Sociedad Eléctrica del Sur Oeste S.A.
Consuelo 310 - Arequipa - Tel.: (54) 381200 Fax: (54) 381199
seal@sealperu.com

SEAL

Ley 28612 LEY QUE NORMA EL USO DE ADQUISICIÓN Y ADECUACION DEL SOFTWARE EN LA ADMINISTRACIÓN PÚBLICA	**FECHA:** **12/10/2011**
INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE N° 11-2011 DS N° 024-2006-PCM	**N° PAGINAS: 10**

INFORME TECNICO PREVIO N° 11-2011
ADQUISICION DE LICENCIAS DE SOFWARE
Ley 28612

LEY QUE NORMA EL USO DE ADQUISICIÓN Y ADECUACION DEL SOFTWARE EN LA ADMINISTRACIÓN PÚBLICA

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE DS N° 024-2006-PCM

Aprobado por:

Ing° Edward Zárate Carlos
Jefe Unidad de Informática
Sociedad Eléctrica del Sur Oeste S.A.

Sociedad Eléctrica del Sur Oeste S.A.
Consuelo 310 - Arequipa - Tel.: (54) 381200 Fax: (54) 381199
seal@sealperu.com

Contenido

Sociedad Eléctrica del Sur Oeste S.A.
Consuelo 310 - Arequipa - Tel.: (54) 381200 Fax: (54) 381199
seal@sealperu.com

SEAL

I. NOMBRE DE AREA

Unidad de Informática

II. RESPONSABLE DE LA EVALUACION

Ing° Edward Zárate Carlos
Jefe Unidad de Informática
Sociedad Eléctrica del Sur Oeste S.A.

III. FECHA

12/10/2011

IV. JUSTIFICACION

Coadyuvar en implementar las recomendaciones y subsanar las debilidades de los Exámenes de Control OCI, enviados a través de Documento Interno GG/GPC-0115 -2011 siguientes:

Informe Largo de Auditoría Financiera- Ejercicio 2007 -Toledo y Lezama Contadores Públicos S.C.

Informe Largo de Auditoría Financiera y Aspectos Operativos – 2008

Memorando de Control Interno del Informe Largo de Auditoría Financiera al 31.12.2009

Revisión de la Estructura de Control Interno: Evaluación de las Tecnologías de la Información y Comunicación en SEAL 002-OCI-SEAL-CTD.

Informe Largo de Auditoría Financiera al 31.12.2010 003-2011-3-0134

V. ALTERNATIVAS

Se ha determinado que existen en el mercado los siguientes productos que cumplen con el requerimiento.

Para soportar la implementación de gobierno de TI alineado a Cobit 4.1

Methodware – Software de aplicación especializado, consolidado en el mercado nacional, latinoamericano y la comunidad económica europea, fabricado en Inglaterra.
http://www.methodware.com/

Meycor Cobit – Software de aplicación especializado, consolidado en el mercado nacional, latinoamericano y norteamericano, recomendado por ISACA Internacional, fabricado en Uruguay.
http://www.datasec-soft.com/en/content/blogcategory/8/22/

Soft Expert Cobit – Software de aplicación especializado, consolidado en el mercado nacional, latinoamericano y norteamericano, fabricado en Brasil.
http://www.softexpert.com/regulation-cobit.php

Para soportar la implementación de la NTP ISO-IEC 17799 buenas prácticas para la gestión de seguridad de la información v2

Callio Secura – Software de aplicación especializado, consolidado en el mercado nacional, latinoamericano y Norteaméricano, fabricado en EEUU.
http://www.callio.com/

Meycor KP – Software de aplicación especializado, consolidado en el mercado nacional, latinoamericano y norteamericano, recomendado por ISACA Internacional, fabricado en Uruguay.
http://www.datasec-soft.com/en/content/view/20/22/

Isosystem SGSI – Software de aplicación especializado, consolidado en el mercado nacional, latinoamericano y Norteamericano, fabricado en Brasil.
http://www.isosystem.com.pe

