

ICFES

ANEXO TECNICO DLP

Mayo de 2012

| | | |
|---|------------------------|----------------|
|  | ANEXO TECNICO DLP 2012 | Código: |
| | | Versión: 3.0 |
| | | Página 2 de 11 |

Contenido

| | |
|--|----|
| 1. ANTECEDENTES..... | 3 |
| 2. NECESIDAD | 3 |
| 3. SERVICIOS Y PRODUCTOS A CONTRATAR | 4 |
| 3.1. ALCANCE..... | 4 |
| 3.2. RED ICFES..... | 4 |
| 3.3. HARDWARE Y SOFTWARE..... | 4 |
| 3.4. EQUIPO DE TRABAJO | 5 |
| 4. CARACTERISTICAS DE LOS SERVICIOS Y PRODUCTOS A CONTRATAR..... | 6 |
| 4.1. ADMINISTRACIÓN..... | 6 |
| 4.2. PUNTOS TERMINALES..... | 6 |
| 4.3. ENCRIPCIÓN | 7 |
| 4.4. RED | 8 |
| 4.5. DESCUBRIMIENTO Y PROTECCIÓN | 8 |
| 4.6. CORREO ELECTRONICO | 8 |
| 4.7. CONSULTORIA Y DOCUMENTACIÓN | 9 |
| 4.8. CAPACITACION Y SOCIALIZACION | 9 |
| 4.9. AFINAMIENTO..... | 10 |
| 4.10. SOPORTE Y MANTENIMIENTO CON FABRICANTE..... | 10 |
| 4.11. SOPORTE CON EL PROVEEDOR..... | 10 |
| 5. GESTION DE PROYECTOS | 11 |

| | | |
|---|-------------------------------|----------------|
|  | ANEXO TECNICO DLP 2012 | Código: |
| | | Versión: 3.0 |
| | | Página 3 de 11 |

1. ANTECEDENTES

El ICFES - Instituto Colombiano para la Evaluación de la Educación, como entidad especializada en ofrecer servicios de evaluación de la educación en todos los niveles, realiza las diferentes pruebas de estado para cumplir esta misión.

La relevancia de estas pruebas es ampliamente conocida, por mencionar algunos ejemplos, la prueba SABER 11 es requisito para el grado de los bachilleres, además de ser de suma importancia para el ingreso a la universidad y evaluar a las diferentes instituciones con todas sus implicaciones, entre otros. La prueba SABER PRO (antes ECAES) es también muy importante para el grado de todos los profesionales.

El ICFES se encarga de diseñar, construir y aplicar cada una de estas pruebas. Las preguntas que componen estos exámenes son el insumo principal para la construcción de las diferentes pruebas y las diferentes versiones de cada prueba.

Existe el riesgo de fraude y filtración de información clasificada (preguntas y respuestas) sobre las pruebas. En el año 2011 en particular, se evidencio filtración de preguntas de los exámenes, con las gravísimas consecuencias que ello implica.

2. NECESIDAD

Dada la gran importancia de las pruebas y todos los intereses asociados a ellas, el ICFES necesita garantizar la confidencialidad y seguridad de toda la información relacionada con ellas. Es por esta razón, que se requiere contratar los servicios de definición, implementación, licenciamiento e infraestructura de una solución de Prevención de fuga de información DLP (Data Loss Prevention) y de encriptación, para la información sensible de todas las pruebas.

| | | |
|---|------------------------|----------------|
|  | ANEXO TECNICO DLP 2012 | Código: |
| | | Versión: 3.0 |
| | | Página 4 de 11 |

3. SERVICIOS Y PRODUCTOS A CONTRATAR

El ICFES requiere contratar los servicios de consultoría, licenciamiento de software, infraestructura de hardware, instalación y puesta en funcionamiento de una solución para la Prevención de fuga de información (DLP) y encriptación, para la fase 1.

3.1. ALCANCE

La solución DLP que se requiere, consta de los siguientes componentes:

- Administración
- Puntos terminales
- Encriptación
- Red
- Descubrimiento y protección
- Correo electrónico
- Consultoría y documentación
- Capacitación y socialización
- Afinamiento
- Soporte con el fabricante
- Soporte con el proveedor

3.2. RED ICFES

La solución DLP debe ser puesta en producción en la red del ICFES, según las especificaciones descritas en el ANEXO 2 - Información DLP¹, el cual contiene un mapa de red detallado e información relevante de segmentos y velocidades, proxy, antivirus y correo corporativo.

