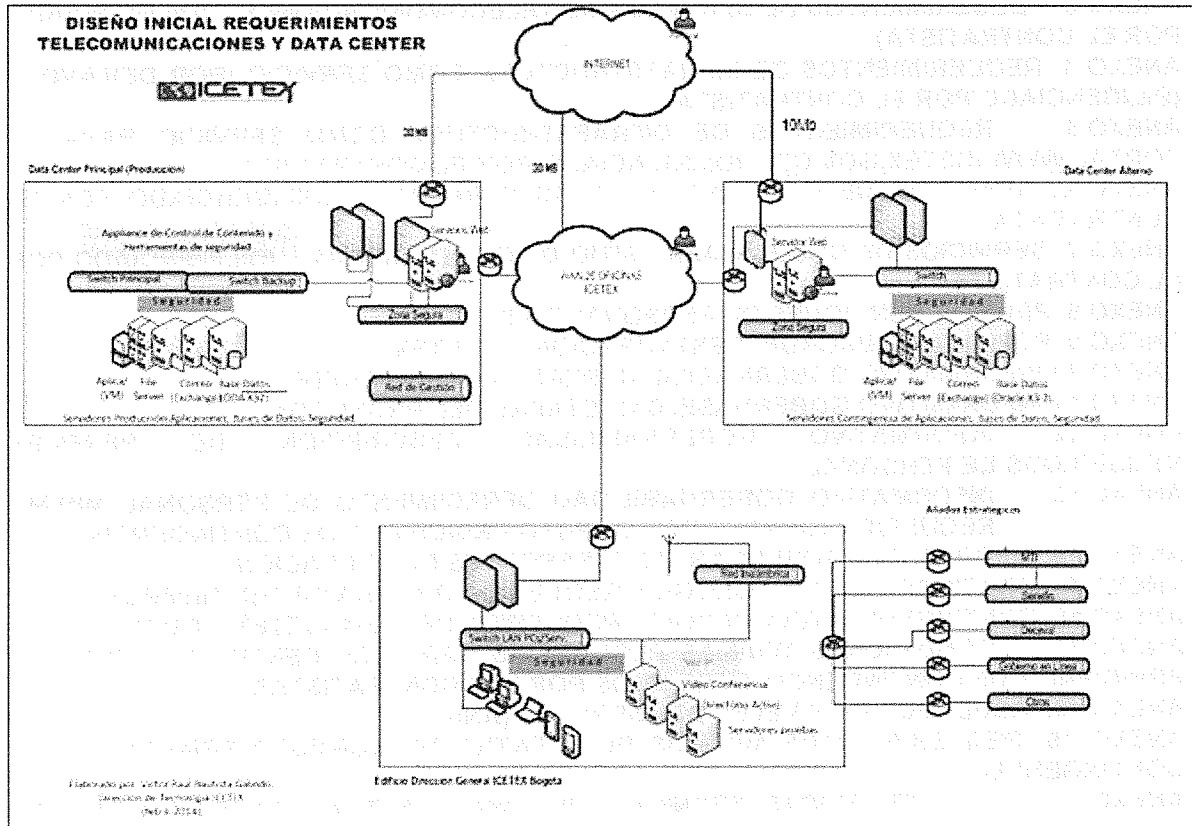


## **ANEXOS TECNICOS DEL APENDICE “ESPECIFICACIONES TÉCNICAS MÍNIMAS DEL SERVICIO”**

- ANEXO 1 TOPOLOGIA DE LA RED ADQUIRIDA
- ANEXO 2. RESUMEN ESPECIFICACIONES SERVICIOS REQUERIDOS. (DILIGENCIADO POR EL CONTRATISTA)
- ANEXO 3. REQUERIMIENTOS DE SERVICIOS DE TELECOMUNICACIONES. . (DILIGENCIADO POR EL CONTRATISTA)
- ANEXO 4. REQUERIMIENTOS DE INFRAESTRUCTURA COMO SERVICIO (POR DEMANDA). (DILIGENCIADO POR EL CONTRATISTA)
- ANEXO 5 REQUERIMIENTOS DE INFRAESTRUCTURA COMO SERVICIO PARA EL PORTAL [WWW.ICETEX.GOV.CO](http://WWW.ICETEX.GOV.CO). . (DILIGENCIADO POR EL CONTRATISTA)
- ANEXO 6. SERVICIOS DE COLOCACION - SITIO PRINCIPAL. . (DILIGENCIADO POR EL CONTRATISTA)
- ANEXO 7. SERVICIOS DE COLOCACION - SITIO DE CONTINGENCIA. . (DILIGENCIADO POR EL CONTRATISTA)
- ANEXO 8. PERFIL Y FUNCIONES DE PERSONAL EN SITIO
- ANEXO 9. POLITICA DE BACKUP- RESTAURACIONES ICETEX.
- ANEXO 10. INFORMATIVO GOBERNABILIDAD PERSONAL REQUERIDO.
- ANEXO 11. INFORMATIVO GOBERNABILIDAD ETAPAS DEL PROYECTO.
- ANEXO 12. INFORMATIVO GOBERNABILIDAD DESCRIPCIÓN DE PERFILES REQUERIDOS DE PERSONAL.
- ANEXO 13. INFORMATIVO GOBERNABILIDAD OFRECIMIENTO DE PERSONAL MINIMO REQUERIDO (CENTRO DE COMPUTO PRINCIPAL Y DE CONTINGENCIA).
- ANEXO 14. INFORMATIVO GOBERNABILIDAD REPORTES DE OPERACIÓN.
- ANEXO 15. CONTINGENCIA TECNOLÓGICA REQUERIDA DRP (BIA ICETEX TIEMPOS RPO).
- ANEXO 16. CONTINGENCIA TECNOLÓGICA REQUERIDA DRP (BIA ICETEX TIEMPOS RTO).
- ANEXO 17. CONDICIONES MINIMAS REQUERIDAS PARA LOS CENTRO DE CÓMPUTO PRINCIPAL Y DE CONTINGENCIA OFRECIDOS POR LOS CONTRATISTAS.
- ANEXO 18. ACUERDOS DE NIVELES DEL SERVICIO (ANS)
- ANEXO 19. REQUERIMIENTOS MINIMOS DEL CENTRO DE CÓMPUTO PRINCIPAL Y DE CONTINGENCIA
- ANEXO 20. CARACTERÍSTICAS TÉCNICAS FIRE WALL ACTUAL ICETEX CENTRO DE CÓMPUTO .
- ANEXO 21. CARACTERÍSTICAS TÉCNICAS MÍNIMAS REQUERIDAS DEL SERVICIO WEB APLICATION FIREWALL - WAF
- ANEXO 22. REQUERIMIENTOS TÉCNICOS MÍNIMOS SISTEMA DE VIDEO CONFERENCIA

**SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015**

**ANEXO 1. TOPOLOGIA DE RED REQUERIDA**





## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

---

### ANEXO 2.

#### RESUMEN ESPECIFICACIONES SERVICIOS REQUERIDOS DE CARÁCTER OBLIGATORIO

Anexo diligenciado por el contratista. Se encuentra en el archivo adjunto "Anexos\_Diligenciados\_Contratista\_2"

### ANEXO 3.

#### REQUERIMIENTOS DE SERVICIOS DE TELECOMUNICACIONES

Anexo diligenciado por el contratista. Se encuentra en el archivo adjunto "Anexos\_Diligenciados\_Contratista\_3\_4\_5\_6\_7"

### ANEXO 4.

#### REQUERIMIENTOS DE INFRAESTRUCTURA COMO SERVICIO (POR DEMANDA)

Anexo diligenciado por el contratista. Se encuentra en el archivo adjunto "Anexos\_Diligenciados\_Contratista\_3\_4\_5\_6\_7"

### ANEXO 5.

#### REQUERIMIENTOS DE INFRAESTRUCTURA COMO SERVICIO PARA EL PORTAL WWW.ICETEX.GOV.CO

Anexo diligenciado por el contratista. Se encuentra en el archivo adjunto "Anexos\_Diligenciados\_Contratista\_3\_4\_5\_6\_7"

### ANEXO 6.

#### REQUERIMIENTOS DE SERVICIOS DE COLOCACION CENTRO DE CÓMPUTO PRINCIPAL (ANS 99,8%)

Anexo diligenciado por el contratista. Se encuentra en el archivo adjunto



## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

### "Anexos\_Diligenciados\_Contratista\_3\_4\_5\_6\_7"

**NOTAS:** El contratista debe aprovisionar, gestionar, monitorear, soportar y aplicar garantías para todos los equipos de telecomunicaciones y red local.

El contratista debe aprovisionar, gestionar, monitorear, soportar y aplicar garantías para todos los equipos puestos en la modalidad de hosting (unidades de procesamiento) en este sitio principal.

El contratista debe aprovisionar, gestionar, monitorear, soportar y aplicar garantías para todos los equipos de Salida a Internet de ICETEX a nivel nacional.

Servicios adicionales telecomunicaciones:

El contratista deberá proveer los "Racks" que sean necesarios para la puesta en producción de todos los elementos descritos en el presente anexo.