VI. ANALISIS COMPARATIVO

Se realizó aplicando la parte 3 de la Guía Técnica sobre Evaluación de Software para la Administración Pública aprobado por Resolución Ministerial N°139-2004-PCM.

a) Propósito de la evaluación

La evaluación de este software se realiza para determinar los atributos o características mínimas para el producto final software de soporte a la implementación de la NTP ISO-IEC 17799 v2 Buenas prácticas para la gestión de la seguridad de la información y soporte para la implementación del Gobierno Corporativo de TI alineado a Cobit 4.1.

b) Tipo de producto

Softwares de aplicación especializados.

c) Modelo de calidad

Se aplicará el Modelo de Calidad de Software descrito en la Parte I de la Guía de Evaluación de Software aprobado por Resolución Ministerial N° 139-2004-PCM.

d) Selección de métricas

Las métricas fueron seleccionadas en base al análisis de la información técnica de los productos de software ofertados, las cuales consisten en características del producto, requerimientos de información, entre otros.

En el Anexo I, se puede apreciar las características de los diversos productos. La información se obtuvo de las especificaciones de los productos publicadas en sus páginas web.

Del análisis realizado se ha determinado las siguientes características técnicas mínimas:

Ítem	Atributos	Descripción
Atributos internos		
1	Sistemas Operativos Estaciones de Trabajo	Microsoft Windows 98, Microsoft Windows NT Workstation, Microsoft Windows 2000 Professional y XP Professional

Ítem	Atributos	Descripción
2	Actualizaciones	Durante el periodo de garantía
Atributos externos		
3	Funcionalidad – Requisitos del negocio	Adecuación a requisitos del negocio
4	Funcionalidad – Adecuación	Integración de información de proyecto en un solo archivo
5	Funcionalidad – Interoperabilidad	Importar/exportar en distintos formatos
6	Usabilidad - Operabilidad	Compartir proyectos en red
Atributos de uso		
7	Usabilidad - Facilidad de uso	El manejo del software debe ser intuitivo y fácil de emplear, sin requerir constantes consultas a los manuales técnicos.
8	Usabilidad - aprendizaje	Manuales técnicos en CD, FAQS, comunidades/foros de consulta.
9	Soporte técnico a usuarios	Acceso a Knowledge Base de proveedor, consultas técnicas por teléfono o correo electrónico

e) Niveles, escalas para las métricas

Ítem	Atributos	Escala
Atributos internos		
1	Sistemas Operativos Estaciones de Trabajo	5
2	Actualizaciones	10
Atributos externos		
3	Funcionalidad – Requisitos del negocio	10
4	Funcionalidad – Adecuación	10
5	Funcionalidad – Interoperabilidad	15
6	Usabilidad - Operabilidad	10
Atributos de uso		
7	Usabilidad - Facilidad de uso	15
8	Usabilidad - aprendizaje	10
9	Soporte técnico a usuarios	15
	TOTAL	**100**

Cabe señalar que la comparación de los productos existentes en el mercado se hace solo para efectos de comparar y establecer características técnicas mínimas de estos tipos de software que sirvan para una posterior comparación y evaluación.

ITEM 01: Software de aplicación que soporte la implementación de la NTP-ISO/IEC 17799:2007 EDI Tecnología de la Información "Código de Buenas Prácticas para la Gestión de Seguridad de la Información", 2da. Edición.

