Índice de Contenido

Índice de Figuras

3. Centros de Datos Nacionales, Software (OVA´s) y Ciberseguridad.

3.1 Centros de Datos Nacionales

La plataforma base computacional de hardware y software, serán proporcionados por La Entidad Contratante y estarán instalados en los Centros de Datos Nacionales de Quito (Iñaquito) y Guayaquil (Salitral), con la finalidad de centralizar y facilitar la administración de sus componentes, por lo que El Oferente debe acoplar y adecuar su solución a la infraestructura existente,

El Oferente debe realizar el aprovisionamiento, instalación y configuración del software necesario (OVAS´s) para soportar los procesos relacionados con la implantación del sistema AMI.

La Cabecera de la Plataforma AMI funcionará en modo activo - pasivo, es decir con una redundancia pasiva que estará en el Centro de Datos 2 en Guayaquil (Salitral), mismo que entrará en operación automática en caso de existir una falla con el Head End principal en el Centro de Datos Nacional 1 en Quito (Iñaquito). Además se implementarán 2 Enlaces Troncales del proveedor celular con el objetivo de tener redundancia en la comunicación, el Enlace troncal Principal será hacia el Centro de Datos Quito (Iñaquito) y el Enlace troncal Secundario hacia Centro de Datos Guayaquil (Salitral).

El tráfico que provenga de los medidores inteligentes deberá ser entregado hacia el HES (Principal), Si falla el Enlace Troncal Principal, el tráfico de las empresas pasará por Enlace Troncal Secundario hacia el HES que se encuentre activo.

De igual forma, en el caso de entrar en operación el HES (Secundario), las interfaces Web Service deberán enrutarse hacia el gateway Data Power de SAP ubicado en el Centro de Datos de Quito.

Tomando en consideración la plataforma base disponible en los Centro de Datos, El Oferente configurará en base a su experiencia, la arquitectura (combinación de hardware, sistema operativo, base de datos, storage, replicación, servidor de aplicaciones, seguridad, entre otros), que mejor se adapte a la solución propuesta.

El Oferente debe instalar y configurar los servidores virtuales necesarios y los componentes de software en 3 ambientes: Desarrollo, Preproducción-Pruebas y Producción, sobre la plataforma base proporcionado por La Entidad Contratante.

El Oferente debe considerar que en el caso que sea necesario crear otros ambientes para llevar a cabo simulaciones u otras actividades específicas, no habrá reconocimiento de ningún costo adicional.

Los ambientes de Desarrollo y Preproducción-Pruebas soportarán los desarrollos y las pruebas integrales de las aplicaciones, bases de datos, despliegues del sistema, además de nuevas versiones del software o parches.

El Oferente debe realizar el dimensionamiento de la solución planteada a fin de que La Entidad Contratante tenga claramente identificado cuáles son los requerimientos de hardware, software, storage, replicación, herramientas de gestión, herramientas de administración y comunicaciones que se requerirán para la implantación.

El Oferente debe implementar protección 1+1 Hot-Stand by entre los servidores instalados en los Centros de Datos Nacionales (Centro de Datos Iñaquito principal y Centro de Datos Salitral secundario) para el ambiente de producción, para lo cual La Entidad Contratante proporcionará el mismo hardware tanto para el Centro de Datos Iñaquito y el Centro de Datos Salitral.

El Oferente debe cumplir con los procedimientos, instructivo, políticas, estándares de Redes y Seguridad establecidos en los Centros de Datos en Quito y Guayaquil.

El Oferente será responsable del cumplimiento de los requerimientos presentados en este Anexo y en la demás documentación que son parte integral de este Proyecto.

3.1.1 Infraestructura existente Centros de Datos:

Como se muestra en la Figura 1. la infraestructura de hardware que dispone La Entidad Contratante consiste de la línea servidores IBM Power E880 de última generación, así como equipos de arquitectura X86 IBM PureFlex, que estarán configurados dentro de una red SAN de datos, utilizando equipos switches de canales de Fibra, y con conexión a un almacenamiento de alta capacidad y rendimiento modelo IBM XIV. Asimismo la solución contempla equipamiento para la gestión de respaldo y recuperación, tanto en disco (VTL) como en cintas de datos (LTO).

ANEXO A3

Figura 1. Sistemas de Hardware proporcionados por el Contratante.