Esta línea base sufrirá modificaciones durante la vigencia del contrato, por lo cual es importante que el contratista incluya los valores en términos de unidad de rack o mínimo en  $\frac{1}{4}$  de unidad de rack con el propósito de que cuando se requiera ingresar o retirar equipos a los Centros de Computo Principal y De Contingencia la factura del mes correspondiente sufra variaciones en forma proporcional. Por procesos actuales de renovación tecnológica del Instituto, es posible que esta línea base sufra variaciones al inicio del contrato o durante la etapa de transición de la operación entre el operador actual y el ingreso del nuevo. En caso de que no se especifiquen valores en proporción de crecimiento por  $\frac{1}{4}$ ,  $\frac{1}{3}$ ,  $\frac{1}{2}$  y un full rack, los costos base de facturación será la cantidad de unidades de rack efectivamente utilizadas por ICETEX.

### ANEXO 7.

#### REQUERIMIENTOS DE SERVICIOS DE COLOCACION CENTRO DE CÓMPUTO DE CONTINGENCIA (ANS 99,7%)

Anexo diligenciado por el contratista. Se encuentra en el archivo adjunto "Anexos\_Diligenciados\_Contratista\_3\_4\_5\_6\_7"

Esta línea base sufrirá modificaciones durante la vigencia del contrato, por lo cual es importante que el contratista incluya, por lo menos los valores en términos de unidad de rack o mínimo en  $\frac{1}{4}$  de unidad de rack con el propósito de que cuando se requiera ingresar o retirar equipos a los Centros de Computo Principal y De Contingencia la factura del mes correspondiente sufra variaciones en forma proporcional. Por procesos actuales de renovación tecnológica del Instituto, es posible que esta línea base sufra variaciones al inicio del contrato o durante la etapa de transición de la operación entre el operador actual y el ingreso del nuevo.

#### NOTAS:

El contratista debe aprovisionar, gestionar, monitorear, soportar y aplicar garantías para todos los equipos de telecomunicaciones y red local.

El contratista debe aprovisionar, gestionar, monitorear, soportar y aplicar garantías para todos los equipos de hosting (unidades de procesamiento).



## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

El contratista deberá proveer los "Racks" que sean necesarios para la puesta en producción de todos los elementos descritos en el presente anexo.

### ANEXO 8.

#### FUNCIONES DE PERSONAL EN SITIO

##### ADMINISTRADOR BASES DE DATOS ORACLE

El CONTRATISTA dedicara un recurso humano en sitio de tiempo completo (horario de 8:00 am a 5:30 pm) de Lunes a Viernes o cuando sea requerido por tareas específicas o casos especiales asignados por el Contratista; Adicionalmente se debe contar con el servicio de Soporte directo para los ambientes Virtualizados, se debe realizar dentro de las tareas permanentes durante la duración del plazo del contrato, las siguientes actividades necesarias para el cumplimiento del numeral.

##### ALCANCES DE LA ADMINISTRACION DE BASES DE DATOS:

- ✓ Diagnóstico preliminar, identificando cuellos de botella, ejecutando acciones correctivas y preventivas, preparando un documento de recomendaciones al área de tecnología informática, que sirva como plan de acción para la operación diaria.
- ✓ Revisión de la instalación actual de ORACLE y SQL Server y verificación del cumplimiento de los prerequisites de instalación sobre el Sistema Operativo actual.
- ✓ Verificación o Implementación del monitoreo de todas las bases de datos.
- ✓ Verificación de la configuración de parámetros adecuados de las Bases de Datos para óptimo rendimiento de las mismas, de acuerdo con los requerimientos propios de ICETEX.
- ✓ Verificación y configuración del Uso de Memoria, CPU, IO: física, virtual a nivel de las máquinas y de las bases de datos.
- ✓ Almacenamiento: Verificación de la distribución de los datafiles, redologs, filegroups, fragmentaciones, etc.
- ✓ Verificación en General de la BD a nivel de: Transacciones, Locks, Lacks
- ✓ Instalación y configuración de soluciones de alta disponibilidad de base de datos.
- ✓ Instalación y configuración de soluciones de contingencia de base de datos.
- ✓ Generar recomendaciones que permitan optimizar el desempeño de las bases de datos y así mismo evaluar las ventajas de las actualizaciones de las versiones de los productos instalados.
- ✓ Generar los planes de avance y mejoramiento para los proyectos.
- ✓ Diseño de arquitecturas de bases de datos de acuerdo a las necesidades del ICETEX.
- ✓ Recibir incidentes, solicitudes de servicio o requerimientos de acuerdo al protocolo de

**SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015**

atención.

- ✓ Resolver y documentar los incidentes y requerimientos que están dentro de su competencia.
- ✓ Generar recomendaciones que permitan optimizar el desempeño de las bases de datos y así mismo evaluar las ventajas de las actualizaciones de las versiones de los productos instalados.
- ✓ Velar por el cumplimiento de las políticas de copias de respaldo (backup) de las bases de datos.
- ✓ Velar por la ejecución de los planes de mantenimiento preventivo.
- ✓ Ejecución de los planes de avance y mejoramiento.
- ✓ Garantizar el cumplimiento de los niveles de servicio acordados.
- ✓ Atención de requerimientos del cliente relacionados con:
  - ✓ Creación de objetos
  - ✓ Compilación de objetos
  - ✓ Modificación de objetos
  - ✓ Manejo de espacios en base de datos
- ✓ Apoyar tareas de generación de SCRIPTS que permitan realizar backups lógicos de las bases de datos.
- ✓ Revisión de logs base de datos. Plantear recomendaciones al respecto.
- ✓ Ejecución de los planes de mantenimiento preventivo.
- ✓ Ejecutar las tareas de monitoreo de las bases de datos con el fin de garantizar su disponibilidad.
- ✓ Contribuir con el cumplimiento de los niveles de servicio acordados con los clientes.

**VIRTUALIZACION:**

- ✓ Soporte especializado mediante línea directa de atención.
- ✓ Soporte especializado mediante conexión remota o intercomunicación con el Recurso en Sitio.
- ✓ El soporte debe estar enfocado al trabajo de casos específicos de las herramientas de Virtualización de Oracle (VM manager) y el ambiente de Virtualización sobre las ODA X3.2 y los SUN X3.2L

El CONTRATISTA deberá suministrar herramientas que permita monitorear y generar diagnostico en Bases de Datos:

**Oracle:**

- ✓ Mensajes de alerta de log de Oracle para corrupciones de bloques de datos, colas de recursos excedidos, errores internos y fallas de lectura/escritura de I/O
- ✓ Situaciones de error como estado SYS.DUAL

### SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

- ✓ Monitoreo de los principales procesos de Oracle: LGWR, DBWR, PMON, ARCH, SMON, TRWR, RECO, SNPX y LCKX
- ✓ Deberá monitorear variables de desempeño propias del manejador de bases de datos Oracle
- ✓ Deberá permitir el monitoreo de las principales variables de manejo de espacio de Oracle, tales como: table spaces, espacio libre y fragmentación de segmentos.
- ✓ Deberá permitir el monitoreo de variables del desempeño del manejador tales como: Sort, buffer, shared pool, dictionary cache ratio, etc.
- ✓ Deberá manejar estadísticas de los segmentos de Rollback, tales como: número de shrinks, porcentaje de esperas.
- ✓ Deberá manejar información de Archive, tal como: tiempo promedio entre escrituras de archive log y número de logs que caben en un dispositivo archive.
- ✓ La solución de administración de Oracle deberá soportar las versiones 7, 10g y superiores de Oracle.
- ✓ Validación de configuraciones de Oracle a nivel de Monitoreo.
- ✓ Participar proactivamente en el afinamiento de Bases de Datos para garantizar el adecuado rendimiento de las aplicaciones de misión crítica del Instituto.
  - Gestión de disponibilidad y rendimiento de Oracle.
  - Monitoreo del archivo Alert.log (validar y verificar errores).
  - Monitoreo de estadísticas de rendimiento, tales como actividad del usuario, el estado, espacio, rendimiento del SGA, detalles del SGA, estado del SGA, detalles de las sesiones, tablas de uso de espacio, detalles del espacio, alarmas, comportamiento de los archivos de datos, Obtención del buffer, lectura en disco, segmentos del rollback, consultas, entre otras.
  - Monitoreo de backups, (modo: archive), y/o Exports; según la metodología implementada.
  - Planes de mantenimiento y optimización.
  - Monitoreo de seguridad.
  - Monitoreo de Tablespace.
- ✓ Firmar un acuerdo de confidencialidad.

#### **Microsoft SQL Server:**

- ✓ Afinamiento de la Bases de Datos cuando sea requerido por el Instituto.
- ✓ Generación de alarmas cuando se superen los umbrales normales de operación para:
- ✓ Información de cache (cache hit percentage, cache free buffer percentage)
- ✓ Utilización de CPU por el MS SQL Server
- ✓ Deadlock rates y deadlock rates por objeto
- ✓ Requerimientos de escritura de la base de datos a sistema operativo que no han sido completados
- ✓ Espacio del log de transacciones usado por cada base de datos
- ✓ Deberá coleccionar información histórica de rendimiento para:
- ✓ Cache Hit Porcentaje

**SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015**

Disponibilidad del servidor (Medición por herramienta de Help Desk con soporte en eventos de alertamientos de indisponibilidad de servidor).

