

1. NOMBRE DEL ÁREA

Gerencia de Tecnologías de la Información

2. RESPONSABLE DE LA EVALUACIÓN

Jorge Guzman Salguero – Gerente de Tecnologías de la Información.

Enith Matías Herrera – Ejecutivo 1

Hernan Urrutia Lerma- Ejecutivo 2

Freling Ramirez Bautista - Profesional en Ingeniería de Sistemas

3. FECHA

20 de agosto de 2019

4. ASUNTO

Suscripción de Software de Registro y Seguimiento de Eventos para Servidores Windows

5. ANTECEDENTE

- El presente informe se ha elaborado sobre la base del Decreto Supremo N° 024-2006-PCM Reglamento de la Ley N° 28612 - Ley que norma el uso, adquisición y adecuación del software en la Administración Pública.
- Mediante R.M. 129-2012-PCM se aprobó el uso obligatorio de la NTP-ISO/IEC 27001. En 2013, Indecopi obtuvo la certificación internacional ISO 27001.
- Mediante D.S. N° 013-2003-PCM se dictaron las medidas para garantizar la legalidad de la adquisición de programas de software en entidades y dependencias del Sector Público. En cumplimiento de ello, se tiene que garantizar el uso de software legal en la institución.

6. JUSTIFICACIÓN

- El Indecopi cuenta con el servicio de Directorio Activo que es de alta criticidad, ya que soporta las conexiones de todos los usuarios para validar y permitir las autenticaciones a las diferentes aplicaciones y/o equipo. Este servicio es de vital importancia para la continuidad de las labores de la entidad.
- El Indecopi tiene implementado los servicios de almacenamiento de archivos (Servidores de archivos) en el cual brinda el acceso para leer, modificar, crear y eliminar archivos y/o directorios compartidos (que son de trabajo diario) a cada una de sus distintas áreas en la sede central y oficinas regionales. Estos servicios a su vez se encuentran integrados a la plataforma de autenticación (Directorio Activo).
- El Indecopi cuenta con servidores de servicios (IIS, impresión, servicio Desk, telefonía, GoGlobal y otros) los cuales son servicios de vital importancia para la continuidad de las labores de la entidad.
- Indecopi no cuenta con una herramienta que sirva de base para la gestión de la información almacenada, en términos de registro, disponibilidad, seguridad, integridad y seguimiento de eventos de autenticaciones a los servidores del directorio activo, servidores de archivos y servidores de servicios.

7. DESCRIPCIÓN DE LOS COMPONENTES DE SOFTWARE

Software de registro y seguimiento de eventos para Servidores de Archivos, Servidores de Servicios y Directorio Activo del Indecopi

8. USO O APLICACIÓN DE LOS COMPONENTES DE SOFTWARE SOLICITADOS

El Indecopi requiere contratar un Software que gestione y realice el seguimiento de los eventos de los Servidores de archivos, Servidores de Servicios y Directorio Activo del Indecopi, de tal manera que permita:

Directorio Activo:

- Rastrear la actividad de los usuarios administradores con información detallada que incluya: quién, que, cuándo, dónde y la estación de trabajo de los eventos registrados.
- Los eventos registrados deben contener los valores originales (antes del cambio) y los valores actuales (después del cambio).
- Enviar inmediatamente una alerta cuando ítems críticos son cambiados o cuando cambios en políticas vitales ocurren. Debe tener la capacidad de modificar la criticidad de un ítem.
- Registrar el inicio de sesión exitoso y fallido a los Servidores del Directorio Activo, el cual debe mostrar la fecha y hora, e historial de inicios de sesiones efectuados a dicho servidor.

Servidores de archivos:

- Registro y seguimiento de cambio en el servidor de archivos, así como los ficheros y/o directorios cambiados por los usuarios, eliminados, movidos o bloqueados.
- Rastrear la actividad de los usuarios y administradores con información detallada que incluya: quién, que, cuándo, dónde y la estación de trabajo de los eventos registrados.
- Registrar el inicio de sesión exitoso y fallido a los Servidores de Archivos, el cual debe mostrar la fecha y hora, e historial de inicios de sesiones efectuados a dicho servidor.

Servidores de servicios:

- Registrar el inicio de sesión exitoso y fallido a los Servidores de Servicios, el cual debe mostrar la fecha y hora, e historial de inicios de sesiones efectuados a dicho servidor.

