servicios de envío de mensajes vía telefonía móvil y/o correo electrónico.
	El proveedor deberá brindar el servicio de envío de mensajes vía telefonía celular y/o correo electrónico en modalidad 24X7X365 (24 horas al día, 7 días a la semana, en el transcurso de 365 días)
	Obligaciones adicionales del Proveedor y la Institución • El oferente deberá mantener un monitoreo continuo del desempeño de las aplicaciones y servicios ofertados, durante la vigencia del contrato; mismo que actuará como punto de contacto para informar sobre incidentes. • El proveedor suministrará una herramienta administrativa y de reportes, la cual será accesible vía protocolo HTTP seguro, donde se muestra el comportamiento transaccional en tiempo real del servicio.
	El proveedor deberá entregar un certificado de estar debidamente autorizado a proveer el Servicio de envío de mensajes (a través de telefonía móvil y correo electrónico).
	La instalación y configuración de todos los equipos y servicios involucrados estará a cargo del Proveedor, proceso que no tendrá costo extra para la Institución. Este proceso incluye absolutamente todas las tareas técnicas requeridas para entregar los bienes y servicios a plena satisfacción de la institución, aunque no estén detalladas explícitamente en el presente documento.
	El proveedor entregará los manuales técnicos de las configuraciones realizadas en todos los equipos involucrados para posibilitar el servicio de envío de mensajes tanto a nivel de telefonía móvil o a nivel de correo electrónico.
	Previo a la finalización del contrato el proveedor deberá realizar la transferencia del conocimiento al personal que designe la Institución sobre la operación, procedimiento, información generada del Servicio de envío de mensajes.
	El proveedor deberá describir el cumplimiento de los requisitos presentados y la arquitectura de software, hardware y comunicaciones con la que cuenta para soportar la cantidad de mensajes que la institución requiere manejar tanto a nivel de telefonía móvil como a través de correo electrónico.

Todos los documentos que el IESS requiera del proveedor están sujetos a revisión y aprobación por parte de la Institución, con el fin de verificar su veracidad y cumplimiento.

1 Indicadores de Niveles de Servicios

MATRIZ DE INDICADORES PARA EVALUACION DE PROYECTO – IMPLANTACION DE MECANISMOS DE SEGURIDADES							
TIPO	**SERVICIO**	**OBJETIVOS**	**VARIABLE**	**INDICADOR**	**PENALIZACIONES Y MULTAS**	**FRECUENCIA**	**DOCUMENTO VALIDADOR DE INDICADOR**
TIEMPO	**Gestión de Proyectos**	Cumplimiento del cronograma para entrega del proyecto	Cumplimiento de cronograma de puesta en producción del proyecto según planificación	Cumplimiento de cronogramas con una holgura del 10% en tiempo	El 1 por mil del monto total del contrato, por cada día de retraso contado a partir de la fecha de fin de proyecto con una holgura del 10% en tiempo.	A término del proyecto	Informe de Avance de Proyecto, estado y cumplimiento del cronograma del proyecto por parte del administrador de proyecto
ARQUITECTURA	**Arquitectura de Sistemas**	Disponibilidad del Core de Seguridades implantado para la atención para las transacciones generadas por las aplicaciones de la intranet e internet de producción	Porcentaje por hora de disponibilidad de las aplicaciones en producción durante la vigencia de la estabilización.	98% de disponibilidad en aplicativos	El 1 por mil del monto total del proyecto, por cada cuatro horas de no disponibilidad de los componentes de la solución en producción, contado a partir del reporte del incidente y al no contar con los tiempos de atención según el tipo de impacto crítico. Ref: Tabla de Tiempo de Diagnóstico y Solución a Fallos	Durante las fase de pruebas y acompañamiento	Reportes de mesa de servicios o producción con respecto a la no funcionalidad brindada por el proveedor.
ARQUITECTURA	**Arquitectura de Sistemas**	La solución debe soportar el nivel de concurrencia requerido, la misma que es generada por todos los sistemas especializados	Nivel de concurrencia para la respuesta a las transacciones generadas por los sistemas especializados considerando el total de usuarios definidos en los términos de referencia, o por el área de arquitectura siempre que se cumpla con las recomendaciones de software, hardware, redes y telecomunicación base del proveedor.	99% del nivel de concurrencia y transaccionalidad solicitado en los pliegos.	El 1 por mil del monto total del contrato, por cada día que no se tenga el nivel de concurrencia requerido.	Durante las fase de pruebas y acompañamiento	Reporte de indicadores generados por mesa de servicios o por control de calidad en ambiente de pruebas o producción.

NO FUNCIONAL	**Aseguramiento de la Calidad**	Cumplir con el número óptimo de iteraciones para la entrega de la documentación y/o productos requeridos.	Número de iteraciones por revisión de documento antes de cumplir con la fecha planificada de entrega final.	La documentación debe cumplir el 99% de aceptación por parte de los responsables. Máximo de 3 (tres) iteraciones (por cada documento entregado) de revisión antes de la entrega formal.	El 1 por mil del monto total del contrato por el número de iteraciones adicionales posteriores a la tercera iteración por cada entregable del proyecto.	A final de cada iteración	Informe de aceptación de los entregables por parte de todos los responsables de la validación del mismo.
NO FUNCIONAL	**Aseguramiento de la Calidad**	Cumplir con el número de iteraciones para fase de revisión de código, de los componentes desarrollados y personalizados para la institución.	Número de iteraciones por revisión de código antes de ser aplicado en pre-producción. En los productos que se entregue código fuente para mantenimiento.	La revisión de código debe cumplir el 99% de aceptación por parte de los responsables. Máximo de 3 (tres) iteraciones (por cada producto entregado) aceptadas antes de que el proyecto pase a ser aplicado en pre-producción.	El 1 por mil del monto total del contrato por el número de iteraciones adicionales posteriores a la tercera iteración de revisión de código por cada componente de la solución.	A final de cada iteración	Informe de revisión de código por parte del área de control de calidad
FUNCIONAL	**Aseguramiento de la Calidad**	Cumplir con el número de iteraciones para pruebas funcionales formales por las que pase el proyecto.	Número de iteraciones por pruebas funcionales formales de la solución informática antes de ser aplicado en producción.	Máximo de 3 (tres) iteraciones (por cada producto entregado) previas a la aceptación del paso a producción de la solución informática.	El 1 por mil del monto total del contrato por el número de iteraciones adicionales posterior a la tercera iteración.	En la etapa de pruebas funcionales previo al despliegue en producción de la solución	Informe o Matriz cruzada reporte de iteraciones de pruebas funcionales por QA
FUNCIONAL	**Aseguramiento de la Calidad**	Cumplir con el nivel de Satisfacción del usuario	Grado de satisfacción de los usuarios según las encuestas realizadas en la fase de pruebas	90% de nivel de satisfacción de los usuarios con el aplicativo que intervinieron en la aprobación del producto en la etapa de pruebas	El 1 por mil del monto total del contrato por cada encuesta que no cumpla con el nivel de satisfacción requerido.	En la etapa de pruebas funcionales previo al despliegue en producción de la solución	Encuesta de Satisfacción Estándar definida por QA
SOPORTE	**Monitoreo de Aplicaciones**	Mantener un canal de comunicación directo entre el proveedor y el área de mesa de servicios de la institución por un tiempo conveniente para dar solución a imprevistos en la adopción del aplicativo	Tiempo de soporte por medio de un canal directo con el proveedor	Soporte 24 / 7 / 365 disponiéndose de un canal de comunicación directa para solución de problemas en el aplicativo	El 1 por mil del monto total del contrato por cada requerimiento de soporte no atendido. Según los tipos de atención referidos en Tabla de Tiempo de Diagnóstico y Solución a Fallos	Durante la fase de estabilización y soporte	Informe del Coordinador de mesa de servicios y Gerente del proyecto sobre la atención del soporte realizado.

Si el valor de las multas excede el valor de la garantía de fiel cumplimiento, el IESS tendrá la potestad de dar por terminado el contrato anticipada y unilateralmente. Las multas impuestas no serán revisadas. ni devueltas por ningún concepto.