En cada Centro de Datos, La Entidad Contratante va a proporcionar lo siguiente:

a) **Base de Datos Oracle 11g o 12c:** Servidor IBM Power E880 con sistema operativo AIX con capacidad de: 3 TB de almacenamiento, 2 cores para producción, 2 cores para pruebas y 1 core para desarrollo. Los recursos proporcionados y la capacidad de almacenamiento, La Entidad Contratante lo entregará bajo demanda durante la implementación y puesta en marcha del sistema, previa evaluación del uso real de los recursos. Los core son procesadores físicos y realizan una virtualización a través de herramientas IBM. El modelo es Power8 para base de datos, al momento todos los sockets están utilizados, sin embargo para este proyecto se van a asignar solo los recursos indicados en éste documento.

b) **Servidor de aplicaciones, red, seguridad, entre otros:** 3 nodos distribuidos en 2 servidores Pureflex, con arquitectura X86, con capacidad: 768 GB de RAM, 144 Cores (cada nodo tiene 2 procesadores y cada procesador 24 cores), 7 TB de almacenamiento, para los ambientes de prueba, desarrollo y producción. Los recursos proporcionados y la capacidad de almacenamiento, La Entidad Contratante lo entregará bajo demanda durante la implementación y puesta en marcha del sistema, previa evaluación del uso real de los recursos.

c) Lo que corresponde a Power E880 con sistema operativo AIX en el caso de las bases de datos, los recursos indicados corresponden a particiones lógicas del equipo, ya que éste cuenta con una cantidad mayor de recursos, el uso de cores para base de datos y almacenamiento es al 100% (2 cores para producción, 2 cores para pruebas,

1 core para desarrollo y 3TB) que se entregarán bajo demanda. Al momento el uso de estos recursos es del 0%, y los IOPS disponibles es de 120.000.

d) El modelo de procesadores es el X240 para arquitectura X86 y Modelo Power8 para Base de Datos.

e) De la memoria de los nodos de aplicaciones, se encuentra utilizado el 0% y se podrá entregar hasta el 35%.

f) Los Nodos se encuentran distribuidos en 2 chasis Pureflex, en uno de ellos se encuentran 2 nodos físicos y el otro nodo físico en el otro chasis; a nivel de ambiente virtual están conformados en un pool de recursos. Para los servidores Pureflex y Power 880 de base de datos, se encuentran conectados a través de un cluster conformado por dos Switch Core en el cual se han creado las siguientes VLANs: Producción, Administración, DMZ y Backup. En el caso que el oferente requiera instalar equipos adicionales en el Centro de Datos deberán integrarse con el Switch Core con base a la arquitectura utilizada por Centro de Datos Nacional y será responsabilidad del oferente la provisión de todos los componentes adicionales (cableado estructurado, módulos de fibra, fibras, patchcord, certificaciones) para la implementación.

g) Los equipos con los que cuentan el centro de datos para arquitectura X86 Pureflex con sus nodos, cuenta con sistema operativo instalado VMWare VSphere Standard, el cual tiene incorporada la funcionalidad HA.

h) Con respecto al equipamiento de arquitectura X86 los recursos se encontrarán compartidos con otros proyectos, por lo que cada oferente deberá dimensionar adecuadamente los requerimientos de hardware con el objetivo de optimizar y ser eficientes en el uso de recursos, sin que esto impacte en la operación del sistema, y se podrá asignar hasta el 35% de lo indicado bajo demanda.

i) Herramientas de virtualización VMWare ESXi 6.0 para los tres nodos Pureflex con sus respectivas licencias.

j) Licenciamiento perpetuo para la base de datos 11g o 12c, incluido soporte y mantenimiento.

k) Servidores de Directorio Activo para las arquitecturas Linux y Windows.

l) Infraestructura de seguridad perimetral (Firewalls de nueva generación).

m) Cableado estructurado, equipos de respaldo y protección eléctrica, refrigeración y respaldo de información.

n) La Entidad Contratante además va a proporcionar Servidores físicos instalados en base de datos Oracle 11g o 12c, los cuales servirán para albergar la información que requiera el proyecto, además tendrán comunicación hacia los servidores físicos que albergarán los servidores de aplicaciones (Servidores Virtualizados); para acceder a los mismos se contará con una seguridad perimetral que brindará el acceso a dichos servidores. En el caso de requerir equipamiento físico adicional a lo indicado deberá ser provisto por el oferente.