9. ALTERNATIVAS

Como se indicó en la justificación, surge la necesidad de contratar software los Servidores de archivos, Servidores de Servicios y Directorio Activo; toda vez que se requiere mantener controlado todas las iteraciones que se realizan con la información (crear, modificar y eliminar archivos y carpetas) de las unidades compartidas con los usuarios, así como monitorear las autenticaciones a los servidores.

En ese sentido, para atender la necesidad se realizará el análisis comparativo de los siguientes productos:

- Quest ChangeAuditor
- ADAudit Plus

10. ANÁLISIS COMPARATIVO TÉCNICO

Para realizar el análisis comparativo de las alternativas, se han definido métricas que fueron seleccionadas en base al análisis de los requerimientos y a la información técnicas de los productos señalados en el numeral 9. ALTERNATIVAS.

La puntuación para la calificación será según los siguientes criterios:

10.1. Propósito de la evaluación

Determinar los atributos o características mínimas para el software y con dicha definición, contar con productos competitivos.

10.2. Tipo de producto

Software.

10.3. Modelo de Calidad

Se aplica el modelo establecido en la Guía Técnica sobre Evaluación de Software para la Administración Pública (R.M. N° 139-2004-PCM).

10.4. Selección de métricas

La selección de métricas se obtuvo a partir de los atributos especificados en el Modelo de Calidad.

10.5. Niveles/Escalas para las métricas

NIVEL	VALOR
Mínimo/No cumple	0
Cumple	1
Excede	2

Puntaje mínimo de aprobación: 80%

10.6. Criterios de valoración

Los atributos internos, atributos externos y la calidad en uso están detalladas en el punto de comparación de criterios de calidad.

10.7. Toma de medidas

Para la medición, las métricas seleccionadas se aplican al producto de software. Los resultados son valores expresados en las escalas de las métricas ya definidos.

10.8. Comparación de criterios de calidad

REQUERIMIENTOS	ADAudit Plus	Quest ChangeAuditor
ESPECIFICACIONES GENERALES		
Auditar y alertar sobre cambios en los servicios a monitorizar como son de alta criticidad: Servidor de archivos y Servidor Controlador de Dominio (Directorio Activo).	2	2
Generar reportes e historial para evaluar sobre consultas por parte de los usuarios de sus archivos, o accesos a la red.	2	2
Ejecución de reportes personalizados y ordenados por las distintas características.	2	2
Detectar rápida y fácilmente riesgos de seguridad o problemas de productividad como resultado del seguimiento y auditoría de los servicios de red (ficheros y directorio activo).	2	2
Generar alertas en tiempo real.	2	2
Centralizar la administración de los servicios a auditar y alertar en una única consola, basada en cliente-servidor o interfaz web.	2	2
Generar reportes, incluyendo una colección completa de informes de cumplimiento (compliance), así como la capacidad de crear rápidamente reportes personalizados.	2	2
Los reportes auditados deben ser exportados a los siguientes formatos: CSV, PDF y Excel.	2	2
Programar la entrega de reportes	2	2
Administración centralizada y con definición para tipos de usuario.	2	2
DIRECTORIO ACTIVO		
Rastrear la actividad de los usuarios y administradores con información detallada que incluya el quién, que, cuándo, dónde y la estación de trabajo de los eventos registrados.	2	2
Los eventos registrados deben contener los valores originales (antes del cambio) y los valores actuales (después del cambio).	2	2
Enviar inmediatamente una alerta cuando ítems críticos son cambiados o cuando cambios en políticas vitales ocurren. Debe tener la capacidad de modificar la criticidad de un ítem.	2	2

Permitir habilitar o deshabilitar eventos generados, en caso de que se requiera excluir cuentas seguras o de alto tráfico de ser auditadas.	2	2
Registro y seguimiento de los eventos sobre grupos incluidos dentro de otro grupo (grupos anidados).	2	2
El generador de reportes debe contar con un tablero de alertas (Dash board) que brinde un resumen general de la actividad.	2	2
Registro y seguimiento de cambios en los principales componentes del directorio activo, tales como schema, sitios, nombres de dominio, e inclusive servicio DNS.	2	2
Registrar el inicio de sesión exitoso y fallido al servidor del directorio activo, el cual debe mostrar la fecha y hora, e historial de inicios de sesiones efectuados a dicho servidor.	2	2
Control de acceso de usuario a través de permisos granulares basados en roles	2	2
SERVIDORES DE ARCHIVO DE WINDOWS		
Registro y seguimiento de cambio en el servidor de archivos, así como los ficheros cambiados por los usuarios, eliminados o bloqueados	2	2
Rastrear la actividad de los usuarios y administradores con información detallada que incluya el quién, que, cuándo, dónde y la estación de trabajo de los eventos registrados.	2	2
Los eventos registrados deben contener los valores originales (antes del cambio) y los valores actuales (después del cambio).	2	2
Registrar el inicio de sesión exitoso y fallido a los servidores de archivos, el cual debe mostrar la fecha y hora, e historial de inicios de sesiones efectuados a dicho servidor.	2	2
Control de acceso de usuario a través de permisos granulares basados en roles	2	2
SERVIDORES DE SERVICIOS DE WINDOWS		
Registrar el inicio de sesión exitoso y fallido a los Servidores de Servicios, el cual debe mostrar la fecha y hora, e historial de inicios de sesiones efectuados a dicho servidor.	2	2
Control de acceso de usuario a través de permisos granulares basados en roles.	2	2
Porcentaje de cumplimiento	100 %	100 %
Total, Puntuación	52	52