**MySQL:**

Generación de alarmas cuando se superen los umbrales normales de operación para:

- ✓ Información de cache (cache hit percentage, cache free buffer percentage)
- ✓ Utilización de CPU por MySQL
- ✓ Requerimientos de escritura de la base de datos a sistema operativo que no han sido completados
- ✓ Espacio del log de transacciones usado por cada base de datos

Deberá coleccionar información histórica de rendimiento para las siguientes métricas:

- ✓ Uso de CPU por sesión
- ✓ Buffers scanned
- ✓ Deadlocks
- ✓ Timeouts
- ✓ Enqueue Waits
- ✓ Free buffer inspected
- ✓ Free buffer requested
- ✓ Active\_sorts

**INFORMES REQUERIDOS**

Documentación técnica de:

- ✓ Diagnóstico de la situación actual, Bases de Datos y Virtualización.
- ✓ Mejoras planteadas.
- ✓ Plan de Trabajo para la ejecución de Mejoras Planteadas (Project)
- ✓ Evidencias encontradas y las recomendaciones a aplicar sobre la base de datos y los ambientes virtualizados (mejores prácticas), proponer cambios a nivel de arquitectura, detectar deficiencias o mejoramientos en las políticas que tiene ICETEX definidas a nivel de base de datos, y demás consideraciones para las bases de datos revisadas y de todos los ambientes virtualizados
- ✓ Formatos de Controles de Cambio de las tareas técnicas realizadas sobre los servidores en producción, contingencia, pruebas y ambientes virtualizados.
- ✓ Sentencias PL-SQL, Querys, Crontab, JOBS o cualquier otro que se elabore por parte del recurso técnico en sitio, como parte de los mecanismos de mejora implementados en pro del cumplimiento de los alcances del presente.
- ✓ Debe ofrecer reportes y gráficas de desempeño de las métricas coleccionadas.



## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

El administrador de bases de datos debe tener al menos la certificación de Oracle OCA y debe contar con experiencia de al menos 3 años en administración y soporte de bases de datos. Actualmente las bases de datos core del ICETEX son ORACLE y SQL SERVER (Portal)

### ADMINISTRADOR PORTAL WEB

Debe prestar sus servicios en las oficinas de ICETEX Dirección General en donde se encuentren ubicadas (hoy, Calle 3ª No-18-32) con disponibilidad las 24 horas, pero con horario básico que será acordado con la Dirección de Tecnología en el momento de la legalización del contrato y válido durante la vida de ejecución del contrato. El ICETEX tendrá la potestad de aprobar o no el recurso humano asignado, con lo cual el contratista hará entrega oportunamente durante el inicio del contrato, la(s) hoja(s) de vida del(os) aspirantes, y posteriormente en caso de cambio del profesional Web Master, se debe reportar oportunamente con por lo menos quince (15) días hábiles de anticipación y haciendo entrega simultáneamente la hoja de vida del nuevo aspirante.

Los costos asociados con los servicios se pueden retirar del cobro mensual en caso de que no se requiera el servicio por parte de ICETEX, lo cual se informará con quince días de anticipación. Igualmente, en caso de incumplimiento en los términos pactados por este servicio con el debido informe del interventor, el contratista deberá retirar los costos asociados por el incumplimiento del servicio pactado.

En general, las funciones primordiales que debe realizar el Web Master, son:

- ✓ Realizar la administración del servidor de Aplicaciones Web asociado al portal [www.icetex.gov.co](http://www.icetex.gov.co).
- ✓ Realizar la administración del servidor de Base de Datos SQL asociado al portal [www.icetex.gov.co](http://www.icetex.gov.co).
- ✓ Realizar la administración del servidor de aplicaciones Intranet para los servicios C&CTEX.
- ✓ Implementar y administrar ambientes de pruebas para las Aplicaciones Web, estos ambientes son solicitados por la Dirección de Tecnología.
- ✓ Realizar la instalación (Catalogación) y estabilización en ambientes productivos de nuevas Aplicaciones Web contratadas o desarrolladas por el Instituto.
- ✓ Asesoramiento y recomendaciones en materia de configuración de las nuevas aplicaciones Web contratadas por el ICETEX.
- ✓ Abrir casos al proveedor del servicio de Centro de Cómputo donde este alojado el portal [www.icetex.gov.co](http://www.icetex.gov.co) en presencia de eventualidades y realizar seguimiento hasta cerrar el caso.
- ✓ Administración de las herramientas de monitoreo del portal [www.icetex.gov.co](http://www.icetex.gov.co), Google Analytics (Indicadores de visita al portal).
- ✓ Revisión periódica de la consola Event Viewer de los Servidores Web solicitando o ejecutando las mejoras correspondientes en aplicaciones (*perfil técnico*).
- ✓ Administración y soporte del gestor de contenidos del Portal. Se requiere preferiblemente conocimientos y/o experiencia en el gestor de contenidos SiteFinity.
- ✓ Asesoría e implementación de nuevos servicios (Módulos DNN) del portal web desde la perspectiva del CMS SiteFinity o en su defecto, el que utilice ICETEX durante la vigencia del contrato.
- ✓ Realizar las actualizaciones de versión del CMS SiteFinity (*perfil técnico*) o en su defecto, el que utilice ICETEX durante la vigencia del contrato.
- ✓ Implementar en el portal estándares de Gobierno en Línea y W3C (*perfil técnico*).
- ✓ Renovación e instalación de los certificados Digitales SSL del Portal Web [www.icetex.gov.co](http://www.icetex.gov.co).



## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

- ✓ Realizar monitoreo y adecuaciones en el servidor de aplicaciones de producción para el control y prevención de vulnerabilidades del portal ICETEX, éstas labores se desarrollan mancomunadamente con el Asesor de Seguridad de la Dirección de Tecnología.
- ✓ Realizar optimización del Portal Web [www.icetex.gov.co](http://www.icetex.gov.co) apoyado en las estadísticas obtenidas por la herramientas de monitoreo.
- ✓ Gerencia de Proyectos Web asignados por la Dirección de Tecnología.
- ✓ Cronograma, plan de trabajo y seguimiento de los proyectos asignados por la Dirección de Tecnología.
- ✓ Firmar un acuerdo de confidencialidad.

Actualmente el ICETEX se encuentra en proyecto de renovación tecnológica de su Portal de Internet motivo por el cual el WebMaster debe entrar a administrar el nuevo portal una vez el mismo salga a producción con las nuevas especificaciones de software base y aplicativo y de hardware.

### REQUISITOS DE EXPERIENCIA DEL WEB MASTER

Ingeniero de sistemas con mínimo 3 años de experiencia en administración técnica y de contenido de portales de Internet, administración de IIS, administración y conocimiento de sistemas operativos Windows Server, bases de datos Sql Server, gestores de contenido y herramientas de Gestión y administración WEB.

### ENTREGABLES O PRODUCTOS DE LA ASESORIA EN ADMINISTRACIÓN WEB

- ✓ Informe(s) de avance mensual de los proyectos de acuerdo con el plan estratégico de Tecnología aprobado por la Dirección y de los cambios efectuados sobre la plataforma tecnológica a nivel de Servidores Web, de acuerdo con los requerimientos del Instituto. Estos informes son mensuales pero en caso de eventualidades sobre la infraestructura gestionada se pueden requerir informes específicos de fallas o mejoras.

### ADMINISTRADOR SEGURIDAD DE LA INFORMACION

### PERFIL SERVICIOS PROFESIONALES ASESOR DE SEGURIDAD EN SITIO

En general, las funciones primordiales que debe realizar el asesor de seguridad informática, son:

- ✓ Realizar la administración de los dispositivos FireWall (4) Check-Point de acuerdo con las políticas de seguridad del Instituto.
- ✓ Realizar la administración de la management y el eventia de los dispositivos FireWall Check-Point de acuerdo con las políticas de seguridad del Instituto.
- ✓ Realizar la administración del Control de Contenido Barracuda de acuerdo con las políticas de seguridad del Instituto.
- ✓ Realizar la administración de la suite Epo de McAfee con sus módulos (Antivirus, Device control, application control, HIPS) de acuerdo con las políticas de seguridad del Instituto.
- ✓ Realizar la administración del AntiSpam McAfee de acuerdo con las políticas de seguridad del Instituto.
- ✓ Realizar la administración del IPS McAfee de acuerdo con las políticas de seguridad del Instituto.
- ✓ Realizar la administración del analizador de vulnerabilidades McAfee del instituto de acuerdo con las políticas de seguridad del Instituto. Se incluye el análisis, recomendaciones y apoyo al cierre proactivo de las vulnerabilidades que existan o que aparezcan sobre toda la plataforma computacional de ICETEX (Servidores, Estaciones de Trabajo – PCs, Impresoras, Equipos activos de telecomunicaciones, equipos activos de red, PDAs, entre otros).
- ✓ Realizar la administración del aplicativo GoAnyWhere y desarrollos de nuevos proyectos en este aplicativo de acuerdo con las políticas de seguridad del Instituto.
- ✓ Realizar las recomendaciones en materia de seguridad informática para el control de virus, Spyware, Spam y demás amenazas informáticas a nivel de redes LAN y WAN.
- ✓ Apoyar activamente el diagnóstico del estado actual del ICETEX frente al Sistema de Gestión de