MATRIZ DE INDICADORES PARA EVALUACION DE PROYECTO – SERVICIO DE CALL-CENTER

TIPO	SERVICIO	OBJETIVOS	VARIABLE	INDICADOR	PENALIZACIONES Y MULTAS	FRECUENCIA	DOCUMENTO VALIDADOR DE INDICADOR
ARQUITECTURA	**Arquitectura de la solución**	Deberá gestionar ante la Corporación Nacional de Telecomunicaciones los reportes de saturación de servicio de los enlaces E1 y garantizar que el bloqueo de tráfico telefónico no sea mayor al 1%.	Número de bloqueos en el tráfico telefónico	Si el bloqueo de tráfico telefónico es mayor al 1%	Se establece una penalidad del 1% de la factura mensual de todo el servicio contratado para CALL-CENTER.	Mensual, después de la puesta en producción o cuando la Institución lo requiera	Reporte generado con apoyo del proveedor y validado / aprobado por el supervisor de la Institución.
FUNCIONAL	**Control de Calidad**	Al menos el 90% de las llamadas deben ser contestadas por un tele operador en 20 segundos o menos.	Número de llamadas que no son contestadas dentro del tiempo mínimo	Si el porcentaje de llamadas contestadas en más de veinte segundos es mayor o igual al 10%	Se establece una penalidad del 5% de la factura mensual de todo el servicio contratado para CALL-CENTER.	Mensual, después de la puesta en producción	Reporte generado con apoyo del proveedor y validado / aprobado por el supervisor de la Institución.
FUNCIONAL	**Control de Calidad**	El porcentaje de llamadas perdidas no debe sobrepasar del 1% de todas las llamadas recibidas. Se entiende como llamadas perdidas aquellas en que el llamante cuelga antes de ser atendido por el tele operador.	Número de llamadas perdidas (Llamadas que no se contestaron)	Si el porcentaje de llamadas perdidas excedió el 1%.	Se establece una penalidad del 5% de la factura mensual de todo el servicio contratado para CALL-CENTER.	Mensual, después de la puesta en producción	Reporte generado con apoyo del proveedor y validado / aprobado por el supervisor de la Institución.
FUNCIONAL	**Aseguramiento de la Calidad**	El 99% de las llamadas atendidas deben sujetarse a un estándar de servicio único (forma de saludar, de despedirse, de pedir que el cliente espere, etc.), que garantice la calidad y calidez del servicio, así como la uniformidad en la atención de las llamadas.	Modelo de calidad para valorar el nivel del servicio al cliente	Si el IESS determina que el porcentaje de uniformidad en atención de los tele operadores de asistencia telefónica es menor a 99%.	Se establece una penalidad del 1% de la factura mensual de todo el servicio contratado para CALL-CENTER. Para el efecto se establecerá este parámetro en base a un muestreo aleatorio del 0,5% de las llamadas atendidas en un día cualquiera dentro del período de facturación	Mensual, después de la puesta en producción	Reporte generado con apoyo del proveedor y validado / aprobado por el supervisor de la Institución.

FUNCIONAL	**Control de Calidad**	Cumplimiento del 99,95% de disponibilidad del servicio prestado por mes facturado. Se entenderá el concepto de disponibilidad del servicio, como el hecho que todos los componentes que el oferente utilice para prestar el servicio contratado, sean estos tecnológicos, recursos humanos, etc. estén disponibles las 24 horas del día, los 365 días del año.	Porcentaje de disponibilidad del servicio	Si el porcentaje de disponibilidad del servicio es menor a 99,95%.	Se establece una penalidad del 1% de la factura mensual de todo el servicio contratado para CALL-CENTER.	Mensual, después de la puesta en producción	Reporte generado con apoyo del proveedor y validado / aprobado por el supervisor de la Institución.
ARQUITECTURA	**Infraestructura**	El proveedor deber estar en la capacidad de incorporar nuevos agentes solicitados por el IESS que incluya la infraestructura, la capacitación (que tomaría 4 días) en el modelo de operación y demás elementos necesarios para disponer de nuevas posiciones en operación y cubrir la nueva demanda de llamadas.	Tiempo que se demora el proveedor para ampliar su capacidad del servicio	Si se presenta un atraso en la incorporación de nuevos agentes, que sobrepase los cuatro días calendario.	Se establece una penalidad del 1% de la factura mensual de todo el servicio contratado para CALL-CENTER por cada día de retraso presentado.	Mensual, después de la puesta en producción	Reporte generado con apoyo del proveedor y validado / aprobado por el supervisor de la Institución.
FUNCIONAL	**Control de Calidad**	El proveedor debe brindar acceso al IESS a su sistema tecnológico para la verificación y obtención de información estadística relacionada con el servicio.	Grado de disponibilidad de acceso por parte del proveedor al supervisor que determine la Institución	Si el proveedor no emite los usuarios de acceso para el supervisor del IESS para que este pueda confirmar los reportes emitidos y auditorías de control de calidad	Cierre unilateral del contrato	Mensual, después de la puesta en producción	Reporte generado con apoyo del proveedor y validado / aprobado por el supervisor de la Institución.
FUNCIONAL	**Control de Calidad**	Porcentaje de llamadas contestadas y resueltas por Call-Center debe ser de al menos el 90%	Porcentaje de llamadas contestadas y resueltas	Si el porcentaje de llamadas contestadas sin respuesta es mayor o igual al 10%	Se establece una penalidad del 1% de la factura mensual de todo el servicio contratado para CALL-CENTER.	Mensual, después de la puesta en producción	Reporte generado con apoyo del proveedor y validado / aprobado por el supervisor de la Institución.
FUNCIONAL	**Control de Calidad**	Porcentaje de reasignación de llamadas con tiempo de atención mayor a 10 minutos	Porcentajes de llamadas reasignadas después del tiempo máximo de atención	Si el porcentaje de llamadas contestadas tienen una duración mayor a 10 min y el	Se establece una penalidad del 1% de la factura mensual de todo el servicio contratado para CALL-CENTER.	Mensual, después de la puesta en producción	Reporte generado con apoyo del proveedor y validado / aprobado por el supervisor de la

				porcentaje es mayor o igual al 10%			Institución.

Si el valor de las multas excede el valor de la garantía de fiel cumplimiento, el IESS tendrá la potestad de dar por terminado el contrato anticipada y unilateralmente. Las multas impuestas no serán revisadas. ni devueltas por ningún concepto. En caso de que la Institución no contaré con el supervisor el área de Control de Calidad será la responsable de aprobar los reportes.
Las penalidades no son excluyentes; el monto final de la penalidad mensual es el resultado de la suma de las penalidades acumuladas de todos los niveles de servicio.
Si la penalidad máxima excede el 50% del monto de factura del mes, El IESS negará el pago de dicha factura por motivo de servicio deficiente.

MATRIZ DE INDICADORES PARA EVALUACION DE PROYECTO - SERVICIO DE ENVIO DE MENSAJERIA.

TIPO	SERVICIO	OBJETIVOS	VARIABLE	INDICADOR	PENALIZACIONES Y MULTAS	FRECUENCIA	DOCUMENTO VALIDADOR DE INDICADOR
FUNCIONAL	**Control de Calidad**	Entrega de reportes diarios sobre el envío de mensajes para seguimiento y control de los mismos, en caso de existir cambio en la periodicidad de los reportes debe ser confirmado por la institución	Número de días de retraso en la entrega de reporte según la periodicidad establecida por la institución.	Por cada día de retraso en la presentación de reportes.	Se aplicará el 1% de la factura mensual de todo el servicio contratado para mensajería, por cada día de retraso en la presentación de reportes.	Diario y mensual, después de la puesta en producción o cuando la Institución lo requiera	Reporte generado con apoyo del proveedor y validado / aprobado por el supervisor de la Institución.
FUNCIONAL	**Control de Calidad**	Cumplimiento del 99,8% de disponibilidad del servicio prestado por mes facturado. Se entenderá el concepto de disponibilidad del servicio, como el hecho que todos los componentes que el oferente utilice para prestar el servicio contratado, sean estos tecnológicos, recursos humanos, etc. estén disponibles las 24 horas del día, los 365 días del año.	Porcentaje de disponibilidad del servicio	Si el porcentaje de disponibilidad del servicio es menor a 99,8%.	Si el proveedor no garantiza el nivel de servicio indicado anteriormente, para lo cual dará un crédito de un treintavo (1/30) de los cargos mensuales por cada hora o fracción que el servicio de mensajería no cumpla con la disponibilidad del servicio mensual mínima del 99.8% las 24 horas del día, los 365 días del año.	Mensual, después de la puesta en producción	Reporte generado con apoyo del proveedor y validado / aprobado por el supervisor de la Institución.