ITEM 02: Software de aplicación que soporte la implementación de un Sistema de Control Interno de las Tecnologías de Información y Sistemas de Información basado en el modelo de Gobierno y Control COBIT 4.1

ITEM 01					
N°	FACTOR DE EVALUACION	ESCALA (MIN-MAX)	Meikor KP	Callio Secura	Isosystem SGSI
Atributos internos					
1	Sistemas Operativos Estaciones de Trabajo	0-5	5	5	5
2	Actualizaciones	0-10	10	10	10
Atributos externos					
3	Funcionalidad – Requisitos del negocio	0-10	10	10	8
4	Funcionalidad – adecuación	0-10	10	10	8
5	Funcionalidad – interoperabilidad	0-15	10	8	8
6	Usabilidad – Operabilidad	0-10	10	9	8
Atributos de uso					
7	Usabilidad – facilidad de uso	0-15	9	9	9
8	Usabilidad – aprendizaje	0-10	8	8	8
9	Soporte técnico a usuarios	0-15	15	12	12
	TOTALES	**100**	**87**	**81**	**76**

ITEM 02					
N°	FACTOR DE EVALUACION	ESCALA (MIN-MAX)	Meikor Cobit	Methodware	Softexpert Cobit
Atributos internos					
1	Sistemas Operativos Estaciones de Trabajo	0-5	5	5	5
2	Actualizaciones	0-10	10	10	10
Atributos externos					
3	Funcionalidad – Requisitos del negocio	0-10	10	8	10
4	Funcionalidad – adecuación	0-10	10	8	10
5	Funcionalidad – interoperabilidad	0-15	10	8	10
6	Usabilidad – Operabilidad	0-10	10	8	10
Atributos de uso					
7	Usabilidad – facilidad de uso	0-15	15	12	14
8	Usabilidad – aprendizaje	0-10	8	7	8
9	Soporte técnico a usuarios	0-15	15	10	15
	TOTALES	**100**	**93**	**76**	**92**

COSTO – BENEFICIO

Los precios de mercado lo determinará el estudio de posibilidades de mercado, no se tiene referencias respecto al precio de estos productos en el Perú, se estima el precio ambos productos incluidos los servicios de valor en US$ 30,000 incluido el IGV.

VII. BENEFICIOS

Gestión de Seguridad de Información:

La solución propuesta debe soporta la totalidad de requisitos para la implementación de un Sistema de Gestión de Seguridad de Información basado en el estándar ISO/IEC 27001 del año 2005 y los de la norma NTP/ISO-IEC 17799 v2 del 2007.

Permitir establecer requisitos de seguridad;
Selección de controles;
Factores críticos de éxito;
Desarrollo de directrices propias;
Categorías principales de seguridad;
Evaluación de riesgos de seguridad;
Tratamiento de riesgos de seguridad;
Política de seguridad de información;

Organización interna;
Seguridad en los accesos de terceras partes;
Responsabilidad sobre los activos;
Clasificación de la información;
Seguridad antes del empleo;
Durante el empleo;
Finalización o cambio del empleo;
Áreas seguras;
Seguridad de los equipos;
Procedimientos y responsabilidades de operación;
Gestión de servicios externos;
Planificación y aceptación del sistema;
Protección contra software malicioso;
Gestión de respaldo y recuperación;
Gestión de seguridad en redes;
Utilización de los medios de información;
Intercambio de información;
Servicios de correo electrónico;
Monitoreo;
Requisitos de negocio para el control de accesos;
Gestión de acceso a usuarios;
Responsabilidad de los usuarios;
Control de acceso a la red;
Control de acceso al sistema operativo;
Control de acceso a las aplicaciones y la información;
Auto evaluación de controles;
Informática móvil y teletrabajo;
Requisitos de seguridad de los sistemas;
Seguridad de las aplicaciones del sistema
Controles criptográficos;
Seguridad de los archivos del sistema;
Seguridad en los procesos de desarrollo y soporte;
Gestión de la vulnerabilidad técnica;
Reporte de eventos y debilidades de la seguridad de información;
Gestión de las mejoras en incidentes en la seguridad de información;
Aspectos de la gestión de continuidad del negocio;
Cumplimiento con los requisitos legales;
Revisión de la política de seguridad y de la conformidad técnica;
Consideraciones sobre la auditoría de sistemas;
Gestión documental;
Gestión de eventos de seguridad de información;

Control y Gobierno de las TI

La solución propuesta debe soportar la totalidad de requisitos para la implementación del marco de gobierno de TI basado en los "Objetivos de Control para los Sistemas de Información y Tecnologías relacionadas" COBIT 4.1 así lo requerido por la R.C. N° 458-2008-CG "Guía para la Implementación del Sistema de Control Interno de las Instituciones del Estado" en lo que corresponde a Tecnologías de Información y Sistemas de Información.