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

- Seguridad de la Información (SGSI).
- ✓ Identificar las oportunidades de mejora del escenario actual.
  - ✓ Apoyar la realización del mapa de riesgos informáticos para el ICETEX.
  - ✓ Gerencia de Proyectos de seguridad informática asignados por la Dirección de Tecnología.
  - ✓ Cronograma y plan de trabajo y seguimiento de los proyectos asignados por la Dirección de Tecnología.
  - ✓ Definición e implementación directa sobre la plataforma de seguridad y networking del ICETEX de los proyectos que no requiera contratación externa.
  - ✓ Apoyar la implementación de las políticas impartidas frente al Sistema de Gestión de Seguridad de la Información (SGSI) y velar por el cumplimiento de las mismas.
  - ✓ Informe mensual de avance de proyectos asignados.
  - ✓ En caso de ser necesario, se deberá dar soporte en sitio en cualquiera de las 28 oficinas de ICETEX en todo el país.
  - ✓ Elaboración y/o actualización del diseño de un diagrama de red seguro, utilizando los equipos activos con los que cuenta el ICETEX, y sugiriendo la manera de fortalecerlo y los equipos requeridos para ello.
  - ✓ Asesoramiento e implementación de los planes de acción definidos para el aseguramiento de las plataformas operativas.
  - ✓ Asesoramiento e implementación de los diferentes planes de acción en la realización del Inventario de Activos de información.
  - ✓ Apoyar a la Dirección de Tecnología en la realización y mitigación de los mapas de Riesgos.
  - ✓ Adelantar análisis de seguridad de los servicios, aplicativos y bases de datos del ICETEX en la internet. Analizar y determinar los riesgos que estos pueden estar presentando, así como el plan de mitigación de estos riesgos.
  - ✓ Apoyo en la implementación del Modelo de Seguridad de la Información.
  - ✓ Apoyar la elaboración del plan de mitigación de riesgos y vulnerabilidades.
  - ✓ Apoyar la implementación de planes de mejoramiento relacionados con la Seguridad Informática del ICETEX mediante actividades relacionadas con la configuración de los dispositivos de networking y cualquier equipo o software relacionado.
  - ✓ Gestión de las plataformas de Seguridad con que cuenta el Instituto durante la vigencia del contrato (FireWall, Control Contenido, Suite Antivirus, IPS). Esto es, manejo activo de los Firewall, manejo de la plataforma de red, implementación en conjunto con los expertos de las acciones de mitigación de vulnerabilidades.
  - ✓ Firmar un acuerdo de confidencialidad.

El administrador de Seguridad debe contar como mínimo con una certificación sobre la plataforma CheckPoint.

### ENTREGABLES O PRODUCTOS DE LA ASESORIA EN SEGURIDA INFORMATICA

Entrega de informes de acuerdo con las directrices del oficial de seguridad informática o quien ejerza dicha función y el (los) Informe(s) de avance mensual de los proyectos de acuerdo con el plan estratégico de Tecnología aprobado por la Dirección y de los cambios efectuados sobre la plataforma tecnológica a nivel de seguridad informática, de acuerdo con los requerimientos del Instituto.

### ADMINISTRADOR NETWORKING

El contratista debe incluir dentro de la propuesta técnica el servicio de un profesional especializado en gestión de redes que preste sus servicios en las oficinas de ICETEX Dirección General en donde se encuentren ubicadas (hoy, Calle 3 No. 19-32) con disponibilidad las 24 horas, pero con horario básico que será acordado con la Dirección de Tecnología en el momento de la legalización del contrato y válido durante la vida de ejecución del contrato. El ICETEX tendrá la potestad de aprobar o no el recurso humano asignado, con lo cual el contratista hará entrega oportunamente durante el inicio del contrato, la(s) hoja(s) de vida del(os) aspirantes, y posteriormente en caso de cambio del profesional en seguridad, se debe reportar oportunamente con por lo menos quince (15) días hábiles de anticipación y haciendo entrega simultáneamente la hoja de vida del nuevo



## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

aspirante.

Los costos asociados con los servicios se pueden retirar del cobro mensual en caso de que no se requiera el servicio por parte de ICETEX, lo cual se informará con quince días de anticipación. Igualmente, en caso de incumplimiento en los términos pactados por este servicio con el debido informe del interventor, el contratista deberá retirar los costos asociados por el incumplimiento del servicio pactado.

El administrador de Networking debe contar como mínimo con la certificación Cisco CCNA

En general, las funciones primordiales que debe realizar el administrador de redes (networking), son:

- ✓ Servir de apoyo a la administración de los dispositivos FireWall (4) Check-Point en caso de ser requerido.
- ✓ Servir de apoyo a la administración del control de contenido Barracuda de acuerdo con las políticas de seguridad del Instituto.
- ✓ Apoyar el cierre de vulnerabilidades, según requerimientos de ICETEX.
- ✓ Apoyar activamente el diagnóstico del estado actual del ICETEX frente al Sistema de Gestión de Seguridad de la Información (SGSI).
- ✓ Identificar las oportunidades de mejora de la topología de red actual.
- ✓ Administrar todos los dispositivos activos de red del Centro de Cómputo Principal y De Contingencia que sean propiedad de ICETEX.
- ✓ Administrar todos los dispositivos activos de red del Edificio de Dirección General ICETEX - AGUAS.
- ✓ Administrar todos los dispositivos activos de red de todas las oficinas de ICETEX a nivel nacional
- ✓ Elaborar Cronogramas y planes de trabajo y seguimiento de los proyectos asignados por la Dirección de Tecnología
- ✓ Informe mensual de avance de proyectos asignados.
- ✓ En caso de ser necesario, se deberá dar soporte en sitio en cualquiera de las 28 oficinas de ICETEX en todo el país.
- ✓ Elaboración y/o actualización del diseño de un diagrama de red, utilizando los equipos activos con los que cuenta el ICETEX, y sugiriendo la manera de fortalecerlo y los equipos requeridos para ello.
- ✓ Asesoramiento e implementación de los planes de acción definidos para el mejoramiento de las plataformas operativas de networking.
- ✓ Asesoramiento e implementación de los diferentes planes de acción en la realización del Inventario de Activos de información.
- ✓ Apoyar a la Dirección de Tecnología en la realización y mitigación de los mapas de Riesgos.
- ✓ Apoyo en la implementación del Modelo de Seguridad de la Información.
- ✓ Apoyo en los planes de mitigación de riesgos y vulnerabilidades.
- ✓ Plan de implementación de oportunidades de mejora mediante la configuración de los dispositivos de networking y seguridad.
- ✓ Manejo de la plataforma de red, implementación en conjunto con los expertos de las acciones de mitigación de vulnerabilidades.
- ✓ Firmar un acuerdo de confidencialidad.
- ✓ Realizar periódicamente Análisis de Tráfico de red. Realizar informes y presentación de alternativas de mejoramiento de la infraestructura a nivel de rendimiento, alta disponibilidad y seguridad.

### ENTREGABLES O PRODUCTOS DE LA ASESORIA EN NETWORKING

Informe mensual de todas las tareas, relacionando números de Control de Cambio de evidencia del avance mensual de los proyectos de acuerdo con el plan Estratégico de Tecnología aprobado por la Dirección y de los cambios efectuados sobre la plataforma tecnológica a nivel de seguridad informática, de acuerdo con los requerimientos del Instituto.

**ANEXO 9.**  
**POLITICA DE BACKUP – RESTAURACIONES ICETEX**

El ICETEX define los siguientes tipos de Backups para respaldar su información: o Incremental: aplicada para los Backups diarios, solamente se almacenan las modificaciones realizadas desde la última copia full de seguridad, con lo que es necesario mantener la copia original sobre la que debe restaurarse el resto de copias.

o Full: aplicada para los Backups mensuales, incluyen una copia de carpetas, programas y Bases de Datos

Periodicidad de los Backups:

- ✓ **Diario:** Corresponde a la copia de información diaria.
- ✓ **Semanal:** Corresponde a la copia de la información realizada al finalizar la semana.
- ✓ **Mensual:** Corresponde a la copia full de la información realizada al finalizar el mes

Medios de almacenamiento:

El ICETEX define que para el resguardo de su información se utilizarán Cintas LTO Ultrium 5.

Rotación de Backups:

- ✓ Semanal: corresponde a un pool de cintas que se utiliza para los Backups diarios incrementales
- ✓ durante la semana, el cual será enviado a custodia externa y reutilizado dos semanas después.
- ✓ Por lo tanto, se requieren dos pool de cintas para cubrir el mes.
- ✓ Mensual: corresponde a un pool de cintas que se utiliza al final del mes en un Backup full, el
- ✓ cual será reutilizado seis meses después de su uso.
- ✓ Clon pool mensual: corresponde a una copia fiel del pool mensual el cual quedará en custodia
- ✓ externa sin rotación.

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

### Restauraciones por demanda:

- ✓ Restauración de la información en cualquier momento debido a daños o pérdida de la misma, la cual se debe realizar de acuerdo con los procedimientos definidos en cualquier día y momento. El CONTRATISTA debe presentar una planilla de programación de backups a un año, la cual será revisada y aprobada por ICETEX.

### Pruebas de Restauración:

- ✓ Verificar periódicamente la integridad y consistencia de la información respaldada de los Backups  
Realizados. El CONTRATISTA debe presentar una planilla de programación de pruebas de restauración a un año, la cual será revisada y aprobada por ICETEX.

### Informes de Gestión:

Documentos escritos con sus evidencias sobre la operación y administración de los Backups, los cuales están definidos de acuerdo con los procedimientos establecidos.

### Custodia externa:

Consiste en trasladar los medios de respaldo a un lugar de condiciones adecuadas situado fuera del sitio de donde se realizan dichas copias, de acuerdo con los procedimientos establecidos para tal fin.