NO FUNCIONAL	**Mantenimiento**	El proveedor podrá realizar cambios, actualizaciones, correcciones de errores, siendo estos planificados y coordinados con la institución. El proveedor deberá notificar con al menos 72 horas de anterioridad cualquier actividad. El mantenimiento podrá realizarse máximo por 3 ocasiones en el año además tendrá una ventana de trabajo de 19h00 hasta las 05h00 cualquier día del año, el servicio podrá ser interrumpido máximo por 3 horas.	Período de tiempo de la interrupción del servicio por mantenimiento	La interrupción del servicio no debe superar de las 3 horas y de las 3 veces al año. Además el tiempo de notificación a la institución debe ser de al menos 72 horas.	Se aplicará el 1% de la factura mensual de todo el servicio contratado para mensajería, por cada día de retraso en la presentación de reportes.	Cada mantenimiento que realice el proveedor	Reporte generado con apoyo del proveedor y validado / aprobado por el supervisor de la Institución.
FUNCIONAL	**Control de Calidad**	Al menos el 99,9% de los mensajes deben ser entregados a sus usuarios finales, en un promedio de 5 minutos para la entrega del mensaje.	Numero de mensajes que no sean procesados	El porcentaje del envío de mensajes no debe ser menor al 99,9%	Se establece una penalidad del 5% de la factura mensual de todo el servicio contratado para mensajería.	Mensual, después de la puesta en producción	Reporte generado con apoyo del proveedor y validado / aprobado por el supervisor de la Institución.
FUNCIONAL	**Control de Calidad**	El proveedor debe brindar acceso al IESS a su sistema tecnológico de mensajería para la verificación y obtención de información estadística relacionada con el servicio.	Grado de disponibilidad de acceso por parte del proveedor al supervisor que determine la Institución	Si el proveedor no emite los usuarios de acceso para el supervisor del IESS para que este pueda confirmar los reportes emitidos y auditorías de control de calidad	No iniciar con el proceso de pagos sobre el servicio debido a que se requiere que el supervisor valide los reportes de sustento.	Mensual, después de la puesta en producción	Reporte generado con apoyo del proveedor y validado / aprobado por el supervisor de la Institución.

Si el valor de las multas excede el valor de la garantía de fiel cumplimiento, el IESS tendrá la potestad de dar por terminado el contrato anticipada y unilateralmente. Las multas impuestas no serán revisadas. ni devueltas por ningún concepto. En caso de que la Institución no contaré con el supervisor el área de Control de Calidad será la responsable de aprobar los reportes.

Las penalidades no son excluyentes; el monto final de la penalidad mensual es el resultado de la suma de las penalidades acumuladas de todos los niveles de servicio.

Si la penalidad máxima excede el 50% del monto de factura del mes, El IESS negará el pago de dicha factura por motivo de servicio deficiente.

2 Plazo de Ejecución

El plazo de ejecución del contrato es de **25,3 meses**, contados a partir de su suscripción. En este tiempo se incluye la inducción del personal del proveedor por parte de la Institución en los procesos técnico y del negocio necesarios en el primer mes, el mismo que no es facturable para el Instituto.

A continuación se especifica la distribución macro estimada referencial de la planificación considerando que existen actividades que se ejecutarían en paralelo, para mayor detalle ver el *ANEXO 6 PLAN DE TRABAJO ESTIMADO REFERENCIAL*:

Iteración	Etapa / Fase	Tiempo (meses)
	Inducción	1
	Planificación	1
Uno	Implementación, levantamiento de la normativa, despliegue en producción y capacitación.	11
	Estabilización	1
	Acompañamiento	3
Dos	Implementación, despliegue en producción y capacitación	5
	Estabilización	1
	Acompañamiento	2
	Soporte en componentes de seguridades, servicio de Call-Center y servicio de envío de mensajería vía SMS y/o correo electrónico	12

3 SECCIÓN ANEXOS

ANEXO 1: Entregables Metodología RUP

Fase	Disciplina		Artefacto
Factibilidad (Líder IESS - PROVEEDOR)	Arquitectura		Documento de Arquitectura Referencial
			Mecanismos de Arquitectura Referencial
			Normas y Estándares de programación
			Acta de aceptación de propuesta Líder IESS - Líder PROVEEDOR (con apoyo de arquitecturas de las partes)
	Modelado del Negocio	Por Procesos	Levantamiento y optimización de procesos
			Acta de entrega - recepción y conformidad Levantamiento y Optimización de procesos
		Por casos de uso del Negocio	Visión del Negocio
			Modelo de Casos de uso del Negocio
			Especificación de casos de uso del negocio
			Diagrama de actividades
			Diagrama de clases de negocio (opcional)
			Diagrama de estados del negocio (opcional)
			Glosario de Términos (opcional)
			Acta de entrega - recepción y conformidad de Modelado del Negocio
	Administración de requerimientos		Visión del Sistema
			Modelo de casos de uso del Sistema
			Especificación de Casos de uso del sistema
			Revisión de especificaciones suplementarias
			Prueba de concepto (opcional)
			Acta de entrega - recepción y conformidad Administración de requerimientos
	Gestión del Proyecto		Cronograma Factibilidad
			Acta de negociación cronograma (Negocio - Líder IESS - Líder PROVEEDOR)
			Plan de Comunicación
			Especificaciones Suplementarias
			Lista de Riesgos, Matriz de Riesgos
			Matriz inicial de funcionalidades y componentes
			Plan de Desarrollo de Software (WBS General, Cronograma)
			Evidencia y Check List Control Calidad (Líder Analistas PROVEEDOR)
			Certificación Control Calidad (Líder Analistas PROVEEDOR)
			Informe Líderes con observaciones de calidad
			Evaluación de niveles de servicio (Líder IESS - Líder PROVEEDOR))
			Acta cierre de fase: entrega - recepción y conformidad (Negocio. Líder IESS - Líder PROVEEDOR)
Fase	**Disciplina**		**Artefacto**

Fase	Disciplina		Artefacto
Elaboración (PROVEEDOR)	Diseño	Vista de Diseño	Diagrama de clases de diseño
			Diagrama de secuencia de diseño
		Vista de Implementación	Diagrama de Componentes
		Vista de Despliegue (deployment)	
		Vista de Datos	Diseño de la Base de Datos
			Diccionario de Datos
		Gestión del proyecto	Evidencia y Check List Control Calidad (Líder Arquitectura PROVEEDOR)
			Certificación Control Calidad (Líder Arquitectura PROVEEDOR)
			Informe Líderes con observaciones de calidad
			Evaluación de niveles de servicio (Líder IESS - Líder PROVEEDOR y si se negocia esta fase sin Desarrollo e Implementación)
			Matriz de componentes afinada
			Acta cierre de fase: entrega - recepción y conformidad (Líder IESS - Líder PROVEEDOR)
Fase	Disciplina		Artefacto
Desarrollo (PROVEEDOR)	Implementación		Código
			Scripts de Base de Datos
			Evidencia de Pruebas Unitarias (Líder IESS - Líder PROVEEDOR - Analista Negocio)
			Evidencia de sincronización de código
			Evidencia Pruebas técnicas (Junit) (Líder IESS - Líder PROVEEDOR)
	Gestión del proyecto		Evidencia y Check List Control Calidad (Líder PROVEEDOR)
			Certificación Control Calidad (Líder PROVEEDOR)
			Informe Líderes con observaciones de calidad
			Evaluación de niveles de servicio (Líder IESS - Líder PROVEEDOR y si se negocia esta fase sin Implementación)
			Acta cierre de fase: entrega - recepción y conformidad (Líder IESS - Líder PROVEEDOR)
Fase	Disciplina		Artefacto

Fase	Disciplina		Artefacto
Implantación (IESS - PROVEEDOR)	Versionamiento y Control de Código		Informe de Control de Código y Versionamiento
	Deployment y Pruebas	Deployment	Plan de Despliegue
		Plan de pruebas	Funcionales
			Rendimiento y de carga
			Ambiente e Integración
		Evidencia Pruebas	Funcionales
			Rendimiento y de carga
			Ambiente e Integración
			No funcionales
			Encuesta satisfacción usuario
		Informe de errores y correcciones	
	Producción		Reporte de capacitación técnica
			Plan de operaciones
			Plan de soporte
			Manual de usuario
			Lecciones aprendidas
	Gestión del proyecto		Evidencia y Check List Control Calidad
			Check List Control Calidad
			Evaluación de niveles de servicio (Líder IESS - Líder PROVEEDOR)
			Acta cierre de proyecto (finiquito): entrega - recepción y conformidad (Líder IESS - Líder PROVEEDOR - Analista de Negocio)

Si bien se definen los entregables por fase de proyecto, la definición de los entregables que aplicarán a cada proyecto deberá ser definido por el IESS y el proveedor, considerando la criticidad de los mismos.