o) Para la Base de Datos Oracle 11g o 12c se entregará licenciamiento, soporte y mantenimiento por parte de la Entidad Contratante. En el caso de requerir otro producto adicional de Oracle debe ser provisto por el Oferente, tanto licenciamiento como soporte y mantenimiento.

p) Para respaldo y recuperación de Base de Datos Oracle se realiza con equipamiento en disco (VTL) como en cintas de datos (LTO).

q) La instalación y configuración de la de la base de datos Oracle y Sistema Operativos AIX para los ambientes de producción, pruebas y desarrollo, estarán a cargo de la Entidad Contratante.

r) El Centro de Datos dispone de un certificado digital tipo Wildcard para el dominio *.redenergia.gob.ec, Cualquier servicio expuesto para este dominio se encuentra cubierto por este certificado, en caso de que se requiera para el despliegue de la solución HTTP´s un nuevo dominio, deberá ser provista por el Oferente Adjudicado.

s) En el Centro de Datos Nacional Quito, se cuenta con un Firewall Fortigate 500E, con capacidad total 7.9 Gbps de ips y 5Gbps de NGFW, capacidad asignada bajo demanda y que será compartida con otros proyectos. La configuración que se

requiera en éste equipo estará a cargo de la Entidad Contratante de acuerdo a la arquitectura de la solución a implementar.

En el Centro de Datos Guayaquil, se cuenta con un Firewall Huawei, modelo USG5530, con capacidad hasta 10 Gbps, La configuración que se requiera en éste equipo estará a cargo de la Entidad Contratante de acuerdo a la arquitectura de la solución a implementar.

En el caso de requerirse módulos y/o componentes adicionales en cualquiera de los centros de datos nacionales, deberá ser provisto por el Oferente.

t) La infraestructura en Centro de Datos Quito y Centro de Datos Guayaquil en cuanto a modelos de equipos es la misma. Los recursos asignados para los ambientes de producción de este proyecto serán los mismos en ambos centros de datos. Los ambientes de desarrollo y pruebas estarán solamente en Centro de Datos Quito por lo que estos recursos serán asignados solo en esta localidad.

u) Toda la infraestructura antes indicada y con la cual cuenta actualmente el Centro de Datos y la que está comprometida para este proyecto, es responsabilidad de la Entidad Contratante. Si para la implementación y funcionamiento de este proyecto se necesita hardware, software y/o componentes adicionales, deberá ser provista por el Oferente.

v) Para este proyecto no se cuenta con mecanismo de replicación. El oferente para implementar su solución debe analizar el esquema más adecuado de replicación que se acople a su plataforma y está solución (módulos, componentes, software, hardware) deberá ser provista por el Oferente.

w) Los procedimientos, instructivos, políticas, estándares de redes y seguridad para los Centros de Datos se coordinará en etapa de diseño entre contratante y contratista, las cuales deben ajustarse a los procedimientos internos de seguridad de la información y estándares de tecnologías de la información con los que cuentan los Centros de Datos.

x) Se debe considerar, que solo en los casos que amerite, el Centro de Datos dispone de infraestructura de conectividad para servicios de acceso remoto (VPN SSL) y servicio de internet, debiendo el Oferente Adjudicado solicitar autorización para su

uso y para trabajos previamente justificados. Para el acceso a internet desde los servidores se realizará en forma controlada y específica a puertos y direccionamiento (No se proporcionará acceso abierto).

y) Los servicios de DNS y DHCP de la plataforma AMI a implementarse deberán ser provistos por el Oferente adjudicado.

3.2 Características del Software (OVA´S) y solución que debe proporcionar El Oferente para Centros de Datos

El Oferente debe proporcionar todo el software y hardware necesarios en los Centros de Datos para soportar los procesos relacionados con la implantación de los OVA´s del Head End principal y secundario según la arquitectura planteada (Figura 2) y debe proporcionar mínimo lo siguiente:

a) Sistemas operativos y su licenciamiento perpetuo de acuerdo a la solución a implementar, para los ambientes virtuales que van a ser instalados mediante VMware en los servidores Pureflex. Los sistemas operativos deben estar vigentes en el mercado, compatibles con los sistemas operativos que actualmente administra el Centro de Datos, para lo cual previa a la implementación, se deben revisar la compatibilidad y demás detalles que hagan posible la administración de estos componentes de software. Los sistemas operativos incluirán las licencias perpetuas, y de todos los servicios que requiera la solución. Los equipos con los que cuentan el Centro de Datos para arquitectura X86 Pureflex con sus nodos, cuenta con sistema operativo instalado VMWare VSphere Standard, el cual tiene la funcionalidad HA y Vmotion.