A continuación se presenta el procedimiento de copias de respaldo que debe ser asumido por el CONTRATISTA:

### PROCEDIMIENTOS DE COPIA DE RESPALDO

1. **OBJETIVO:** Los objetivos de este procedimiento son: Contar con los recursos técnicos, humanos y procedimientos necesarios para realizar copias de toda la información de los servidores puestos en Centro de Computo Principal y De Contingencia de acuerdo con las necesidades propias de ICETEX.
2. **ALCANCE:** Durante la vigencia del Contrato, ICETEX especificará a que archivos del Centro de Cómputo Principal y De Contingencia se debe realizar copias y pruebas de restauraciones.
3. **DEFINICIONES**
  - **FULL:** Indica que es completo
  - **INC:** Indica que es incremental
  - **DIA:** una serie de días consecutivos
  - **MEN:** una vez al mes
  - **OFFSITEDIAPOOL:** Pool de almacenamiento diaria externo

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

- OFFSITEPOOL: : Pool de almacenamiento mensual externo
- ONSITEPOOL1: Pool de almacenamiento diario interno
- ONSITEPOOL2: Pool de almacenamiento diario interno
- MENSUALPOOL: Pool de almacenamiento mensual interno
- SEMANALPOOL: Pool de almacenamiento semanal interno
- VE: Versión Existente = 30 Días
- VD: Ultimas Borradas = 2 Versiones
- RE: Retención versiones existentes = 30 Días = NL: No Limit
- RO: Retención Ultimas Borradas = 60 Días

### 4. CONDICIONES GENERALES

#### Medios

El tipo de medios de almacenamiento externo o medios serán en cintas Linear Tape Open (LTO-5). Adicionalmente a esto, la herramienta realiza temporalmente Backups a disco mientras son llevados a la cinta correspondiente.

#### Actividades Operativas

El operador encargado de la administración de los backups, ejecutará las siguientes actividades:

1. Monitorear la infraestructura utilizada en la función operativa de backups.
2. Verificar diariamente la consola de administración de la herramienta de backups.
3. Llevar registro diario en bitácora de los backups ejecutados.
4. Realizar cambios en la política, instalaciones, configuración y/o creación de nuevos clientes, actualización, con el apoyo del proveedor cuando sea requerido. Tramitar soporte ante el proveedor en caso de fallas de acuerdo con el alcance del contrato de soporte del fabricante.
5. Control y seguimiento de la ejecución de los respaldos.
6. Tramitar soporte ante el proveedor en caso de fallas de acuerdo con el alcance del contrato de soporte del fabricante.
7. Realizar las actividades de restauración de las cintas de acuerdo con lo previsto en el capítulo 5 de este documento.

#### Actividades Administrativas

1. Informar oportunamente al técnico administrativo de la Dirección de Tecnología de ICETEX la necesidad de proveer cintas regulares cada vez que sea necesario.
2. Verificar que las cintas se encuentren correctamente etiquetadas (es decir, se debe verificar que la cinta tenga su label, marca legible por el lector optico). Ver la

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

siguiente tabla de "Solicitud de Label".

### TABLA DE SOLICITUD DE LABEL

Tipo de cartucho LTO Ultrium 5  
 Marca y modelo de la librería IBM System Storage TS3100  
 Cantidad de etiquetas 50 each  
 Rango de las etiquetas \* ICE140 – ICE190  
 Orientación etiquetas Horizontal X Vertical  
 Color de fondo de las etiquetas Blanco  
 Las letras y números en color negro, el fondo en color 4 (gris).

3. Preparar envío de cintas para entregar en custodia externa al proveedor.
4. Se debe garantizar para el proceso de migración y reclamación cintas scratch que deben permanecer en librería, esto con el fin de permitir una disponibilidad de medios para los Backups tanto OFFSITE como ONSITE y evitar que el proceso de toma de backups diario se detenga o cause inconvenientes.
5. Informar oportunamente al autorizado ante el proveedor de custodia externa del ICETEX, la necesidad de nuevas planillas de transporte.
6. Supervisar las actividades del operador encargado del manejo de las cintas.
7. Resguardar las cintas en la cintoteca mientras son llevadas para custodia externa.
8. Mantener un inventario de las cintas recibidas (nuevas) y las que estén en operación (cintoteca y custodia externa).
9. Proveer los materiales, herramientas, hardware y software requeridos para los backups.

### DESCRIPCIÓN DE ACTIVIDADES

### CARACTERÍSTICAS DEL DISEÑO DE BACKUPS

1. Garantizar el respaldo de la información.
2. Optimizar el uso de la herramienta de backups.
3. Programación de pruebas de restauración tanto de Bases de Datos como de File Systems.
4. Implementación de esquemas rotativos de consumo de medios.
5. Definición de tiempos de retención o almacenamiento de los medios.
6. Realizar restauraciones de backups periódicas o cuando éstas sean requeridas.

### CLASIFICACIÓN DE LOS RESPALDOS PARA EL SISTEMA DE BACKUPS DEL ICETEX



## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

Los archivos que son respaldados pueden variar desde archivos del sistema operativo, bases de datos y file systems de servidores, y archivos de configuración y de base de datos del servidor de backups.

Copia completa, aplicada para los backup Mensuales, incluyen una copia de carpetas, programas y Bases de Datos.

Copia incremental, aplicada para los Backups Diarios, solamente se almacenan las modificaciones realizadas desde la última copia full de seguridad, con lo que es necesario mantener la copia original sobre la que debe restaurarse el resto de copias.

### VOLUMEN DE INFORMACIÓN A COPIAR

Dado que la información a respaldar es dinámica, ICETEX entrega en su momento una tabla que contiene la ubicación específica de la información a respaldar (se incluyen las bases de datos, archivos de usuarios, sistemas operativos, configuraciones, buzones de correo, rutas e instalación de aplicaciones, file systems y cualquier otra que el ICETEX considere relevante para cumplir con sus objetivos misionales) la cual es susceptible de modificaciones, sin ser necesario cambiar la versión del presente procedimiento.

### ROTACIÓN DE CINTAS (NO INCLUYE BASE DE DATOS)

En la cintoteca deben permanecer las cintas que corresponden al backup diario con una vigencia semanal antes de ser reutilizadas.

Las cintas con backup full – mensual se mantienen en custodia externa permanente.

Dependiendo de la plataforma de backups utilizada para los respaldos de la información de ICETEX, se debe garantizar mantener una copia diaria, una semanal y una mensual de la información contenida en sus servidores de archivos, aplicaciones y bases de datos.

A continuación se detalla un ejemplo del esquema de rotación de las cintas gráficamente:

**SEMANA 1.** Durante la semana se utiliza un “pool 1” de cintas en los backups diarios. Al final de la semana se solicita transporte a custodia externa al proveedor encargado del transporte y bodegaje de medios para despachar una copia del pool 1 para su correspondiente salvaguarda.

**SEMANA 2.** Durante la semana se utiliza un “pool 2” de cintas en los backups diarios. Al final de la semana se solicita transporte a custodia externa al proveedor encargado del transporte y bodegaje de medios para despachar una copia del pool 2 para su correspondiente salvaguarda. Al mismo tiempo, la compañía que recoge el “pool 2” deja la copia del “pool 1”.

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

**SEMANA 3.** Durante la semana se utiliza un “pool 1” de cintas en los backups diarios. Al final de la semana se solicita transporte a custodia externa al proveedor encargado del transporte y bodegaje de medios para despachar una copia del pool 1 para su correspondiente salvaguarda.

**SEMANA 4.** Durante la semana se utiliza un “pool 2” de cintas en los backups diarios. Al final de la semana se solicita transporte a custodia externa al proveedor encargado del transporte y bodegaje de medios para despachar una copia del pool 2 para su correspondiente salvaguarda. Al mismo tiempo, la compañía que recoge el “pool 2” deja la copia del “pool 1”. En esta misma semana se realiza una copia full, la cual también se envía a custodia externa.

### RESTAURACIÓN DE BACKUPS

#### RESTAURACIONES POR DEMANDA

Se realizarán restauraciones de backups cuando éstas sean requeridas, teniendo en cuenta que si se solicita una cinta que se encuentra en custodia externa, una vez restaurada la información deberá solicitarse el envío inmediato a custodia externa.

#### PRUEBAS DE RESTAURACIÓN PERIÓDICA

Con el fin de verificar la integridad de la información respaldada, se realizarán restauraciones de forma periódica que lo garanticen.

##### Periodicidad

Se establece efectuar pruebas de restauración dos (2) veces al mes, ejecutadas al finalizar cada uno de los Full Backup programados de acuerdo con la programación de restauraciones mensuales. El ICETEX entregará un cronograma de las restauraciones que se deben realizar anualmente. Una vez realizada la verificación de la información restaurada, se debe borrar de los repositorios asignados y presentar el informe con las evidencias correspondientes. Cuando se requiera una restauración mensual específica, ésta remplazará una de las ya programadas.

##### Ubicación de la información restaurada

El tipo de información a restaurar y su ubicación, se detalla de común acuerdo entre la Dirección de Tecnología y el proveedor de la solución.

Informe Restauraciones:

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

La siguiente información debe ser parte del informe mensual de gestión de backups.