El contratista debe asumir toda la infraestructura de hardware (incluyendo los elementos de red) y software de la solución a instalar en los distintos datacenters del ICFES, para garantizar el buen funcionamiento de la solución protegiendo toda la red.

3.3. HARDWARE Y SOFTWARE

- Describir detalladamente las funcionalidades de cada uno de los componentes ofrecidos.

¹ Anexo confidencial que no se publica, solamente se envía a las empresas participantes del proceso.

- Si la solución requiere servidores para instalar el software ofertado, se debe incluir el valor de ese hardware en la oferta económica. Por favor describir las características de este hardware.
- Si la solución requiere appliances, se debe incluir el valor de ese hardware en la oferta económica. Por favor describir las características de este hardware.
- El proveedor debe incluir y ofertar los elementos de red que se requieran para monitorear cada uno de los componentes de la solución, que se instalen en los distintos datacenters del ICFES (Calle 17 y Externo). Por favor describir las características de este hardware.

3.4. EQUIPO DE TRABAJO

Es de aclarar que en la oferta económica deben estar incluidos todos los costos correspondientes a los recursos humanos que hacen parte del equipo de trabajo para el proyecto.

El equipo de trabajo mínimo requerido consta de un gerente de proyectos, un líder técnico, y un ingeniero implementador, tal y como esta descrito en los términos de referencia. Además, el equipo puede incluir la participación de otros ingenieros o consultores (funcionales, encriptación, instructores, etc.), según se requiera para ejecutar el alcance del contrato. Puede incluir otro personal de apoyo según considere.

La dedicación para el equipo de trabajo es la siguiente:

| | |
|--------------------------------|---|
| Gerente de Proyecto | Tener un porcentaje de dedicación mensual de por los menos 20%. |
| Líder Técnico | Tener un porcentaje de dedicación mensual de por los menos 30% en las fases de diseño y de implementación de la solución. |
| Ingeniero Implementador | Tener un porcentaje de dedicación mensual de por los menos 50% en las fases de implementación, pruebas y afinamiento inicial de la solución |

| | | |
|---|-------------------------------|----------------|
|  | ANEXO TECNICO DLP 2012 | Código: |
| | | Versión: 3.0 |
| | | Página 6 de 11 |

4. CARACTERISTICAS DE LOS SERVICIOS Y PRODUCTOS A CONTRATAR

La solución de Prevención de fuga de información (DLP) ofertada, debe contar con las siguientes características:

4.1. ADMINISTRACIÓN

La solución debe tener una plataforma web de administración y monitoreo centralizado de las herramientas que conforman la solución.

- La solución ofertada debe permitir la definición, consulta, modificación y monitoreo de políticas asociadas a los componentes de Data Loss Prevention y Cifrado.
- La solución ofertada debe permitir un esquema de administración de autenticación y autorización que maneje al menos: usuarios, roles y permisos por rol.
- La solución ofertada debe permitir el monitoreo de políticas por usuario, área y roles asociados a los componentes de Data Loss Prevention y Cifrado.
- La solución ofertada debe permitir enviar notificaciones de violaciones a las políticas.
- La solución debe tener integración nativa en todos los módulos de Data Loss Prevention y encriptación.
- La solución debe poder generar reportes mensuales de todos los incidentes y eventos, categorizándolos por diferentes criterios.
- La solución ofertada debe permitir la correlación de eventos, el monitoreo y consulta de los eventos correlacionados.

4.2. PUNTOS TERMINALES

El ICFES desea proteger la información en CUARENTA (40) puntos terminales distribuidos de la siguiente manera:

- DIEZ Y SIETE (17) computadores y UN (1) servidor que se encuentran en la Subred 1 Calle 17.
- DIEZ Y SIETE (17) equipos de funcionarios y UN (1) servidor que se encuentran en la Red Principal Calle 17.
- Adicionalmente, el ICFES entrega información confidencial a dos proveedores y esta información reside en CUATRO (4) computadores, 2 por cada proveedor. Esta

| | | |
|---|-------------------------------|----------------|
|  | ANEXO TECNICO DLP 2012 | Código: |
| | | Versión: 3.0 |
| | | Página 7 de 11 |

información debe ser protegida y existirá comunicación vía VPN entre estos PC's y la Red Principal ICFES Calle 17 o el Datacenter externo.

La Prevención de fuga de información en puntos terminales debe tener las siguientes restricciones:

- No se debe permitir impresión ni capturas de pantalla.
- Debe restringir todos los periféricos de cada punto terminal (unidades de CD/DVD/BluRay, USBs, Firewire, tarjetas de memoria, etc).
- Si el mouse del punto terminal es USB, debe estar restringido para que solo se pueda usar ese dispositivo en particular, y no se pueda conectar ningún otro elemento en ese puerto.