b) Licencias de acceso cliente, dependiendo del tipo de solución que El Oferente implemente y si lo requiera debe adquirir ese tipo de licenciamiento.

c) El Oferente debe utilizar para la gestión de usuarios los servicios de directorio disponible de los Centros de Datos Nacionales para los servidores y estaciones de trabajo. Se cuenta con Directorio Activo para ambientes Microsoft Windows y Open LDAP para ambientes de autenticación basados en open source linux.

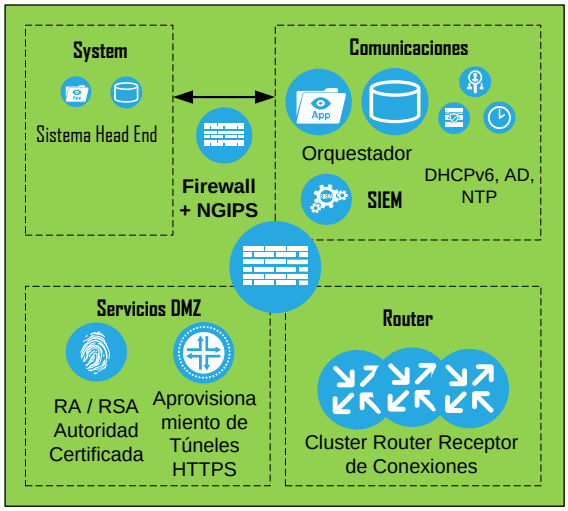

Figura 2. Arquitectura OVA´s Head End Centro de Datos Principal y Secundario

Si la Empresa Contratista necesita equipamiento físico que sea indispensable para cubrir el proyecto y que no conste en las especificaciones, debe ser solucionado en la etapa diseño y planificación en conjunto con La Entidad Contratante, el mismo que no deberá de tener costo adicional para La Entidad Contratante:

a) El equipo será de última tecnología/generación, fabricados en el año en que se tenga prevista la entrega a la entidad Contratante; elaborado, ensamblado, terminado y documentado; de conformidad con las normas de control de calidad vigentes del fabricante.

b) El equipo será nuevo y adecuado para las condiciones ambientales imperantes en los sitios de instalación.

c) Accesorios necesarios para su instalación, puesta en producción y seguridad.

3.2.1 Requerimientos Generales

La solución debe ser multiusuario que permita a las empresas eléctricas gestionar y monitorear sus medidores, red de comunicaciones entre otros, de manera individual.

La solución debe estar configurada y operativa en el idioma Español o Inglés.

La solución debe estar bajo la arquitectura SOA (Services Oriented Architecture). Todos los servicios deben interoperar a través de servicios web, REST/WSDL (Web Services Description Language)/SOAP (Simple Object Access Protocol).

En el caso de que la solución permita un acceso web, la solución debe ser de manera segura y avalada por una entidad certificadora (HTTPS).

Se deberán proveer los servicios de red y seguridad al menos de: DNS (Domain Name System), SNMP v2/v3 (Simple Network Management Protocol), DHCPv6 (Dynamic Host Configuration Protocol), NTPv4 (Network Time Protocol), AAA (Autenticación, Autorización y Auditoria), NMS (Network Management System), para el correcto funcionamiento de entornos de redes FAN (Field Area Network)/WAN (Wide Area Network).

El Oferente debe suministrar las licencias del sistema que se requiera para el correcto funcionamiento de toda la solución implementada en los Centros de Datos y Centros de Gestión.

La solución ofertada debe tener capacidad de funcionar en ambientes virtualizados.

El Oferente tendrá la responsabilidad del mantenimiento de todo el software con anterioridad a la entrega operando comercialmente y a satisfacción de La Entidad Contratante en el sitio estipulado.