Organización del área de informática;
Plan de sistemas de información;
Permitir definir logros gerenciales de acuerdo al modelo de madurez de COBIT 4.1
Controles de datos fuente, de operación y salida;
Mantenimiento de equipos de computación;
Seguridad de programas de datos y equipos de cómputo;
Plan de contingencias;
Aplicación de técnicas de intranet;
Gestión óptima de software adquirido a medida por entidades públicas;
Permitir realizar una evaluación del desempeño de las actividades de cada proceso según el RACI chart de COBIT 4.1

Planeamiento de la administración de riesgos;
Identificación de los riesgos;
Valoración de los riesgos;
Respuesta al riesgo;
Segregación de funciones;
Evaluación costo beneficio;
Controles sobre el acceso a los recursos o archivos;

Controles para las tecnologías de la información y comunicaciones
- Definición de los recursos
- Planificación y organización
- Requerimiento y salida de datos o información
- Adquisición e implementación
- Servicio y soporte
- Seguimiento y monitoreo

Funciones y características de la información;
Información y responsabilidad;
Calidad y suficiencia de la información;
Permitir crear y gestionar proyectos de auditoría de TI basados en las guías de auditoría de COBIT.

Controles sobre los sistemas de información;
Herramienta de autoevaluación de acuerdo al COBIT 4.1 y COSO 2.

Gobierno de TI:
- Alineación estratégica;
- Entrega de valor;
- Administración de recursos;
- Administración de riesgos;
- Medición del desempeño.

Debe permitir el desarrollo y mantenimiento de sistemas de gestión basado en el ciclo de Deming durante el proyecto de implantación del gobierno de TI;
Permitir tratamiento de documentos y procesos, análisis de riesgos;

Debe incluir el proceso Aseguramiento del a Continuidad del Servicio documentado como DS4 en el COBIT 4.1.

Metas de negocio;
Metas de TI;
Procesos de TI;
Actividades clave;
Matrices RACI;
Indicadores claves de desempeño;
Indicadores claves de meta;
Modelos de madurez;
Pruebas de resultado de control;
Objetivos de control;
Pruebas de diseño del control;
Prácticas de control.

Debe permitir la administración de indicadores de gestión a través de un cuadro de mando integral de las tecnologías de información.

SERVICIOS COMPLEMENTARIOS

- Instalación y configuración remota de ambos productos;
- Capacitación on-site remota de ambos productos;
- Soporte y mantenimiento anual que incluye actualizaciones.

VIII. CONCLUSIONES Y RECOMENDACIONES

Existen en el mercado distribuidores autorizados de estos productos, lo más importante en una adquisición de este tipo es el soporte, actualización y mantenimiento garantizado de parte del fabricante.

Existen al menos 03 productos por cada software requerido que cumplen con los requisitos funcionales y técnicos, consecuentemente existente tanto pluralidad de productos como pluralidad de postores.

En cuanto al software de soporte a la implementación de la NTP ISO-IEC/17799 buenas prácticas para la gestión de la seguridad de información los productos más recomendable es o bien el Meikor KP o el Callio Secura.

En cuanto al software de soporte a la implementación de gobierno de las Tecnologías de Información alineado a Cobit 4.1 los productos más recomendables son Meikor Cobit Suite o el Soft Expert Cobit.

FIRMA

Sociedad Eléctrica del Sur Oeste S.A.
EDWARD ZARATE CARLOS
Unidad de Informática