ANEXO 1.1: Artefactos técnicos

Además el proveedor deberá entregar para uso perpetuo del IESS previo a la aceptación del proyecto, los siguientes insumos asociados con la solución:

- Licencias de todos los componentes de la solución, de sistema base y hardware.
- Manuales de uso y técnicos de los mecanismos de seguridad instalados, así como de los demás módulos que intervengan en la solución.
- Manuales de instalación y configuración a nivel de servidores y en los clientes, de la solución de seguridades, servicio de Call-Center y servicio de envío de mensajes.
- Manuales técnicos de integración de los componentes de seguridad con los sistemas especializados (Dependiendo de su arquitectura) con la documentación técnica de respaldo.
- Fuentes de los componentes desarrollados o personalizados para la Institución y manuales técnicos.
- Documentación y modelado de los procesos avalados por las áreas responsables de la Institución:
    - Administración de seguridades a nivel nacional y por unidad administrativa.

- Autenticación y autorización incorporada en los sistemas especializados por tipo de usuario y unidad de negocio, tanto para la intranet como para el internet.
- Proceso de integración con el servicio de Call-Center
- Proceso de integración con el servicio de Mensajería vía SMS y correo electrónico.

ANEXO 2: Arquitecturas Referenciales

SERVIDOR DE APLICACIONES	ARQUITECTURA		
	PERISITENCIA	NEGOCIO	WEB
JBoss 4.2.3 y JBoss 5.1 EAP	JPA	EJB 3.0	JSF
JBoss 4.2.3 y JBoss 5.1 EAP	JPA	EJB 3.0	JSF (ADF)
JBoss 5 EAP	JDBC	JSP	JSP
IAS 9i, versión 1.3.22.0.1a	JDBC	JSP	JSP
OAS 10G, 10.1.2.0.2	JBDC	EJB 2.1	cocoon
JBoss 4.2.3	hibernate	spring	struts
JBoss 4.2.3	hibernate	spring	struts

ANEXO 3: Tiempo de Diagnóstico y Solución a Fallas

TIEMPO DE DIAGNOSTICO Y SOLUCION A FALLAS					
IMPACTO SOBRE LOS SISTEMAS AFECTADOS POR LA SOLUCIÓN	DEFINICION DE IMPACTO SEGÚN EL TIPO DE EVENTO	TIEMPO DE INICIO DE ATENCION (Horas Laborables)	TIEMPO DE DIAGNOSTICO (Horas Laborables)	TIEMPO DE SOLUCION DE FALLOS (Horas Laborables)	TIPO DE ASISTENCIA
Crítico	Todo aquel evento que impida el normal funcionamiento operativo de la aplicación parcial, total u ocasionen el funcionamiento inadecuado de sistemas relacionados.	1	1	Dependerá del diagnostico y aprobación del IESS	En Sitio
Grave	Todo aquel evento que retrasase de alguna manera la operatividad del funcionario sobre la aplicación.	1	3	Dependerá del diagnostico y aprobación del IESS	En Sitio
Menor	Todo aquel evento que implique solamente temas de forma con respecto a la aplicación.	4	4	Dependerá del diagnostico y aprobación del IESS	Remota o En Línea

Tipos de Asistencia	
TIPO	REFERENCIA
En Sitio	La asistencia será proporcionada por el proveedor con un recurso que haya formado parte en el desarrollo de la aplicación y posea el conocimiento necesario sobre la misma.
Remota	Con la resolución del problema en las instalaciones del proveedor y la entrega de la solución en el IESS.
En Línea	Con la resolución de problemas sobre el uso del aplicativo apoyando al área de mesa de servicios a través de un canal directo con el proveedor disponible las 8 horas laborables, 5 días a la semana de lunes a viernes.

NOTAS:	1. Si existiera el caso no consentido de algún problema en el SOFTWARE NUEVO se aplicarían los parámetros descritos en el cuadro "TIEMPO DE DIAGNOSTICO Y SOLUCION A FALLAS". El tiempo de solución no se especifica pues depende del diagnostico realizado.
	2. Cualquier BUG de la aplicación debe ser corregido a la brevedad posible sin costo adicional para el IESS.

ANEXO 4: Perfiles por Rol

ROL	PERFIL
Gerente de Proyecto	**Formación académica** • Formación de cuarto nivel en administración de empresas (MBA) o gestión de proyectos, o formación profesional universitaria en ingeniería de sistemas de computación y/o informática y/o afines. • Certificado PMP o cursos en gestión de proyectos según PMI. • Certificado RUP o cursos de metodología RUP. • Cursos de planificación, liderazgo, gestión de calidad, mando integral, organización y proyectos. **Experiencia y conocimientos** • Conocimiento de técnicas de formulación y evaluación de proyectos, análisis y desarrollo de sistemas de información y aplicaciones de software. • Experiencia de al menos 4 años de trabajo ocupando posiciones de liderazgo de proyectos. • Experiencia de al menos 5 años de trabajo en disciplinas del ciclo de desarrollo de software con tecnología JEE apoyados con Metodología RUP. • Certificado (s) (Actas de cierre de proyecto) de cada proyecto en el que a participado el Gerente de Proyecto de manera satisfactoria en soluciones informáticas. (obligatorio). • Deseable experiencia de al menos 1 año de trabajo con herramientas Rational Clear Quest. • Deseable conocimiento organizacional y negocio del IESS. • Deseable experiencia en proyectos de desarrollo de software y sistemas de información en el IESS. • Deseable conocimiento y experiencia en tecnologías de integración e interoperabilidad. **Funciones/Responsabilidades** El Gestor de Proyecto de TI desempeña una labor fundamental en el diseño, el desarrollo y los resultados de sus proyectos. El líder de proyectos ofrece soluciones a sus clientes y, por tanto, ofrece creatividad en respuesta a las necesidades de éstos. Para atender las demandas de sus clientes integra un grupo de especialistas a los que dirige y coordina, además de integrar sus ideas en una solución definitiva.
Analista de Sistemas y procesos	**Formación académica** • Formación profesional universitaria en ingeniería de sistemas de computación y/o informática y/o afines. **Experiencia y conocimientos** • Experiencia de al menos 3 años de trabajo ocupando posiciones de Analista de Sistemas aplicando metodología RUP, UML, DFDs y diagramas de procesos y levantamiento de requerimientos funcionales, casos de uso y casos de prueba. • Experiencia de al menos 3 años de trabajo ocupando posiciones de Analista de Sistemas haciendo uso de herramientas de modelado de procesos • Certificado (s) de cada proyecto en el que ha participado el Analista de Sistemas de manera satisfactoria en soluciones informáticas. (obligatorio). • Deseable experiencia de al menos 1 año de trabajo con herramientas Rational Software Architect. • Conocimientos de herramientas y técnicas de análisis de requerimientos. • Conocimientos y experiencia en análisis y diseño orientado a servicios y procesos del negocio. • Deseable conocimiento organizacional y procesos de negocio del IESS. • Deseable experiencia en proyectos de desarrollo de software y sistemas de

	información en el IESS. • Deseable cursos de metodología RUP. • Conocimiento en diagnostico, definición, control y evaluación de procesos de negocio • Conocimiento en normativa de especificación de procesos aplicando programas de mejoramiento continuo • Conocimiento en certificación de calidad y auditorías internas • Conocimiento en programas de sistematización **Funciones/Responsabilidades** La actividad principal del Analista de Sistemas y Procesos es coordinar la elicitación de requerimientos, especificar y mantener la especificación detallada de requerimientos, modelado de casos de uso de sistema para delinear la funcionalidad del sistema y delimitar el sistema; además la realización del diagnostico, especificación formal de procesos de negocio aplicando programas de mejoramiento continuo, y la generación de la normativa necesaria para amparar la implantación de la solución informática. Como una persona clave dentro del equipo de proyectos, debe tener la habilidad para colaborar efectivamente con otros miembros del equipo. Mantiene relaciones con el líder de proyecto, los analistas del negocio y Arquitectos. El análisis de los requerimientos y especificación formal de procesos tiene un alcance empresarial. Sus responsabilidades o deberes están en función de las políticas de la Tecnología de la Información (IT), la participación permanente en proyectos de TI y de los requerimientos de los sistemas.
Especialista de la plataforma	***<u>Referente a los componentes de Seguridades</u>*** **Formación académica** • Formación profesional universitaria en ingeniería de sistemas de computación y/o informática y/o afines. • Certificados oficiales sobre los productos ofertados • Certificados oficiales sobre la plataforma que soporta los productos ofertados **Experiencia y conocimientos** • Experiencia de al menos 3 años de trabajo ocupando posiciones como especialista de la plataforma ofertada • Conocimiento en instalación, configuración, administración de componentes de verificación de acceso a sistemas empresariales (Core de seguridades) y demás de funcionalidad para usuarios finales. • Conocimientos en instalación, configuración y administración en software base (plataforma) que soporte la solución ofertada. **Funciones/Responsabilidades** Es responsable de apoyar en la implantación, configuración, personalización de la solución y de transferir el conocimiento necesario al área técnica del IESS. ***<u>Referente a servicio de Call-Center</u>*** **Formación académica** • Formación profesional universitaria en ingeniería de sistemas de computación y/o informática y/o afines. • Certificados oficiales sobre los productos ofertados **Experiencia y conocimientos** • Experiencia de al menos 3 años de trabajo ocupando posiciones como especialista de la plataforma ofertada • Conocimiento en instalación, configuración, administración de Call-Center. **Funciones/Responsabilidades** Es responsable apoyar en la implantación, configuración, personalización y puesta en marcha del servicio de Call-Center. ***<u>Referente a servicio de Mensajería vía SMS o E-mail</u>***