3.2.1.1 Interfaz de Usuario

La Interfaz de usuario deberá ser totalmente funcional y cumplir mínimo con las siguientes guías de diseño:

a) Los usuarios deberán tener realimentación positiva y visual cuando hagan una selección, la cual debe permanecer visible hasta que la solicitud se complete o hasta cuando se realice una nueva selección.

b) Los botones de control, ayudas de navegación, ventanas de mensajes, ventanas emergentes y demás funciones de ventana deben tener apariencia, función y ubicación consistente, se debe hacer uso de colores y fuentes.

c) Los usuarios deberán poder navegar por diferentes pantallas u opciones de navegación, sin necesidad de tener que salir de la pantalla en el que se encuentra ubicado.

d) Se deberán suministrar las siguientes ayudas:

I. Hipervínculos que faciliten la navegación, para llegar a información más detallada rápidamente.

II. Opciones de navegación a Favoritos (sitios más visitados por el usuario en la aplicación, para agilizar la navegación a estas pantallas). Estos favoritos deben estar siempre visibles para el usuario.

III. Botones que permitan la Navegación hacia atrás y hacia adelante.

IV. Hipervínculos de alertas para que puedan ser exploradas por el usuario y así obtener mayor detalle de la situación que genera la alerta.

La Interfaz de Usuario deberá cumplir con las siguientes características:

a) La Interfaz de Usuario deberá tener un ambiente gráfico basada en navegador (GUI) disponible a nivel comercial, de manejo sencillo e intuitivo, de tal forma que se facilite el uso de la aplicación a los distintos usuarios que hagan uso de ella. Podrá estar en idioma inglés o español.

b) La interfaz de usuario gráfico, suministrado con el sistema, se ejecutará en todas las estaciones de trabajo de los Centros de Gestión y en todas las solicitadas por La Entidad Contratante.

c) La interfaz de usuario deberá permitir realizar tareas de consulta, gestión y configuración.

Se suministrarán módulos de ayuda para hacer más fácil la comprensión del sistema en cuanto a los módulos, programas y herramientas que lo conforman, considerando mínimo lo siguiente:

a) La ayuda deberá relacionarse con aquellas funciones mostradas en una ventana o campo en particular, para proveer acceso a los datos de la aplicación.

b) La ayuda deberá proveer capacidades de desglose para acceder a sub tópicos que son de interés particular del usuario.

c) La ayuda deberá crecer con las funcionalidades particulares de la implementación, sin que sea sobrescrita al momento de una actualización de la versión del Software.

3.2.1.2 Consultas y Búsquedas

El software proveído deberá contar con una herramienta de generación dinámica de consultas, que permita de una manera sencilla y visual, construir filtros con diferentes criterios para la obtención de diferentes tipos de datos. Los resultados de las consultas deberán estar disponibles para imprimir o para exportar a Hojas de cálculos, CSV, entre otros.

Proveer una herramienta de búsquedas que permita encontrar información almacenada. Se debe permitir que las búsquedas se realicen utilizando más de un campo, como los criterios de la búsqueda (combinación de campos) y búsquedas con caracteres comodines en diferentes campos.

3.2.1.3 Histórico

El Oferente en coordinación con La Entidad Contratante deberán definir conjuntos de datos del sistema que pueden ser archivados y removidos del sistema en producción.

El Oferente en coordinación con La Entidad Contratante deberán establecer reglas de archivamiento e históricos de datos (tiempos, datos, ruta de almacenamiento, entre otros).

La Entidad Contratante podrá definir el conjunto de datos, que estarán disponibles en el sistema de producción durante un tiempo parametrizable para reportes y análisis.

3.2.1.4 Tareas Programadas

Se debe permitir la creación de tareas programadas de acuerdo con la hora, día, período y otros eventos.

Las tareas programadas deben monitorear el inicio y finalización de las aplicaciones periódicas.

3.2.1.5 Versiones de Software

1. El Oferente debe entregar e implementar la última versión del Software liberada, estable y probada mundialmente y que esté disponible en la región.

2. El software debe disponer de mecanismos o planes de contingencia que permitan regresar a versiones anteriores en caso de fallos en el registro de nuevas versiones.

3. Durante el tiempo de garantía técnica del sistema, El Oferente deberá actualizar el software de cada uno de los componentes del sistema.

4. La Entidad Contratante y la Empresa Contratista podrán, según acuerdo mutuo, optar por actualizaciones (upgrades) adicionales al hardware o software en fecha posterior al plazo de garantía.

5. El Contratista será responsable de garantizar que todas las versiones de software entregado interoperen exitosamente en el sistema.

6. Si fuere necesario revertir a una versión anterior software para solucionar el problema de incompatibilidades entre hardware y software, El Oferente asumirá los costos y tiempos del "downgrade" e igualmente presentará un plan para corregir los problemas que se presenten con la versión más reciente. Esta corrección de problemas será a cargo del Oferente.