4.3. ENCRIPCIÓN

El ICFES desea realizar la encriptación de disco de DIEZ (10) portátiles, adicionalmente el ICFES requiere la encriptación de archivos y carpetas para que sean accedidos desde TREINTA (30) estaciones de trabajo.

Algunos de los archivos que se encriptarán, pueden ser accedidos por los CUATRO (4) equipos de los proveedores que se conectan vía VPN y de los que se habla en el componente Protección de puntos terminales.

- La solución ofertada debe permitir el cifrado de contenidos sensibles ó el cifrado completo de disco duro de los equipos (desktops y laptops), y la apertura de los datos cifrados solamente por las personas que el ICFES designe.
- La solución ofertada debe permitir la encriptación de carpetas y archivos sensibles. Estos carpetas/subcarpetas/archivos se deben poder crear/consultar/modificar/eliminar solamente por los usuarios que se configuren en la herramienta.
- El proponente debe describir en su propuesta los protocolos, mecanismos o algoritmos de encriptación que ofrece como parte de la solución.
- El proponente debe describir en su propuesta si las técnicas de cifrado son simétricas o asimétricas, y si usan certificados digitales (en especial para la información compartida con los proveedores).
- La solución ofertada debe permitir que las claves de autenticación se pueden asignar por cada usuario, por rol y/o por grupos de usuarios.

| | | |
|---|-------------------------------|----------------|
|  | ANEXO TECNICO DLP 2012 | Código: |
| | | Versión: 3.0 |
| | | Página 8 de 11 |

- La solución ofertada debe tener un componente de encriptación que permita la creación/consulta/edición/eliminación de la información cifrada solamente a usuarios que tengan una llave o clave autorizada en el sistema.
- La solución ofertada debe poder manejar llaves de hardware o de software. Las llaves para creación/consulta/edición/eliminación de información cifrada deben permitir la integración con dispositivos físicos.
- La solución de cifrado ofertada debe ser integrable con dispositivos físicos de autenticación como tokens y tarjetas inteligentes. El proponente debe describir el listado genérico de dispositivos físicos integrables, tales como dispositivos biométricos como lectores de huella, etc.

4.4. RED

El ICFES desea evitar la fuga de información de la información que viaja vía http, https, ftp, mail de internet (gmail, hotmail, yahoo, etc), mensajería instantánea y redes sociales.

Esto aplica a máximo CUATRO CIENTOS (400) usuarios en la Red Principal Calle 17, la Subred 1 Calle 17 y usuarios remotos que acceden a los servicios vía VPN.

4.5. DESCUBRIMIENTO Y PROTECCION

El ICFES desea que la solución incluya un componente de descubrimiento y protección de información sensible en servidores (windows y unix) y estaciones de trabajo ubicados en la Red Principal Calle 17 y la Subred 1 Calle 17.

La cantidad de servidores y estaciones de trabajo es aproximadamente TRES CIENTOS (300).

- La solución ofertada debe permitir la detección de información sensible y el monitoreo de la información en dispositivos de almacenamiento, unidades de red, servidores, desktops, portátiles.
- La solución ofertada debe poder realizar descubrimiento y protección de información sensible en bases de datos.

4.6. CORREO ELECTRONICO

El ICFES desea proteger la información de su sistema de correo electrónico, el cual tiene capacidad hasta CUATRO CIENTOS (400) usuarios.

| | | |
|---|-------------------------------|----------------|
|  | ANEXO TECNICO DLP 2012 | Código: |
| | | Versión: 3.0 |
| | | Página 9 de 11 |

El servidor de correo electrónico se encuentra en un Datacenter Externo, y los clientes de correo acceden a este a través de webmail desde la sede del ICFES o desde Internet, y del cliente de outlook desde la sede del ICFES.

4.7. CONSULTORIA Y DOCUMENTACIÓN

El ICFES requiere que se incluya en la propuesta los servicios de consultoría necesarios para la configuración de la solución, definición de políticas para configuración, definición reglas de los componentes, criterios de establecimiento de los roles y permisos de los usuarios y su acceso a la información, estrategias de prevención, categorización de los eventos de violaciones a las políticas de seguridad, definición de protocolos de respuesta a los eventos de violaciones en las políticas de seguridad, y en general todo lo necesario para el diseño, instalación, configuración y puesta en producción de la solución.