En esta evaluación se verifica que dos alternativas **ADAudit Plus** y **Quest ChangeAuditor** cumplen con todos los requisitos técnicos mínimos, por lo que se demuestra pluralidad de marcas y postores.

11. ANÁLISIS COMPARATIVO DE COSTO BENEFICIO

Software	Modalidad	Cantidad Activos	Precio
Quest ChangeAuditor <ul style="list-style-type: none"> • Change Auditor for Logon Activity Per Enabled User ACCT • ChangeAuditor for AD Per Enabled User ACCT • ChangeAuditor for Windows File Servers Per Enabled User ACCT 	Adquisición	82	S/. 367,931,08 Nota: El monto se toma de la cotización referencial del contratista Praxa consultores (Anexo A)
ADAudit Plus	Suscripción por 12 meses	82	S/. 45,992.58 Nota: El monto se toma de la cotización referencial del contratista Xentic (Anexo B)
ADAudit Plus	Suscripción por 12 meses	82	S/. 30,950.00 Nota: El monto se toma de la cotización referencial del contratista Dimcontech (Anexo C)

Beneficio:

La contratación de unos de los softwares mencionados permitirá tener un mejor control sobre las políticas aplicadas a los servidores (Directorio activo, Servidores de Archivos y Servidores de Servicios). Además, permitirá llevar un registro detallado de los cambios realizados en estos y la notificación de cambios serán en tiempo real. Asimismo, permitirá identificar de manera rápida los cambios anómalos que se estén registrando en los servidores de archivos y/o directorio activo y poder mitigarlos rápidamente.

Se podrá monitorear a los administradores de TI la veces que han iniciado sesión exitoso y fallido en los Servidores del Directorio Activo, Servidores de Archivos y Servidores de Servicios.

Finalmente se precisa que, la solución ADAudit Plus y Quest ChangeAuditor cumplen con todos los requerimientos técnicos mínimos requerido por el Indecopi por lo que se demuestra pluralidad de marcas y postores.

12. EVALUACIÓN DE RIESGOS

Con el uso del software de registro y seguimiento de eventos se garantizará una adecuada tarea de auditoria de las actividades de los usuarios respecto de las modificaciones, creaciones o eliminación de archivos y directorios del sistema de archivos compartidos, así como las actividades realizadas por los administradores de TI dentro del Directorio Activo, Servidores de Archivos y Servidores de Servicios.

De no contar con un software que realice las tareas antes mencionadas conlleva a que el usuario y/o administrador de TI pueda borrar, modificar o crear directorios o archivos sin tener identificado, quien, cuando y desde que estación se realizó dicho evento, del mismo modo no se puede conocer las modificaciones realizadas sobre el Directorio Activo.

13. CONCLUSIONES

Con la contratación Software de Registro y seguimiento de eventos, se garantiza el control y registro de actividades de los usuarios y administradores de TI respecto de los archivos y directorios y del directorio activo, e ingreso a cada servidor de tal manera que se tenga el registro de fechas, usuarios y estaciones de trabajo de donde se realizan las modificaciones.

Por las razones antes expuestas, se recomienda la contratación del Software para el registro y seguimiento de eventos el directorio activo, servidores de archivos y servidores de servicios del Indecopi.