En el momento de efectuar restauraciones por demanda o periódicas, el operador encargado de la administración de los backups generará el informe respectivo, el cual deberá contener la siguiente información como mínimo:

- Fecha de Ejecución
- Información Restaurada
- Origen y Destino de la información restaurada
- Verificación de la restauración:
  - o Validar si la restauración fue exitosa.
  - o Validar si el tamaño y cantidad de archivos reportados en el backups corresponde a lo restaurado.
  - o Nombre de las carpetas o archivos restaurados.
  - o Ubicación de la restauración.
- Descripción de Problemas (si aplica)
- Descripción Plan de Acción a ejecutar por fallas en la restauración (si aplica)

El proveedor deberá anexar capturas de imagen de pantalla donde se evidencie las actividades realizadas.

Una vez restaurada la información el proveedor informará a través de correo electrónico a la Dirección de Tecnología de ICETEX para que sea valide la información restaurada y responderá por el mismo medio el resultado de la validación. Tanto los informes como los correos, serán incluidos en el informe de gestión mensual de operación.

### INFORMACIÓN DE GESTIÓN

Todos los servicios inherentes a la toma de los Backups, tal y como se define en este documento, deben realizarse de la manera estipulada en tiempos y frecuencia. Mensualmente se deben entregar a la Dirección de Tecnología de ICETEX las siguientes mediciones:

- Eventos ó incidencias presentadas en la infraestructura física y lógica de la solución de backups
- Inconsistencias detectadas en los medios utilizados (daños en cintas, sobredimensionamientos, etc.)
- Cantidad de cintas utilizadas en el período
- Cantidad de cintas enviadas a custodia externa
- Inventario de cintas nuevas, en operación y custodia externa
- Informe que contenga la identificación de cada cinta, el contenido de la información respaldada, la fecha, el(los) servidor(es) al(os) que pertenece.

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

### INDICADORES DE SERVICIO

Todos los servicios inherentes a la toma de los Backups, tal y como se define en este documento, deben realizarse de la manera estipulada en tiempos y frecuencia. El contratista entregará mensualmente las siguientes mediciones en el informe de gestión:

- Eventos ó incidencias presentadas en la infraestructura física y lógica de la solución de backups
- Inconsistencias detectadas en los medios utilizados (daños en cintas, sobredimensionamientos, etc.)
- Cantidad de cintas utilizadas en el período
- Cantidad de cintas enviadas a custodia externa.
- Informe que contenga la identificación de cada cinta, el contenido de la información respaldada, la fecha, el(los) servidor(es) al(los) que pertenece.

### CONSOLIDACIÓN Y PRESENTACIÓN DE INFORMES DE GESTIÓN

Los informes mensuales presentados al ICETEX, consolidan los indicadores de gestión, identificando el estado de la calidad y el progreso de las actividades correspondientes asociadas al servicio, así como las incidencias y problemas presentados durante el período, mediante la realización de consultas del aplicativo especializado en esta tarea y el análisis de la actividad de monitoreo.

Los informes de gestión de backups, contendrán la siguiente información:

1. Movimiento mensual de cintas, monitoreo y gestión de infraestructura y comportamiento mensual de backups, a cargo del proveedor del servicio de CENTRO DE CÓMPUTO.
2. Consolidación de incidencias registradas en la herramienta de gestión, a cargo del proveedor del servicio de CENTRO DE CÓMPUTO.
3. Mediciones de indicadores de desempeño.
4. Inventario de cintas.
5. Informe que contenga la identificación de cada cinta, el contenido de la información respaldada, la fecha, el(los) servidor(es) al(los) que pertenece.

A continuación se presenta la matriz de responsabilidad que será acordada con el proveedor del servicio de CENTRO DE CÓMPUTO:

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

### MATRIZ DE RESPONSABILIDADES

Actividades		ICETEX	GESTOR DE BACKUPS
<b>Operativas</b>			
1	Monitorear la infraestructura utilizada en la función operativa de backups.		X
2	Verificar diariamente la consola de administración de la herramienta de backups.		X
3	Llevar registro diario en bitácora de los backups ejecutados.		X
4	Realizar cambios en la política, instalaciones, configuración y/o creación de nuevos clientes, actualización, con el apoyo del proveedor cuando sea requerido.		X
5	Control y seguimiento de la ejecución de los respaldos.		X
6	Tramitar soporte ante el proveedor en caso de fallas de acuerdo con el alcance del contrato de soporte del fabricante.		X
7	Realizar las actividades de restauración de las cintas de acuerdo con lo previsto en la política de backup.	X	X
<b>Administrativas</b>			
1	Informar oportunamente al técnico administrativo de la Dirección de Tecnología de ICETEX la necesidad de proveer cintas regulares cada vez que sea necesario.	X	X
2	Verificar que las cintas se encuentren correctamente etiquetadas (es decir, se debe verificar que la cinta tenga su label, marca legible por el lector óptico).		X
3	Preparar envío de cintas para entregar en custodia externa al proveedor contratado.		X
4	Se debe garantizar para el proceso de migración y reclamación cintas scratch que deben permanecer en librería, esto con el fin de permitir una disponibilidad de medios para los Backus tanto OFFSITE como ONSITE y evitar que el proceso de toma de backups diario se detenga o cause inconvenientes.		X
5	Informar oportunamente al autorizado ante el proveedor de custodia externa del ICETEX, la necesidad de nuevas planillas de transporte.		X
6	Supervisar las actividades del operador encargado del manejo de las cintas.		X
7	Resguardar las cintas en la cintoteca mientras son llevadas para custodia externa.		X



## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

8	Mantener un inventario de las cintas recibidas (nuevas) y las que estén en operación (cintoteca y custodia externa).		X
9	Proveer los materiales, herramientas, hardware y software requeridos para los backups.	X	

IMPACTO DEL CONTRATO EN EL VESTIR

### ANEXO 10

### INFORMATIVO GOBERNABILIDAD PERSONAL REQUERIDO



El Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior

PERFILES PROFESIONALES REQUERIDOS PARA EL PROYECTO SIN DEDICACION DE TIEMPO COMPLETO EN LA SEDE DE ICETEX.

SERVICIO	ROL	FORMACIÓN ACADÉMICA	EXPERIENCIA LABORAL	CERTIFICACIONES
<b>GERENTE DE PROYECTO</b> (Recurso necesario durante la etapa de implementación del proyecto (Transición) o cuando se requieran cambios sobre la Infraestructura Entregada por el proveedor en la Etapa de Transición; posteriormente se debe hacer entrega al Gerente de Servicio, quien debe garantizar la operación de durante el Plazo del contrato.)	Gerente del proyecto	Ingeniero de sistemas o ingeniero electrónico o Ingeniero Eléctrico o ingeniero de telecomunicaciones con especialización en áreas administrativas o de gerencia proyectos; o Administradores o Informáticos con especialización en Áreas de Ingeniería de Sistemas, Electrónica o Comunicaciones	Experiencia mínima de 4 años como gerente, director o jefe de proyectos de prestación de servicios en el área de Tecnologías de la Información y Comunicaciones.	Certificación PMP (Project Management Professional), vigente. Expedida por el Project Management Institute PMI o Certificación CAPM del PMI
<b>GERENTE DE SERVICIO</b> (Asignado durante la duración del Proyecto)	Debe garantizar la administración y soporte efectivo de la operación durante los 36 meses del contrato	Ingeniero de Sistemas, electrónico, eléctrico o Telecomunicaciones con certificación ITIL V2011 Foundations, Conocimientos en: Gerencia de Proyectos, Administración del Cliente, Manejo de Conflictos	3 años en Áreas Técnicas, de Servicio o Atención a clientes y mínimo 2 años como Gerente de Servicio, Gerencia de Proyectos, Comercial y Atención de Clientes Telecomunicaciones.	Certificación ITIL Fundamentos versión 2011. Preferiblemente si adicionalmente tiene certificación ITIL OSA Intermedio. Certificar por el contratista, experiencia y Conocimientos Específicos de este personal, en: Redes de telecomunicaciones, Tecnologías de la información, Mercado de las telecomunicaciones, Servicio al Cliente.

NOMBRE DEL REPRESENTANTE LEGAL

FIRMA DEL REPRESENTANTE LEGAL

NOMBRE DE CONTRATISTA

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

### CERTIFICACIONES MINIMAS REQUERIDAS DE EXPERIENCIA PARA EL PERSONAL EN SITIO

DESCRIPCION FUNCIONES	CERTIFICACIONES REQUERIDAS/EXPERIENCIA
Web Master	<ul style="list-style-type: none"> <li>- Título Profesional ingeniería Sistemas</li> <li>- Tarjeta profesional</li> </ul> <p><b>CERTIFICACIONES DE EXPERIENCIA, EN:</b></p> <ul style="list-style-type: none"> <li>➤ Experiencia profesional mínimo de 3 años en roles asociados al cargo</li> <li>➤ Administración de IIS 7.5.</li> <li>➤ Administración de los sistemas Operativos Windows Server 2003, 2008.</li> <li>➤ Programación .ASP y .NET, por lo menos dos (2) años.</li> <li>➤ Programación Java Script, CSS, JQUERY, HTML5.</li> <li>➤ Conocimiento en Bases de Datos SQL Server 2000 y 2008, por lo menos un (1) años.</li> <li>➤ Dominio de estándares W3C.</li> </ul>
Administrador Networking	<ul style="list-style-type: none"> <li>- Título Profesional ingeniería Sistemas, electrónica, Telecomunicaciones o afines.</li> <li>- Tarjeta profesional.</li> <li>- 3 años de experiencia laboral en administración de redes</li> </ul> <p><b>CERTIFICACIONES:</b></p> <ul style="list-style-type: none"> <li>- Certificación de Experiencia mínima de 3 años en administración y operación de redes.</li> <li>- Certificación CCNA.</li> <li>- Experiencia en administración de redes basadas en Cisco</li> </ul>
Seguridad de la información	<ul style="list-style-type: none"> <li>- Título Profesional ingeniería Sistemas, electrónica, telecomunicaciones o afines.</li> <li>- Tarjeta profesional.</li> <li>- Mínimo 3 años de experiencia profesional en roles relacionados con el cargo</li> </ul> <p><b>CERTIFICACIONES:</b></p> <ul style="list-style-type: none"> <li>- Certificación en plataforma CheckPoint</li> <li>- Experiencia en administración de soluciones de seguridad de McAfee</li> </ul>
Administrador base de datos	<ul style="list-style-type: none"> <li>- Experiencia mínimo de 3 años como Administrador de Base de Datos (DBA) en Oracle 10g y/o 11g.</li> <li>- Experiencia como Administrador de Base de Datos (DBA) SQL Server 2003 y/o 2008.</li> <li>- Certificación mínima Oracle OCA</li> </ul>