La consultoría será aceptada con base en los siguientes criterios de aceptación:

- Finalización etapa de análisis y diseño de la solución: Arquitectura, análisis de información y diseño de políticas, reglas, permisos, estrategias, categorización eventos, protocolos de respuesta.
- Configuración exitosa en la herramienta de las políticas de seguridad, reglas, roles, permisos, eventos, y en general todo lo necesario para el correcto funcionamiento de la solución.
- Finalización etapa de pruebas, monitoreo y afinación iniciales de la solución.
- Generación exitosa de reportes desde la herramienta.
- La puesta en producción oficial de la solución.
- Entrega de la documentación completa del proyecto.
- Entrega de un documento resumen que contenga las políticas de seguridad definidas, estrategias de prevención, categorización de eventos y protocolos de respuesta. Además, debe contener las conclusiones y recomendaciones de la consultoría.

4.8. CAPACITACION Y SOCIALIZACION

El ICFES requiere que se incluya en la propuesta de la solución, la capacitación ofrecida a las personas designadas para la administración y soporte de la solución. El contratista debe especificar las características y temas a manejar en dicha capacitación, esta no debe ser en ningún caso inferior a 24 horas, debe ser impartida en bloques de máximo 4 horas diarias.

| | | |
|---|-------------------------------|-----------------|
|  | ANEXO TECNICO DLP 2012 | Código: |
| | | Versión: 3.0 |
| | | Página 10 de 11 |

Adicionalmente, el contratista debe brindar al menos 24 horas de capacitaciones a los usuarios, para el correcto uso de la solución. El plan de capacitación estará sujeto a aprobación por parte del ICFES.

Por otra parte, el contratista debe diseñar y ejecutar un plan y una estrategia de comunicaciones para la prevención de fuga de información en el ICFES. Habrá un plan general para los usuarios normales, y un plan dirigido especialmente a aquellos usuarios que manejen directamente la información sensible. Estos planes estarán sujetos a aprobación por parte del ICFES.

4.9. AFINAMIENTO

El ICFES requiere que se incluya en la propuesta de la solución, el servicio de acompañamiento para el afinamiento de la herramienta, el contratista deberá realizar mínimo dos vistas al mes de 4 horas cada una, por un período de dos meses contados a partir de la fecha de puesta en producción oficial de la solución, para el acompañamiento y afinamiento de la misma. Este acompañamiento busca que el ICFES logre obtener un mayor valor de la solución adquirida, por medio del afinamiento de la solución, generación de nuevos reportes, etc.

4.10. SOPORTE Y MANTENIMIENTO CON FABRICANTE

El ICFES requiere que se incluya en la oferta el soporte y mantenimiento con el fabricante, por 1 año contado a partir de la fecha de puesta en producción oficial de la solución. La propuesta debe incluir las características de este servicio.

4.11. SOPORTE CON EL PROVEEDOR

El ICFES requiere que se incluya en la oferta el soporte directo con el proveedor. Este debe ofrecer canales telefónicos, correo y/o web, y presencial (cuando el incidente así lo requiera).

El tiempo de atención debe ser de máximo 4 horas, y el tiempo de solución se asignará de acuerdo a la complejidad del incidente.

Este soporte debe ser por 1 año contado a partir de la fecha de puesta en producción oficial de la solución.

La propuesta debe incluir las características de este servicio.

| | | |
|---|-------------------------------|-----------------|
|  | ANEXO TECNICO DLP 2012 | Código: |
| | | Versión: 3.0 |
| | | Página 11 de 11 |

5. GESTION DE PROYECTOS

La ejecución del servicio objeto del presente términos de condiciones se realizará como un proyecto, de forma que se pueda tener una gestión y control adecuado sobre el avance y el logro de los objetivos y alcance propuesto. Se requiere que la metodología a utilizar por el oferente esté alineada con el Project Management Body of Knowledge (PMBOOK®) del Project Management Institute (PMI). También, se deben cumplir los lineamientos que el ICFES indique al contratista con respecto a la gestión, reporte y control del proyecto.

El contratista deberá presentar informes semanales del rendimiento del proyecto, en las reuniones de seguimiento durante toda la ejecución del proyecto.

El contratista debe contar con el licenciamiento de las herramientas de software necesarias para la realización de todos los procesos de la gerencia de proyectos, descritos en este anexo. Se requiere que el oferente use el software de gestión de proyectos MS Project Management versión 2007, o la versión que tenga el ICFES en su momento para poder revisar el cronograma, con sus propias licencias.