3.2.1.6 Sesiones de Usuario

1. La solución debe permitir el manejo de múltiples sesiones concurrentes para la gestión y operación del sistema.

2. El sistema debe estar diseñado para ambiente y acceso multiusuario, dicha cantidad de accesos no debe estar limitado ni por operación ni tampoco restringido o sujeto a una licencia; el desempeño va a depender totalmente de la capacidad y características de procesamiento y memoria de los servidores utilizados.

3.2.1.7 Fechas

La solución debe soportar años bisiestos, permitir la configuración de días feriados y otras fechas importantes.

3.2.1.8 Copias de Respaldo/Restauración (Backup)

El sistema deberá poder configurar servicios para copias de respaldo en forma automática y manual, de archivos y restauración de datos del sistema, con el equipamiento para la gestión de respaldo disponible de los Centros de Datos.

3.2.1.9 Licencia del software

Las licencias que conforman el sistema AMI serán perpetuas para los ambientes de desarrollo, pruebas, producción, ambientes de entrenamiento y cualquier back up alterno y

permitirán a las empresas eléctricas participantes, el uso de la aplicación e interfaces asociadas. El oferente debe incluir en su propuesta las restricciones de uso, si las tuviere.

Todo el software desarrollado por El Oferente (software, licencias entre otros) que no se contemple en el alcance del proyecto y que sea prioritario para el correcto funcionamiento del sistema no incurrirá en costos a La Entidad Contratante.

Las licencias deberán permitir múltiples instancias del sistema en desarrollo, pruebas y producción.

Se deberá incluir el listado de las licencias que requieran contratos de mantenimiento asociados a las mismas, los cuales deben tener una duración inicial como mínimo hasta la finalización de la garantía.

Se debe considerar la cantidad de licencias a proveer de acuerdo al dimensionamiento y número de medidores del proyecto.

Durante la vigencia de la garantía técnica, los precios para la adquisición de nuevas licencias deberán ser iguales o menores a los ofertados. Pasado ese período, y para los próximos diez (10) años El Oferente debe entregar la Política de precios que aplica para la adquisición de nuevas licencias de software para todos los componentes que forman parte de su oferta en el presente proceso.

3.2.1.10 Actualizaciones

1. El Oferente deberá tener mecanismos de implementación de actualizaciones, que garantice incorporar nuevas funcionalidades, pudiendo de esta forma arreglar alguna inconsistencia e incorporar mejoras, sin variar la funcionalidad del sistema. Además se deben realizar actualizaciones del software de aplicación que traten sobre seguridad cibernética.

2. Antes de ponerse en producción, las actualizaciones deberán ser aplicadas y probadas en el ambiente de desarrollo o pruebas.

3. El Oferente deberá cumplir con los siguientes requerimientos para versiones de Software:

    a) Las actualizaciones del Software deberán incluirse en el costo de soporte y mantenimiento anual.

b) El Oferente deberá garantizar la actualización (instalación, configuración, etc.) de nuevas versiones de Software sin costo adicional, dentro del periodo de soporte y mantenimiento.

3.3 Ciberseguridad

Un aspecto importante de la seguridad son los tipos de usuarios que pueden acceder a los diferentes componentes del sistema y las acciones permitidas a cada uno de ellos.

Se debe poder definir áreas de operación o grupos de perfiles, para cada empresa participante.

Los usuarios realizarán tareas de administración, operación y mantenimiento de los diferentes componentes del sistema. Se los puede clasificar en al menos los siguientes, para cada empresa participante:

a) Monitoreo.- Ejecuta únicamente comandos de consulta de información.

b) Operación.-Ejecuta gestión de alarmas, tarifas horarias, calendarios de lecturas, reseteo de demandas, cortes y reconexiones, entre otros.

c) Administrador.- Ejecuta gestión de comunicaciones, configura lo relacionado al rendimiento y fallas del sistema, mantenimiento del sistema, gestión de usuarios y acceso a todas las configuraciones de seguridad y del sistema.

d) Super-administrador.- Asignación de permisos a perfil Administrador, acceso para soporte y mantenimiento.

Se debe poder configurar nuevos tipos de usuarios de acuerdo a las necesidades de La Entidad Contratante. Se debe considerar separación de roles para funciones seguras y no seguras, los roles y responsabilidades de los usuarios deben ser especificadas, definidas e implementadas basadas en la sensibilidad de la información manejada por el sistema.