	Formación académica • Formación profesional universitaria en ingeniería de sistemas de computación y/o informática y/o afines. • Certificados oficiales sobre los productos ofertados **Experiencia y conocimientos** • Experiencia de al menos 3 años de trabajo ocupando posiciones como especialista de la plataforma ofertada • Conocimiento en instalación, configuración, administración de mensajería móvil y mailing. **Funciones/Responsabilidades** Es responsable apoyar en la implantación, configuración, personalización y puesta en marcha del servicio de mensajería.
Supervisor de Servicio	***Referente a servicio de Call - Center*** **Formación académica** • Formación profesional universitaria en ingeniería de sistemas de computación y/o informática y/o afines. • Certificados oficiales sobre los productos ofertados **Experiencia y conocimientos** • Experiencia de al menos 3 años de trabajo ocupando posiciones como supervisor de Call-Center. • Capacitaciones en Servicio al Cliente y temas afines a CALL-CENTER **Funciones/Responsabilidades** Es responsable de supervisar y controlar el funcionamiento operativo del Call Center, asegurando que se cumpla la calidad de servicio ofertado. ***Referente a servicio de Mensajería vía SMS o E-mail*** **Formación académica** • Formación profesional universitaria en ingeniería de sistemas de computación y/o informática y/o afines. • Certificados oficiales sobre los productos ofertados **Experiencia y conocimientos** • Experiencia de al menos 3 años de trabajo ocupando posiciones como supervisor de servicio de mensajería móvil y mailing. • Capacitaciones en Servicio al Cliente y afines a servicio de mensajería móvil y mailing **Funciones/Responsabilidades** Es responsable de supervisar y controlar el funcionamiento operativo del servicio de mensajería móvil y mailing, asegurando que se cumpla la calidad de servicio ofertado.
Arquitecto de Software e Información	**Formación académica** • Formación profesional universitaria en ingeniería de sistemas de computación y/o informática y/o afines. **Experiencia y conocimientos** • Experiencia de al menos 5 años de trabajo ocupando posiciones de arquitecto de software en el desarrollo de sistemas con tecnologías JEE con metodología RUP. Además experiencia como Arquitecto de información en el desarrollo de sistemas con tecnologías Oracle con metodología RUP • Certificado (s) de cada proyecto en el que a participado el Arquitecto de Software y / 0 Arquitecto de información de manera satisfactoria en soluciones informáticas. (obligatorio).

	• Deseable cursos de arquitectura de sistemas de información. • Conocimientos de herramientas y técnicas de modelado y diseño de estructuras de datos. • Deseable cursos de Tecnologías de la información. • Conocimientos de herramientas y técnicas de diseño de componentes y servicios. • Conocimientos de XML, XSD, WSDL, WS, SOAP. • Conocimientos de marcos de referencia de Arquitectura Empresarial. • Conocimiento y experiencia en tecnologías de integración e interoperabilidad. • Conocimientos de arquitectura orientada a servicios. • Conocimientos de patrones de integración y SOA. • Deseable conocimiento organizacional y procesos de negocio del IESS. • Deseable experiencia en proyectos de desarrollo de software y sistemas de información en el IESS. • Deseable cursos de arquitectura de sistemas de información. • Deseable cursos de Tecnologías de la información. **Funciones/Responsabilidades** La actividad principal del Arquitecto de sistemas es el análisis y el diseño de alto nivel. Las personas que ocupen estos puestos trabajan con tecnologías y soluciones de software que son las bases fundamentales con los que se construye la Arquitectura de Sistemas y de Información Integrada de la Organización (IESS). Los arquitectos de sistemas e información tienen que vigilar el progreso técnico de un proyecto de TI para asegurar que se ajusta a la arquitectura o el diseño vigentes o los mejora. Un Arquitecto de Sistemas e información es la persona responsable de los aspectos de diseño de componentes de integración, servicios y de estructuras de datos. Dependiendo de sus respectivas funciones, los arquitectos de sistemas e información pueden realizar investigaciones y análisis, modelar y diseñar. El análisis y diseño de los componentes y diseño de estructuras de datos de la arquitectura tienen un alcance empresarial. Sus responsabilidades o deberes están en función de las políticas de la Tecnología de la Información (IT) y de los requerimientos de los sistemas.

Desarrollador Senior Java - PLSQL	**Formación académica** • Formación profesional universitaria en ingeniería de sistemas de computación y/o informática y/o afines. • Deseable cursos de herramientas de desarrollo. • Deseable cursos de arquitectura basada en componentes. **Experiencia y conocimientos** • Experiencia de al menos 5 años de trabajo ocupando posiciones de Desarrollador Senior en el desarrollo de aplicaciones de software con tecnologías Java JEE usando metodología RUP. • Certificado (s) de cada proyecto en el que a participado el Desarrollador Senior de JAVA de manera satisfactoria en soluciones informáticas. (obligatorio). • Certificado (s) de cada proyecto en el que a participado el Desarrollador Senior de PL/SQL de manera satisfactoria en soluciones informáticas. (obligatorio). • Conocimientos de IDEs de Desarrollo de BDD: TOAD, PL/SQL Developer, SQL Navigator. • Deseable experiencia de al menos 1 año de trabajo con herramientas Rational Clear Quest, Rational Clear Case. • Experiencia en desarrollo sobre servidores de Aplicación Oracle iAS y Jboss 4.2.3 y Jboss EAP 5.x. • Experiencia en desarrollo de software sobre las arquitecturas referenciales que maneja el IESS *ANEXO 2 ARQUITECTURA REFERENCIAL* • Conocimientos de IDEs de Desarrollo Java: Eclipse y Red Hat Developer Studio y Oracle Jdeveloper. • Conocimientos de JEE5 (Java 5) con los frameworks JSF 1.2, EJB 3.0 o superior. • Conocimiento de componentes JSF: Rich Faces-3.3.3 y ADF Rich Client. • Conocimiento de programación PL/SQL. • Conocimiento de herramientas y técnicas de diseño de componentes y servicios. • Conocimiento de tecnologías de primera y segunda generación de servicios Web. • Deseable conocimiento organizacional y procesos de negocio del IESS. • Deseable experiencia en proyectos de desarrollo de software y sistemas de información en el IESS. • Deseable cursos de herramientas de desarrollo. • Deseable cursos de SQL y PL/SQL. **Funciones/Responsabilidades** En este puesto, el desarrollador Java / PL-SQL, construye, prueba y mantiene aplicaciones y objetos de base de datos para atender las necesidades específicas de los clientes utilizando los lenguajes existentes, herramientas de desarrollo, etc. Además, conoce toda una serie de aplicaciones y cómo atender las necesidades de los clientes con aplicaciones reales y robustas. Las aplicaciones que desarrolla este tipo de desarrollador son aplicaciones empresariales integradas. Tiene que conocer los requisitos de sus clientes y las herramientas necesarias para reflejar esos requisitos en una aplicación robusta y desarrollar dicha aplicación de la forma más eficaz posible. Desarrolla software de capas de presentación, aplicación, integración, acceso a datos, y de objetos de base de datos. Es responsable del desarrollo y pruebas de componentes y servicios, en concordancia con los principios, estándares y mejores prácticas de