**Nota:** Todas las personas en sitio, relacionadas en la tabla anterior, deberán mantener disponibilidad para contingencias en caso de que estas se presenten en horarios de oficina establecidos inicialmente en caso de cualquier evento sobre la infraestructura que gestionen.

**SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015**
**ANEXO II**  
**INFORMATIVO GOBERNABILIDAD ETAPAS DEL PROYECTO**

ETAPA	FASES	OBJETIVO	CONDICION INICIAR ETAPA	INSUMOS LA ETAPA	DE MESES TRANSICIÓN	ENTREGABLES	DURACIÓN MÁXIMA
<b>TRANSICION:</b> entrega de los servicios de los proveedores actuales al CONTRATISTA. Duración Máxima total de 2 meses. Responsabilidad sobre la continuidad del servicio será de proveedores actuales hasta que a través de la gestión de cambios se entregue la Administración al CONTRATISTA y dicho cambio sea exitoso.	a. Planeación b. Diseño de la Solución c. Ejecución del Plan de Transición	Diseño e instalación de la solución a partir de la línea base. ICETEX solicitará el plan que permita corroborar la línea base. Se debe garantizar la continuidad del servicio y tiempos de respuesta. Durante esta fase no se penalizan ni se miden ANS		Acta de inicio del proyecto. Documentación, reuniones, entrevistas, visitas. Conocer las instalaciones. Infraestructura	1	Plan de trabajo aprobado por la gerencia del proyecto y la Supervisión y /o Interventoría. Informe donde detalle la solución y diagrama de Red con dispositivos de seguridad incluidos (Firewall, Centro de Cómputo en Operación, Servidores, filtro antispam de correo), mostrando su integración con los demás componentes de la red. Plan de trabajo para la implementación y sensibilización de las Gestiones de Solicitudes de Usuarios, Incidentes, Requerimientos, Gestión de Cambios, Gestión del Catálogo de Servicios y Gestión de Problemas. (Nota: La implementación de Incidentes debe finalizarse antes del inicio de la etapa de Operación) Plan para realizar campaña de sensibilización a Nivel Nacional por el cambio de operador.	Para la entrega de la solución hasta 2 meses después del perfeccionamiento del contrato
					2	Herramienta de Gestión de Servicios de Seguimiento de casos o tickets configurada. Enlace de Internet instalado y configurado Enlace entre el Centro de Cómputo externo y El Centro de Cómputo de la Sede Nacional Infraestructura (hardware	



### SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

						y software) instalada en el Centro de Datos externo.	
					3	<p>Pruebas de aceptación del esquema de soporte y administración de cada servicio.</p> <p>Informe y diagnóstico de la migración.</p> <p>Implementar y configurar los ANS en la herramienta de gestión de apertura y seguimiento de casos o tickets relacionado con los Servicios</p> <p>Contratados, en Línea base de software y documentación técnica.</p> <p>Acta de inicio de la administración de cada Sistema de Información del ICETEX que estará a cargo del contratista, incluyendo la línea base de la documentación.</p> <p>Actas de aceptación de entrada en producción de cada servicio debidamente firmadas por las partes (Incluyendo el Operador, la Interventoría y o/ Supervisión y las entidades involucradas), con sus correspondientes manuales de instalación.</p> <p>Informe financiero del contrato.</p> <p>Plan de capacitación sobre las herramientas y esquemas de soporte al ICETEX.</p> <p>Plan de Calidad para asegurar el cumplimiento de los ANS.</p> <p>Otros informes solicitados por la supervisión.</p>	

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

<b>OPERACIÓN:</b> Operación de los servicios, monitoreo, medición de los ANS. Responsabilidad sobre la continuidad del servicio será de El CONTRATISTA.	a. Operación de los servicios, Configuración ANS y Herramientas de Monitoreo, ajustes, afinamiento (1 mes)	Configurar e instalar las herramientas que permitan la medición y monitoreo de los ANS. El CONTRATISTA presta el servicio y configura ANS, no se penalizan, se miden, se ajustan los ANS y la infraestructura. Seguimiento Línea Base. <b>Nota:</b> La configuración de los ANS de Mesa debe realizarse en la Etapa anterior.	Aprobación etapa anterior	Aprobación de la línea base y de los ANS y su medición de común acuerdo entre las partes de tal forma que se garanticen los adecuados tiempos de respuesta para la operación del ICETEX.	Herramientas de monitoreo y medición de ANS en funcionamiento. Operación inicial, configuración y monitoreo de servicios, infraestructura y ANS. Plan trabajo para la implementación y sensibilización de: *Gestión de Capacidad. (Que debe incluir plan de capacidad transversal para todos los servicios para ejecutar durante la duración del contrato) *Gestión de Activos y Configuración. *Gestión del Conocimiento. *Gestión de Niveles de Servicios. *Gestión de Portafolio de Servicios. Ajustes a los procesos y procedimientos del modelo de gestión.	1 mes
	b. Operación de los servicios, medición de ANS, seguimiento línea base (máximo el plazo del contrato)	Es la etapa donde El CONTRATISTA empieza a prestar el servicio. Se mide, se penaliza. El Seguimiento de la Línea Base se realizará cada tres (3) meses.	Terminar la etapa anterior.	Estrategia de entrega de todos los servicios. ANS de los servicios. Acta de inicio de operación	Ejecución Plan de Trabajo Implementación y Sensibilización de Procesos. Acta Comité Operativo - Mensual. Informe general del estado de cada uno de los servicios y ANS. Detallado en el Anexo Informativo - Reportes Operación.	Entrega Mensual Informe gestión los cinco primeros días hábiles del siguiente mes. El servicio cubre los 36 meses de operación
					Comité semanal de control de cambios.	Calendario Semanal de cambios, Informe mensual de control de cambios.
					Monitoreo y revisión de ANS y línea Base.	Cada 2 meses.
					Planes de Contingencia.	Se verificarán dos veces al año
					Ejecución plan de capacidad	Mínimo 1 por año.

### SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

		DEVOLUCIÓN: Transición con el nuevo operador últimos 2 meses del contrato.					
	c. Devolucion y Entrega de los Servicios (Últimos 2 meses de operación)	Entrega de Servicios. Entrega de equipos, información, procedimientos, instalaciones, mejoras y demás elementos a los cuales se encuentra obligado El CONTRATISTA.	Terminar la etapa anterior.	Acta de finalización del contrato.		Plan de entrega de los Servicios, validado y aprobado por el ICETEX. Acta de terminación del servicio e infraestructura aprobado por el ICETEX. Entrega de la documentación de proyecto. Plan de Transición.	Durante los 2 últimos meses de operación, simultáneamente con la operación.

**SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015**
**ANEXO 12**
**INFORMATIVO GOBERNABILIDAD DESCRIPCION DE PERFILES REQUERIDOS DEL PERSONAL**

ROL	DESCRIPCIÓN DEL PERFIL	DEDICACIÓN
Gerente de proyecto (Transición)	Un (1) Ingeniero con al menos cuatro (4) años de experiencia en gerencia de proyectos de Infraestructura y Centro de Datos. Experiencia específica de al menos tres (3) años en Outsourcing de Servicios de Centro de Cómputo y Telecomunicaciones.	50%
ROL	DESCRIPCIÓN DEL PERFIL	DEDICACIÓN
Personal en Sitio	<p>Cuatro (4) Ingenieros especialistas en:</p> <ul style="list-style-type: none"> <li>• ADMINISTRADOR BASES DE DATOS ORACLE</li> <li>• ADMINISTRADOR PORTAL WEB</li> <li>• ADMINISTRADOR SEGURIDAD INFORMATICA</li> <li>• ADMINISTRADOR NETWORKING</li> </ul> <p>Este personal debe contar con la experiencia y perfiles específicos definidos en ANEXO 8. PERFIL Y FUNCIONES DE PERSONAL EN SITIO. Este recurso tendrá una asignación de tiempo completo, y su ubicación será en las instalaciones de EL ICETEX, atendiendo las solicitudes que no puedan ser solucionadas directamente por la mesa de ayuda. Este recurso apoyará además todas las tareas operativas que requiera EL ICETEX. Los ingenieros deben de tener como objetivo el cumplimiento de los ANS.</p>	100%
Gerente de Servicio	Un (1) ingeniero de sistemas con al menos tres (3) años de experiencia en administración de operaciones tecnológicas bajo el rol de gerente de servicio administrando operaciones que incluyan como alcance la gestión de servicios de Centro de Datos, Telecomunicaciones y servicios de Gestión de TI	Según requerimientos



## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

### ANEXO 13

#### INFORMATIVO GOBERNABILIDAD OFRECIMIENTO DEL PERSONAL MINIMO REQUERIDO (CENTRO DE COMPUTO PRINCIPAL Y DE CONTINGENCIA)

El suscrito representante legal del Contratista se compromete a suministrar el Personal Mínimo requerido que se describe a continuación al momento de suscribir el acta de inicio del contrato que resulte del presente proceso de selección pública del contratista, el cual cumplirá con lo descrito en el presente formato.