3.3.1 Manejo de cuentas de usuario

1. Se debe poder manejar las cuentas de usuario, incluyendo autorizaciones, configuración, modificación, revisión, inhabilitación y eliminación de cuentas.

2. Se debe poder identificar usuarios autorizados y especificar derechos de acceso y privilegios mediante el uso de listas de control de acceso.

3. Se debe poder inhabilitar las cuentas de usuario después de un periodo de tiempo predeterminado de inactividad.

4. Se debe evitar la creación de cuentas duplicadas.

5. Se deberá notificar a los administradores de cuentas cuando haya cambios en las cuentas de usuarios.

6. No se debe permitir el uso de cuentas anónimas, públicas y de invitado.

7. Se debe detectar las acciones realizadas sobre el sistema sin identificación ni autorización.

3.3.2 Control de Acceso

1. La lista de control de acceso debe ser manejada mediante la adición, modificación y eliminación de los derechos de acceso. Cualquiera de estas acciones deberán quedar registradas, para futuras acciones de auditoría.

2. Se deberán cumplir con las autorizaciones asignadas para el control de acceso al sistema en concordancia con políticas aplicables por parte de La Entidad Contratante.

3. Se deberá tener la habilidad para limitar a 5 números de sesiones simultáneas para cualquier usuario.

4. Se debe tener la capacidad de registrar ingresos exitosos, fecha-hora del último ingreso, intentos sin autorización y el número de intentos fallidos desde el último ingreso exitoso. Información que se almacenara en el log de eventos de la aplicación. El Oferente deberá entregar un reporte de logs post implementación, para verificar este cumplimiento.

5. Se debe limitar el número intentos fallidos por un usuario durante un periodo de tiempo dado.

6. Se debe bloquear la cuenta de usuario cuando el máximo número de intentos fallidos es excedido.

7. Las cuentas bloqueadas únicamente serán liberadas por un usuario con perfil de administrador o super-administrador.

8. Después de un determinado tiempo de inactividad, las sesiones remotas/locales y las interfaces de usuario deben bloquearse y permanecer en ese estado hasta que un usuario con su nombre de usuario y clave correctos lo desbloqueen.

9. El acceso remoto a los componentes del sistema con acceso remoto debe ser habilitados por un usuario administrador, solamente cuando sea necesario, el mismo deberá ser aprobado y protegido.

10. Todos los componentes del sistema con acceso remoto deben permitir que el acceso solo sea habilitado en concordancia con las políticas y con el nivel de autenticación que va a depender de la criticidad del sistema.

11. Se deben definir mecanismos de encriptación para proteger la confidencialidad e integridad de las sesiones de acceso remoto como mínimo AES 128 bits. Cualquier latencia inducida por el uso de encriptación, no debe degradar el rendimiento del sistema.

12. Se debe contar con mecanismos de Login para todas las interfaces del sistema.

13. Se deben implementar medidas de seguridad para restringir el ingreso de información al sistema. Únicamente el personal autorizado realizará acciones que podrían involucrar afectación de los componentes.

3.3.3 Manejo de Claves

1. Se deben acoplar a los procedimientos administrativos para: criterios iniciales del contenido de la clave, olvido de la clave.

2. Las claves deben hacer cumplir un nivel de complejidad (Longitud máxima/mínima, combinación de letras mayúsculas y minúsculas, números, caracteres especiales, etc.) para cada nivel de criticidad y las políticas de gestión de claves establecidas por La Entidad Contratante. De acuerdo a lo establecido en el reglamento interno de ciberseguridad de las empresas.

3. Se deben cambiar las claves de seguridad periódicamente.

4. Se deben cambiar las claves de seguridad por defecto luego de la instalación del sistema.

5. Se deben prohibir que las contraseñas se muestren cuando sean ingresadas (mediante el uso de asteriscos o cualquier otro método que oculte la información).

6. Se deben hacer cumplir restricciones en cuanto al tiempo de vida mínimo y máximo de las claves, cambiar y refrescar los claves de seguridad periódicamente.

7. Se deben prohibir la reutilización de claves.

8. Las claves no deben estar embebidas dentro de herramientas, códigos fuentes, scripts, alias o accesos directos.

9. Los equipos de campo (Hand Held o equipos móviles) no deberán grabar o almacenar información de los clientes, claves, llaves de encriptación, o cualquier otro tipo de información que pueda comprometer la seguridad del sistema; o en el caso de almacenar esta información, la misma debe tener tiempo de caducidad programada.