	Arquitectura de Sistemas y Arquitectura de información para los proyectos, para su integración en los sistemas.
QA- Tester	**Formación académica** • Formación profesional universitaria en ingeniería de sistemas de computación y/o informática y/o afines. **Experiencia y conocimientos** • Experiencia de al menos 3 años de trabajo ocupando posiciones QA-Tester realizando pruebas funcionales y no-funcionales del software. • Experiencia mínima de 2 años con herramientas de automatización de pruebas de software, tales como JMeter, HP LoadRunner, Borland Silk Performer, Perfomance Tester, SOAP-UI. • Deseable conocimiento y experiencia RUP. **Funciones/Responsabilidades** El probador es responsable de realizar las pruebas y registrar los resultados. Utiliza herramientas, técnicas y metodologías para el ciclo de vida de pruebas y las pruebas requeridas.
Capacitador	**Formación académica** • Formación profesional universitaria en ingeniería de sistemas de computación y/o informática y/o afines. • Cursos oficiales sobre los productos ofertados **Experiencia y conocimientos** • Experiencia de al menos 3 años de trabajo ocupando posiciones como Capacitador • Conocimiento en instalación, configuración, administración de componentes de verificación de acceso a sistemas empresariales y demás de funcionalidad para usuarios finales. **Funciones/Responsabilidades** El Capacitador es responsable de planificar, ejecutar y evaluar las capacitaciones de los productos desarrolladores o implantados; considerando la utilización de materiales didácticos necesarios para asegurar un alto nivel de comprensión.
Soporte técnico	**Formación académica** • Formación profesional universitaria en ingeniería de sistemas de computación y/o informática y/o afines. • Cursos oficiales sobre los productos ofertados **Experiencia y conocimientos** • Experiencia de al menos 3 años de trabajo ocupando posiciones como soporte técnico y despliegue de componentes de seguridad, servicios de Call-Center y servicios de envío de mensajes vía SMS o correo electrónico. • Conocimiento en instalación, configuración, administración de componentes de verificación de acceso a sistemas empresariales y demás de funcionalidad para usuarios finales. **Funciones/Responsabilidades** El Rol Despliegue y soporte técnico es responsable de la instalación, configuración de componentes de seguridades en las localidades que defina la institución, la planificación y ejecución del soporte a usuarios finales ajustado a la metodología del área de mesa de servicios.

ANEXO 5: Entregables de la Administración de Proyectos

Fase	Entregable
Inicio	0. Notificación de nuevo Programa /proyecto asignado
	1. Acta de Constitución del Proyecto
	2. Carta de Compromiso
Planificación	3. Plan de Proyecto, que incluye: plan de alcance, plan de tiempo, plan de costo, plan de calidad, plan de Recursos Humanos, plan de comunicaciones, plan de riesgos, plan de adquisiciones, plan de configuración y cambios.
	4. Cronograma de Proyecto
Ejecución	5. Minuta de Reunión
	6. Solicitud de Cambio
	7. Matriz de Riesgos y Plan de Mitigación de riesgos
	8. Documento de Seguimiento de Calidad
	9. Documento Seguimiento Administrativo
Monitoreo	10. Informe Estado de Avance
Cierre	11. Cierre técnico
	12. Cierre Administrativo (oficio)
	13. Lecciones aprendidas

Si bien se describen los entregables para la Administración del Proyecto, la definición de los entregables que aplicarán será definida por el IESS en la etapa inicial del proyecto.

ANEXO 6: Plan de trabajo estimado referencial.

Id	Id	Nombre de tarea	Duración	Predec
1	**1**	**Proyecto: IMPLANTACIÓN DEL MECANISMO BIOMETRICO EN LA ENTREGA DE CLAVES Y APROBACION DE CUENTA BANCARIA**	**760 días**	
2	**2**	**0 INDUCCION A PROVEEDOR NO FACTURADA**	**30 días**	
3	3	Inducción al proveedor sobre procesos, estandares y procedimientos a seguir	30 días	
4	4	Actas de socialización por parte de las áreas de la institución y proveedor	0 días	3
5	**5**	**1. INICIO**	**5 días**	**2**
6	**6**	**Acta de Constitución**	**5 días**	
12	**12**	**2. PLANIFICACION**	**30 días**	**5**
13	**13**	**Declaración de Alcance**	**10 días**	
14	**14**	**Documentación de Requisitos**	**7 días**	
15	15	Plan de Gestión Requisitos	4 horas	11
16	**16**	**Recopilación de Requisitos**	**5 días**	
17	17	Taller 1	2 días	15
18	18	Taller 2	2 días	17
19	19	Documento Requisitos	4 horas	18
20	20	Revisar y aprobar documento	4 horas	19
21	**21**	**Matriz de Trazabilidad**	**1,5 días**	
22	22	Elaborar Matriz	1 día	20
23	23	Revisar y aprobar matriz	4 horas	22
24	**24**	**Definir Alcance**	**3 días**	
25	25	Doc. Declaración de Alcance	1,5 días	23
26	26	Plan Gestión Alcance	1 día	25
27	27	Revisar, aprobar Doc. Alcance	4 horas	26
28	28	Doc. Alcance aprobada	0 días	26
29	**29**	**Estructura de División del Trabajo (EDT)**	**3 días**	
30	30	Especificar PDTs	1 día	28
31	31	Elaborar diagrama EDT	2 días	30
32	32	EDT elaborado	0 días	31
33	**33**	**Cronograma**	**3 días**	
34	34	Plan de Gestión Cronograma	1 día	32
35	35	Desarrollar Cronograma	2 días	34
36	36	Plan y Crongorama elaborados	0 días	35
37	**37**	**Presupuesto**	**1,5 días**	
38	38	Estimar Costos	4 horas	36
39	39	Plan Gestión	4 horas	38
40	40	Determinar Presupuesto	4 horas	39
41	41	Doc, Presupuesto elaborados	0 días	40
42	**42**	**Calidad del Proyecto**	**2 días**	
43	43	Línea Base de Calidad	4 horas	41
44	44	Matriz de Actividades	4 horas	43
45	45	Plan de Gestión de Calidad	4 horas	44
46	46	Métricas de Calidad	4 horas	45
47	47	Doc. Calidad elaborados	0 días	46
48	**48**	**RRHH**	**1,5 días**	
49	49	Plan de Gestión de RR.HH.	1 día	47
50	50	Matriz de Asignación de Responsabilidades (RAM)	4 horas	49
51	51	Doc. RRHH elaborados	0 días	50
52	**52**	**Plan de Gestión de Comunicaciones**	**2 días**	
53	53	Identificar Interesados	1 día	51
54	54	Plan de Gestión de Comunicaciones	1 día	53
55	55	Doc. Comunicaciones elaborada	0 días	54

56	**56**	**Plan de Riesgos**	**3 días**	
57	57	Identificar Riesgos	1 día	55
58	58	Realizar Análisis de Riesgo	1 día	57
59	59	Planificar la gestión y respuesta al riesgo	1 día	58
60	60	Doc. Riesgos elaborada	0 días	59
61	**61**	**Doc. Integral proyecto**	**4 días**	
62	62	Plan Integral del Proyecto	2 días	60
63	63	Presentación del proyecto	4 horas	62
64	64	Check List Fase	4 horas	63
65	65	Aprobación ODP/Interesado	1 día	64
66	66	Doc. Aprobada por ODP	0 días	65
67	67	Presentación formal proyecto	4 horas	66
68	68	Proyecto aprobado para ejecución	0 días	67
69	**69**	**3. EJECUCION ITERACIÓN 1**	**450 días**	**12**
70	**70**	**IMPLEMENTACIÓN Y DESPLIEGUE EN PRODUCCCION**	**330 días**	
71	71	Duración de la etapa	330 días	
72	72	LEVANTAMIENTO DE PROPUESTA DE NORMATIVA	0 días	
73	73	INSTALACION Y CONFIGURACION DE SERVIDORES DE AMBIENTES	0 días	
74	74	CAPACITACION A TECNICOS ADMINISTRADORES	0 días	
75	75	DESARROLLO E INTEGRACION DEL COMPONENTE DE SEGURIDADES CON SISTEMAS ESPECIALIZADOS PARA EL UNICO PUNTO DE ACCESO (SSO)	0 días	
76	76	DESARROLLO E INTEGRACION DEL SEGUNDO FACTOR PARA TRANSACCIONES (ACTUALIZACION DE DATOS, PRESTACIONES, RESETEO DE CLAVE)	0 días	
77	77	DESARROLLO DEL FRONT PARA IMPRESIÓN DE CLAVES CON EL NUEVO API	0 días	
78	78	DESARROLLO DE INTERFACES PARA ENROLAR USUARIOS AL NUEVO ESQUEMA DE SEGURIDADES	0 días	
79	79	MIGRACION DE USUARIOS, ROLES Y PERMISOS AL NUEVO CORE DE SEGURIDADES	0 días	
80	80	CONFIGURACIÓN DE POLITICAS DE SEGURIDAD PARA ACCESO A LOS APLICATIVOS	0 días	
81	81	GENERACIÓN DE REPORTES PARA AUDITORIA Y SEGUIMIENTO	0 días	
82	82	IMPLANTACIÓN, INTEGRACION Y CONFIGURACIÓN DEL SMS Y MAILING PARA OTP	0 días	
83	83	IMPLANTACIÓN, INTEGRACION Y CONFIGURACIÓN DEL CALL CENTER	0 días	
84	84	REVISION DE ENTREGABLES Y ACEPTACIÓN DE CONTROL DE CALIDAD DE LA INSTITUCIÓN	0 días	
85	85	PILOTO EN SISTEMA ESPECIALIZADO DE FUNCIONARIOS	0 días	
86	86	PUESTA EN PRODUCCION DE LA SOLUCIÓN	0 días	85
87	87	CAPACITACION A TECNICOS DESARROLLADORES	0 días	
88	88	CAPACITACION A FUNCIONALES	0 días	
89	89	CAPACITACION A SOPORTE/CALL-CENTER Y MESA DE SERVICIOS	0 días	
90	**90**	**ESTABILIZACION**	**30 días**	**70**
91	91	COMPONENTE DE LA SOLUCION	30 días	70
92	92	SMS	30 días	70
93	93	CALL CENTER	30 días	70
94	**94**	**ACOMPAÑAMIENTO**	**90 días**	**90**
95	95	FUNCIONAL	90 días	90
96	96	TECNICO	90 días	90
97	97	OPTIMIZACION DE BASES DE DATOS SEMESTRAL	90 días	90
98	**98**	**4. EJECUCION ITERACIÓN 2**	**240 días**	**90**
99	99	IMPLEMENTACIÓN DE SSO PARA INTRANET Y DESPLIEGUE EN PRODUCCION	150 días	90
100	100	CAPACITACION A TECNICOS DESARROLLADORES, FUNCIONALES, SOPORTE, CALL-CENTER Y MESA D	0 días	99
101	101	ESTABILIZACION	30 días	99
102	102	ACOMPAÑAMIENTO	60 días	101
103	**103**	**ETAPA DE SOPORTE**	**365 días**	
104	104	Soporte de Hardware y Software	365 días	70
105	105	Servicio de envío de SMS y correo	365 días	70
106	106	Servicio de CALL CENTER	365 días	70