14. FIRMAS

ELABORADO POR:	REVISADO POR:	REVISADO POR:	APROBADO POR:
Freling Ramirez Bautista Profesional en Ingeniería de Sistemas.	Enith Matías Herrera Ejecutivo 1 de Producción y Servicios de TI	Hernan Urrutia Lerma Ejecutivo 2 de Producción y Servicios de TI	Jorge Guzman Salguero Gerente de Tecnologías de la Información
FIRMA:	FIRMA:	FIRMA:	FIRMA:

ANEXO A

16 de noviembre de 2018
LICENCIAS QUEST
Proforma N° INDECOPI24
Señores: INDECOPI
Atención: Freling Ramírez Bautista
 Profesional en Ingeniería de Sistemas
 Gerencia de Tecnologías de la Información
framirez@indecopi.gob.pe
 Tel.: (51-1) 2247800 anexo 1938
 Presente.-


1. Licencias

ÍTEM	Descripción	Cant.	Precio Unit. S/	Precio Total S/
1	Intrust Enterprise Edition Per Enabled User ACCT	1,900	87.35	165,965.00
2	Change Auditor for Logon Activity Per Enabled User ACCT	1,900	52.41	99,579.00
3	Change Auditor for AD Per Enabled User ACCT	1,900	53.43	101,517.00
4	Change Auditor for Windows File Servers Per Enabled User ACCT	1,900	52.90	100,510.00
5	Password Manager Per Managed Person	1,900	31.62	60,078.00
Sub - Total S/.				527,649.00
IGV S/.				94,976.82
Total S/.				622,625.82

2.- Implementación de ChangeAuditor/InTrust

ÍTEM	Descripción	Precio Total S/
2.1	<ul style="list-style-type: none"> ✓ Instalación y configuración del ChangeAuditor para Directorio Activo, File Servers y Logon Activity ✓ Instalación y configuración del Quest InTrust ✓ Instalación de consolas administrativas en estaciones de trabajo (max 5 equipos) ✓ Instalación de consolas web de administración de ChangeAuditor e InTrust ✓ Despliegue de agentes en servidores a auditar ✓ Habilitación de Alertas y Notificaciones (Max 10) ✓ Elaboración de reportes personalizados (Max 5) ✓ Ejecución de pruebas de funcionamiento, reportes y últimos ajustes ✓ Charla técnica de ChangeAuditor e InTrust (6 horas) ✓ Elaboración de documento de Diseño e Implementación de las soluciones 	10,200.00
Sub - Total S/.		10,200.00
IGV S/.		1,836.00
Total S/.		12,036.00

ANEXO B

 <i>Your Partner Technology</i>	Correo: ventas@xentic.com.pe Web: Teléfono: 713 1800-652 4960					
Presupuesto N° CM-COT-90800854 Fecha: 09/08/2019						
Datos del Cliente: RUC: 2013384053 Cliente: Indecopi Dirección: CAL.DE LA PROSA NRO. 104 LIMA - LIMA - SAN BORJA Teléfono: 224-7800 anexo 1425	Atención: Freling Ramírez Bautista Cargo: Profesional en Ingeniería de Sistemas E-mail: framirez@indecopi.gob.pe					
Atendiendo su amable solicitud, estamos enviándole la cotización de los productos requeridos, para nosotros es un placer poner nuestra compañía a su servicio.						
Nº de Parte	Detalles de Producto	Familia	Marca	Cant.	Valor Venta	Total
MAuditD-Subs	ManageEngine ADAudit Plus Professional Edition - Subscription Model - Subscription fee for 2 Domain Controllers. 1 Yrs	Software	ManageEngine	1	S/. 3,713.28	S/. 3,713.28
MAuditF-Subs	ManageEngine ADAudit Plus Professional Edition - Subscription Model - Annual subscription fee for 80 File Servers. 1 Yrs	Software	ManageEngine	1	S/. 24,241.48	S/. 24,241.48
WG-XEN	Servicio de Implementación + Servicio de Soporte por 365 días	Servicio	XENTIC	1	S/. 11,022.00	S/. 11,022.00
					Subtotal:	S/. 38,976.76
					IGV (18%):	S/. 7,015.82
					Inversión Total:	S/. 45,992.58

ANEXO C

COTIZACION 2019.08.19 (Versión 1.0)

ITEM	DESCRIPCION	CANTIDAD	PRECIO UNITARIO SOLES	PRECIO TOTAL SOLES
1	ManageEngine ADAudit Plus Professional Edition- Subscription Model Annual subscription fee for 2 Domain Controllers Annual subscription fee for 8 File Servers Annual subscription fee for 82 Member Servers Servicios de Implementación y Puesta en marcha.	1	30,950.00	30,950.00
			30,950.00	30,950.00