3.3.4 Desactivar servicios del sistema no utilizados

1. El Oferente ejecutará como parte de las actividades de post instalación y post configuración del Software, un “hardening”, siguiendo particularmente los métodos desarrollados por el proveedor original del Software, el Instituto Nacional de Normas y Tecnología (NIST) u organizaciones similares reconocidas.

2. El Oferente definirá y documentará el uso de puertos y servicios abiertos del sistema para todos los servidores previo a la puesta en producción.

3.3.5 Sistema Modular

1. El Sistema será diseñado y construido de manera Modular. No contendrá ningún mecanismo que desactive automáticamente una parte o la totalidad de sus funciones o que degrade su operación en cierta fecha o cuando ocurra un evento específico.

3.3.6 Disponibilidad (Control de Configuración y Gestión de fallas)

1. Se debe reconocer cuando existan órdenes de conexión/desconexión de un gran número de clientes sin cronogramas, notificar este hecho, suspender su ejecución hasta que la situación sea entendida y resuelta por el personal de la empresa.

2. Es de gran importancia para La Entidad Contratante que el sistema tenga la capacidad de realizar sus tareas específicas bajo condiciones normales y en condiciones de falla de algún módulo de Hardware o Software.

3. Se deberá proveer un plan de contingencia, plan de continuidad del negocio y recuperación de desastres en un esquema activo-pasivo y disponer de herramientas que permitan llevar el control de los planes.

3.3.7 Errores de Software

1. El hardware y software proporcionado por El Oferente deberá estar probado y certificado por el fabricante, en consecuencia, los errores en el software no deberán tener su origen en la plataforma proporcionada por la Contratista.

2. Se deben emplear controles para identificar y manejar condiciones de error, sin proveer información que puede ser utilizada por terceros. Los mensajes de error que contengan información detallada de la falla, deberá ser vista únicamente por personal autorizado.

3. Los mensajes de error desplegados por cualquier componente del sistema deben proveer información limitada de tal forma que no muestren información detallada de la operación interna del sistema. La información que se puede incluir debe mostrar información de diagnóstico (Ej. Datos de validación de errores), pero no debe proveer información a nivel de desarrollo. Los mensajes de error detallados deben ser transmitidos únicamente al servidor de registro de eventos designados.

3.3.8 Auditoria

1. El sistema debe contar con herramientas que permitan realizar auditorías periódicas de la seguridad y del funcionamiento del sistema AMI, para validar que los mecanismos de seguridad estén operativos y funcionen correctamente.

2. El sistema debe entregar reportes de auditoría.

3.3.9 Eventos Auditables

1. Los componentes del sistema deberán generar registros auditables, al menos de los siguientes eventos:

    a) Eventos de seguridad.

    b) Eventos de control.

    c) Cambios de la configuración.

    d) Inicio o encendido de las funciones de auditoría

    e) Ingresos al sistema exitoso o fallido.

    f) Autenticaciones fallidas de requerimientos de login o encriptados.

    g) Cambios en control de acceso o privilegios.

    h) Cambios en las configuraciones de seguridad.

    i) Creación, eliminación o modificaciones de usuarios, claves y llaves de seguridad, generación de alarmas en sensores de intrusión.

    j) Cambios en información crítica como lecturas de consumo, cortes y/o reconexiones, voltajes, etc. que se definirán en la etapa de diseño.

3.3.10 Contenido de los registros de auditoría:

1. Se deberá capturar la información suficiente y detallada en los registros de auditoría, para establecer que eventos ocurrieron, las fuentes de los eventos y sus resultados.

2. La información generada contenida en los eventos de auditoría deberá al menos contener la siguiente información:

    a) Fecha y hora del evento.

    b) El componente del sistema (dispositivo) AMI donde ocurra el evento (Software, hardware).

c) Tipo de evento.

d) Identificación del usuario/rol.

e) Las consecuencias operacionales en caso de un evento de operación.

f) Información detallada del evento.

3. Se debe tener la capacidad para incluir información más detallada en los registros de eventos de auditoría identificados por tipo, dispositivo que generó el evento.

4. Se debe tener la capacidad de manejar de una manera centralizada el contenido de los registros generados por componentes individuales a través del sistema.