ANEXO 7: Componentes informáticos de software y hardware

Descripción	Tipo	Cantidad	Licencias	Garantía
Servidores para el core de seguridades Principal	Software	La cantidad requerida para soportar la demanda de transacciones considerando un universo de 4'000.000 de usuarios, siendo esta cifra estimada para 3 años.	Perpetua e ilimitada.	Un año de garantía de buen funcionamiento de los bienes y sistemas implementados después de la puesta en producción.
Servidores para el core de seguridades esquema de alta disponibilidad, contingencia, ambiente de desarrollo y pruebas.	Software	Dos servidores pasivos, requeridos para establecer un esquema en el centro de cómputo principal activo-pasivo y en el centro de cómputo de contingencia un esquema pasivo. Además dos servidores con una capacidad limitada para uso de 2000 personas, este esquema servirá para ambientes de desarrollo y pruebas.	Perpetua e ilimitada.	Un año de garantía de buen funcionamiento de los bienes y sistemas implementados después de la puesta en producción.
Hardware, Software Base y Licenciamiento para servidores de los aplicativos a implantar y base de datos.	Hardware	Infraestructura necesaria en: hardware de servidores, almacenamiento, licenciamientos de Sistemas Operativos y software base adicional; tomando en cuenta los lineamientos emitidos por el IESS. Con el objeto de garantizar la funcionalidad requerida del servicio o aplicación a implementar.	Perpetua e ilimitada	Un año de garantía contra defectos de fábrica después de la puesta en producción.
Componentes de integración de los mecanismos de seguridades con los sistemas especializados para la verificación y autenticación (opciones de menú) del usuario.	Software	Considerar para 36 sistemas especializados.	Perpetua e ilimitada	Un año de garantía de buen funcionamiento de los bienes y sistemas implementados después de la puesta en producción.
Componentes de	Software	Licencia para sistemas	Perpetua e	Un año de garantía de buen

Descripción	Tipo	Cantidad	Licencias	Garantía
integración del segundo factor de autenticación OTP con sistemas especializados que representan transacciones de salida de dinero por parte de la institución.		especializados con transacciones que permitan confirmar salida de dinero y actualización de parámetros de seguridad del usuario; según se especifica en la sección "ARQUITECTURA Y ESTÁNDARES".	ilimitada	funcionamiento de los bienes y sistemas implementados después de la puesta en producción.
Desarrollo del módulo para posibilitar la impresión de la clave (nuevo API e interfaces) a los usuarios en las ventanillas de agencias del IESS, integrado con los componentes de verificación biométrica que ponga a disposición la institución.	Software	Entrega de fuentes generados por el proveedor	Perpetua	Un año de garantía de buen funcionamiento de los bienes y sistemas implementados después de la puesta en producción.
Migración de información de roles, opciones y permisos, del actual sistema de seguridades al nuevo core de seguridades a implantarse.	Software	Entrega de mecanismos de migración buscando evitar la duplicidad de información	Perpetua	Un año de garantía de buen funcionamiento de los bienes y sistemas implementados después de la puesta en producción.
Desarrollo del módulo de gestión de lista de observados	Software	Entrega de fuentes generados por el proveedor	Perpetua	Un año de garantía de buen funcionamiento de los bienes y sistemas implementados después de la puesta en producción.
Desarrollo del módulo de generación de información de auditoría para instituciones de control.	Software	Entrega de fuentes generados por el proveedor	Perpetua	Un año de garantía de buen funcionamiento de los bienes y sistemas implementados después de la puesta en producción.
Desarrollo del modulo de generación de reportes de seguimiento para las unidades de negocio.	Software	Entrega de fuentes de diez (10) reportes por tipo de usuario (internet e intranet) generados por el proveedor.	Perpetua	Un año de garantía de buen funcionamiento de los bienes y sistemas implementados después de la puesta en producción.
Servicio de Call-center	Servicio	Según la demanda de los usuarios finales del internet	Por un año	Un año de garantía según los SLA's definidos.
Base de conocimiento de Call-Center	Datos	Entrega de datos a la institución generados en el registro de eventos por llamada del usuario final asociados o no a la solución.	Por un año	Un año de garantía según los SLA's definidos.
Servicio de envío de	Servicio	Debe considerarse un	Por un año	Un año de garantía según

Descripción	Tipo	Cantidad	Licencias	Garantía
mensajes vía SMS y/o correo electrónico		universo de mínimo 5'000.000 de envío de mensajes / OTP: siendo 2'500.000 a través de telefonía móvil y 2'500.000 a través de correo electrónico; para confirmar una transacción que represente salida de dinero o actualización de información del usuario		los SLA's definidos.
Configuración de servicios de Call-Center y envío de mensajería	Servicio	Adquisición de las líneas para el call center Adquisición de los números cortos de todas las operadoras Configuración para mailing y dominio	Por un año	Un año de garantía según los SLA's definidos.

ANEXO 8: Catalogo de Sistemas Especializados

APLICATIVO	ÁMBITO	SERVIDOR DE APLICACIONES	ARQUITECTURA			
			PERSISTENCIA	NEGOCIO	WEB	BDD
Aplicativo 1	INTRANET	JBOSS 4.2.3	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 2	Internet	JBOSS 4.2.3	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 3	INTRANET	JBOSS 5	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 4	INTRANET	JBOSS 4.2.3	hibernate	spring	struts	Oracle 11G
Aplicativo 5	Internet	JBOSS 4.2.3	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 6	INTRANET	JBOSS 5	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 7	Internet	JBOSS 5	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 8	INTRANET	JBOSS 5	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 9	INTRANET	JBOSS 4.2.3	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 10	Internet	JBOSS 5	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 11	Internet	JBOSS 4.2.3	hibernate	spring	struts	Oracle 11G
Aplicativo 12	Internet	JBOSS 4.2.3	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 13	Internet	JBOSS 4.2.3	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 14	Internet	JBOSS 4.2.3	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 15	INTRANET	JBOSS 5	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 16	INTRANET	JBOSS 4.2.3	JPA	EJB 3.0	JSF (ADF)	Oracle 11G
Aplicativo 17	INTRANET	JBOSS 4.2.3	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 18	INTRANET	JBOSS 4.2.3	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 19	Internet	JBOSS 4.2.3	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 20	INTRANET	JBOSS 5	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 21	INTRANET	JBOSS 5	JPA	EJB 3.0	JSF (ADF)	Oracle 11G
Aplicativo 22	Internet	JBOSS 4.2.3	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 23	Internet	JBOSS 4.2.3	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 24	Internet	JBOSS 5	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 25	INTRANET	JBOSS 4.2.3	JPA	EJB 3.0	JSF	Oracle

APLICATIVO	ÁMBITO	SERVIDOR DE APLICACIONES	ARQUITECTURA			
			PERSISTENCIA	NEGOCIO	WEB	BDD
						11G
Aplicativo 26	Internet	JBOSS 4.2.3	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 27	INTRANET	JBOSS 4.2.3	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 28	INTRANET	JBOSS 5	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 29	Internet	JBOSS 5	JPA	EJB 3.0	JSF	Oracle 11G
Aplicativo 30	INTRANET	IIS 6.0	BPM			Oracle 11G
Aplicativo 31	INTRANET	Weblogic 10.3.6.0	BPM			Oracle 11G
Aplicativo 32	internet	JBOSS 5	JDBC	JSP	JSP	Oracle 11G
Aplicativo 33	Internet	IAS 9i, versión 1.3.22.0.1a	JDBC	JSP	JSP	Oracle 11G
Aplicativo 34	INTRANET	OAS 10G, 10.1.2.0.2	JBDC	EJB 2.1	cocoon	Oracle 11G
Aplicativo 35	INTRANET	OAS 10G, 10.1.2.0.2	JBDC	EJB 2.1	cocoon	Oracle 11G
Aplicativo 36	INTRANET	JBOSS 5	Portal			Oracle 11G

El total de los aplicativos a integrar con los componentes de seguridades se confirmarán en la etapa de planificación del proyecto.

Características agrupadas de los aplicativos Web desarrollados en el IESS

CANTIDAD	ÁMBITO	SERVIDOR DE APLICACIONES	ARQUITECTURA			
			PERISITENCIA	NEGOCIO	WEB	BDD
12	Intranet	JBoss 4.2.3 y JBoss 5.1 EAP	JPA	EJB 3.0	JSF	Oracle 11G
13	**INTERNET**	JBoss 4.2.3 y JBoss 5.1 EAP	JPA	EJB 3.0	JSF	Oracle 11G
2	Intranet	JBoss 4.2.3 y JBoss 5.1 EAP	JPA	EJB 3.0	JSF (ADF)	Oracle 11G
1	**INTERNET**	JBoss 5 EAP	JDBC	JSP	JSP	Oracle 11G
1	**INTERNET**	IAS 9i, versión 1.3.22.0.1a	JDBC	JSP	JSP	Oracle 11G
2	Intranet	OAS 10G, 10.1.2.0.2	JBDC	EJB 2.1	cocoon	Oracle 11G
1	Intranet	JBoss 4.2.3	hibernate	spring	struts	Oracle 11G
1	**INTERNET**	JBoss 4.2.3	hibernate	spring	struts	Oracle 11G

- Las aplicaciones bajo la arquitectura: JPA, EJB 3.0, JSF; poseen un componente centralizado para la autenticación y autorización.

ANEXO 9, Componentes Principales CALL-CENTER

Ítem	Descripción
Servidor Telefónico (Central Telefónica)	La central telefónica se basará en servidores telefónicos industriales de alta capacidad de procesamiento, que permiten administrar alta cantidad de posiciones simultáneas de Call Center, con una alta disponibilidad de la plataforma.
Servidor de Interacciones	Plataforma tecnológica la cual deberá tener la habilidad de integrar muchas aplicaciones. Con la facilidad de que estas puedan trabajar por separado.
PBX	Un completo switch digital capaz de manejar llamadas de la compañía telefónica o de otro PBX.
ACD	Distribuidor de llamadas totalmente automático que permite manejar ruteo de llamadas y gestión de distribución de tráfico. Las llamadas entrantes serán direccionadas al mejor agente que se encuentre disponible tomando en consideración la prioridad y el tipo de llamada.
IVR (Interactive Voice Response)	Sistema que permita proveer a los usuarios de las llamadas entrantes cualquier tipo de información tomada desde una base de datos, que permita transformar la información digital en información de audio para el usuario del servicio.
Mensajería Unificada	Sistema integrado de correo de voz, fax, e-mail con un servidor de correo. A su vez integrado al software telefónico
Fax Server	Servidor para el envío de faxes desde un computador central
Grabación de llamadas	Plataforma que permita obtener la grabación del 100% de llamadas tanto entrantes como salientes. Se debe garantizar un respaldo permanente de la información generada como consecuencia del servicio de Call Center prestado al IESS. De común acuerdo se debe establecer la periodicidad de entrega de los medios magnéticos con la información de respaldo.
CTI (Computer Telephony Integration)	Plataforma tecnológica que garantice la compatibilidad e integración de la infraestructura telefónica con cualquier sistema informático
Quality Assurance	La empresa contratista deberá contar con un área de control de calidad y métricas que monitoree a los teleoperadores de Call Center
CRM	Plataforma tecnológica que combina políticas, estrategia y procesos para gestionar la interacción con los clientes
Base de Datos	Software (DBMS) y servidor de base de datos
Marcación predictiva	Sistema que permita maximizar el rendimiento de un agente eliminando la marcación manual, optimizando tiempo de conexión
Service Desk	Plataforma tecnológica de apoyo para seguimiento y solución de problemas
Costos Telefónicos	Software de gestión telefónica y tarifación
Gestión Call Center	Software de Operación y Control del Call Center
Software de Administración	Panel de administración que permita al administrador el manejo de funciones, colas, indicadores de gestión, reportes, líneas y usuarios
Monitoreo en tiempo real	Capacidad para monitorear, evaluar e interactuar con un teleoperadores mientras este se encuentre en línea
Manejo de llamadas	Facilidad de realizar llamadas, contestar, desconectar, poner en espera, transferir bajo los perfiles asignados.
Screen Pop Up	El sistema abrirá “ventanas” automáticamente a los teleoperadores con información de un cliente en particular, extraída de bases de datos
Controles de Acceso	Cada teleoperador debe tener su propio usuario y contraseña individual, de acuerdo a los perfiles definidos para la atención por el IESS
Estado de Teleoperadores	El administrador podrá visualizar el estado de los teleoperadores

Estado de colas	Capacidad de revisar en línea el estado de las colas de atención, inclusive a nivel de teleoperador
Estado de líneas	Información sobre las líneas telefónicas, su estado, así como también la información de quién está conectado a ellas
Mensajes de audio personalizados	El proveedor deberá contar con el servicio y recursos necesarios para la grabación de los mensajes de audio que se transmitirán al usuario que se comunique con el Call Center.
Reportes de Gestión	Capacidad de generar consultas, reportes de seguimiento y monitoreo. La información estadística y de reportes podrá ser exportada a formato de hoja electrónica o en archivo separado por punto y coma, para que el IESS pueda realizar sus propios escenarios de análisis
Acceso Remoto	El CONTRATISTA deberá dar acceso al administrador del contrato, a facilidades de monitoreo vía TCP/IP, para que el IESS pueda analizar en cualquier momento el desempeño del Call Center.
Infraestructura LAN	100 Mbps mínimo categoría 6 mínimo
Enlaces	Soporte de conexión tipo E1 y TCP/IP para manejar el tráfico de las llamadas del servicio del IESS (Garantizar disponibilidad de 99,96%).
Sistemas de Evacuación	Para la seguridad de los teleoperadores el call center deberá disponer de sistemas de evacuación de emergencia.
Expansión y crecimiento	El PROVEEDOR debe contar con capacidad de expansión futura para atender otras necesidades/servicios que se requiera por parte de los usuarios de IESS (en al menos 100 posiciones adicionales a las requeridas).

ANEXO 10. LISTA DE APLICATIVOS DE INTRANET PARA INCORPORAR EL CONTROL DE ACCESO A NIVEL DE SISTEMA OPERATIVO.

- Servicios:
    - Portal de intranet e internet:
        - Liferay
    - Herramientas SOA/BPM:
        - Consola de Administración de Weblogic,
        - Enterprise Manager,
        - BPM Composer,
        - BPM workspace.
    - Herramientas de IBM Rational:
        - Asset Manager
    - Sistema de Gestión de trámites (Sobre plataforma Lotus)
    - Correo electrónico:
        - IBM Lotus 8.2

- Aplicaciones de escritorio:
    - Cliente de mensajería interna:
        - IBM Lotus Sametime.
    - Putty (cliente SSH, Telnet, rlogin, y TCP).
    - cliente SFTP gráfico para Windows que emplea SSH:
        - Winscp
    - RealVNC