Operador para el servicio de Copias de Respaldo	Un (1) Ingeniero con al menos tres (3) años de experiencia. Experiencia específica en Copias de Respaldo de Servidores Windows, Solaris, Linux con herramientas tipo Tivoli o similares. El CONTRATISTA debe incluir en su propuesta la hoja de vida con los respectivos soportes que permitan comprobar el cumplimiento de este requerimiento. Las funciones básicas de este personal son responder por las copias de respaldo, su historial y restauraciones cuando sea requerido y de acuerdo con las Políticas de de Backup establecidas por ICETEX. Este recurso debe gestionar las copias de respaldo y recuperación tanto en Centro de Computo Principal y De Contingencia por demanda de acuerdo con las necesidades propias de la operación de ICETEX durante la vigencia del contrato en la modalidad 7x24. Su ubicación será en las instalaciones del proveedor.	Según requerimientos
Administrador de Sistema Operativo Oracle-Linux.	Un (1) Ingeniero con al menos tres (3) años de experiencia. Experiencia específica en administración de Servidores Oracle - Linux. Este personal debe contar con la experiencia y perfiles específicos en administración de servidores ORACLE-LINUX. Este recurso debe gestionar las configuraciones y administración de los servidores ORACLE-LINUX tanto en Centro de Computo Principal y De Contingencia por demanda de acuerdo con las necesidades de ICETEX durante la vigencia del contrato en la modalidad 7x24. Su ubicación será en las instalaciones del proveedor.	Según requerimientos

Firma Representante Legal

**SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015**
**ANEXO 14**  
**INFORMATIVO GOBERNABILIDAD REPORTES OPERACIÓN**

Servicio	Descripción	Periodicidad
Seguridad	Informe de los sistemas de detección de intrusos de host (servidor) Debe contener para cada uno de los dispositivos instalados: política actualizada, eventos relevantes durante el periodo, recomendaciones y conclusiones.	Mensual
	Informe de análisis de vulnerabilidades y remediación de las mismas. Políticas implementadas, cambios realizados durante el periodo, recomendaciones y conclusiones.	
Soporte y monitoreo	Informe de los ANS de cada uno de los servicios que operan en el centro de datos.	Mensual
Almacenamiento	Reporte de consumo y disponibilidad de almacenamiento - Copias de respaldo de respaldos ejecutadas - Copias de respaldo que fallaron y acciones correctivas	Mensual
Aplicaciones	Reporte de eventos inesperados máximo 24 horas luego de presentarse el problema donde se identifique - Situación presentada, impacto. - Acciones Tomadas - Tiempo de solución.	Por demanda
	Informe mensual sobre el comportamiento del desempeño de las aplicaciones, disponibilidad, consumo de recursos, estadísticas de consumo, tiempos de respuesta y uso que incluya comportamiento estadístico de uso de y desempeño de aplicaciones, procesos que consumen más recursos, páginas más pesadas, número de usuarios, páginas más visitadas, tiempos de respuesta, recomendaciones.	Mensual
Bases de datos	Llevar bitácora de control de las bases de datos del ICETEX, incluyendo como mínimo crecimiento mensual, incidentes, ejecución de backup, tareas automáticas, análisis de errores y alertas. Se requiere generar alertas automáticas a los líderes de las aplicaciones en el momento en que no se encuentren disponibles las bases de datos.	Mensual
Control de Cambios	Cambios realizados en el Mes anterior. Se debe entregar los 5 primeros días hábiles del mes.	Mensual

SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

**ANEXO 15.**  
**CONTINGENCIA TECNOLÓGICA REQUERIDA DRP**  
**(BIA ICETEX TIEMPOS RPO)**

APLICATIVOS - SERVICIOS	RPO<= 4HORAS	RPO<=24 HORAS	SERVIDOR O SERVICIO ASOCIADO PARA EL CUMPLIMIENTO DE LOS RPO Y RTO
C&CTEX	X		ITEM 14, ANEXO 6. SERVICIOS DE COLOCACION - SITIO PRINCIPAL
APOTEO SYS	X		ITEM 10, ANEXO 6. SERVICIOS DE COLOCACION - SITIO PRINCIPAL
MERCURIO	X		ITEM 4, ANEXO 7. SERVICIOS DE COLOCACION - SITIO DE CONTINGENCIA
BIZAGI	X		ITEM 5, ANEXO 6. SERVICIOS DE COLOCACION - SITIO PRINCIPAL
PORTAL WEB	X		ANEXO 5.1. HOSTING LINEA BASE CENTRO DE CÓMPUTO PRINCIPAL. Ver numeral 9.2.2. HOSTING PORTAL WWW.ICETEX.GOV.CO.
SEVINPRO (SERVICIO RED)	X		NUMERAL 9.1. TELECOMUNICACIONES CENTRO DE CÓMPUTO PRINCIPAL, DE CONTINGENCIA Y DIRECCIÓN GENERAL.
DECEVAL (SERVICIO RED)	X		NUMERAL 9.1. TELECOMUNICACIONES CENTRO DE CÓMPUTO PRINCIPAL, DE CONTINGENCIA Y DIRECCIÓN GENERAL.
IGMETRICA (SERVICIO RED)		X	NUMERAL 9.1. TELECOMUNICACIONES CENTRO DE CÓMPUTO PRINCIPAL, DE CONTINGENCIA Y DIRECCIÓN GENERAL.
REPORTEADOR		X	ITEM 10 y 14, ANEXO 6. SERVICIOS DE COLOCACION - SITIO PRINCIPAL
ORACLE	X		ITEM 1, ANEXO 6. SERVICIOS DE COLOCACION - SITIO PRINCIPAL
DDCMANAGER		X	ITEM 14, ANEXO 6. SERVICIOS DE COLOCACION - SITIO PRINCIPAL

**ANEXO 16.**  
**CONTINGENCIA TECNOLÓGICA REQUERIDA**  
**(BIA ICETEX TIEMPOS RTO)**

APLICATIVOS	RPO<= 4HORAS	RPO<=8 HORAS	RPO<=48 HORAS	SERVIDOR O SERVICIO ASOCIADO
C&CTEX	X			ITEM 14, ANEXO 6. SERVICIOS DE COLOCACION - SITIO PRINCIPAL.
APOTEO SYS	X			ITEM 10, ANEXO 6. SERVICIOS DE COLOCACION - SITIO PRINCIPAL

**SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015**

APLICATIVOS	RPO<=4 HORAS	RPO<=8 HORAS	RPO<=48 HORAS	SERVIDOR O SERVICIO ASOCIADO
MERCURIO	X			ITEM 4, ANEXO 7. SERVICIOS DE COLOCACION - SITIO DE CONTINGENCIA
BIZAGI	X			ITEM 5, ANEXO 6. SERVICIOS DE COLOCACION - SITIO PRINCIPAL
PORTAL WEB	X			ANEXO 5.I. HOSTING LINEA BASE CENTRO DE CÓMPUTO PRINCIPAL. Ver numeral 9.2.2. HOSTING PORTAL <a href="http://WWW.ICETEX.GOV.CO">WWW.ICETEX.GOV.CO</a> .
SEVINPRO (SERVICIO RED)		X		NUMERAL 9.I. TELECOMUNICACIONES CENTRO DE CÓMPUTO PRINCIPAL, DE CONTINGENCIA Y DIRECCIÓN GENERAL.
DECEVAL (SERVIDOR EXTERNO)	X			NUMERAL 9.I. TELECOMUNICACIONES CENTRO DE CÓMPUTO PRINCIPAL, DE CONTINGENCIA Y DIRECCIÓN GENERAL.
IGMETRICA (SERVICIO RED)		X		NUMERAL 9.I. TELECOMUNICACIONES CENTRO DE CÓMPUTO PRINCIPAL, DE CONTINGENCIA Y DIRECCIÓN GENERAL.
REPORTEADOR			X	ITEM 14, ANEXO 6. SERVICIOS DE COLOCACION - SITIO PRINCIPAL.
ORACLE (ODA-X32-L2)	X			ITEM 1, ANEXO 6. SERVICIOS DE COLOCACION - SITIO PRINCIPAL
ORACLE -TOAD (APLICACIÓN CLIENTE)	X			NUMERAL 9.I. TELECOMUNICACIONES CENTRO DE CÓMPUTO PRINCIPAL, DE CONTINGENCIA Y DIRECCIÓN GENERAL.
CRM (PROVEEDOR EXTERNO)				NUMERAL 9.I. TELECOMUNICACIONES CENTRO DE CÓMPUTO PRINCIPAL, DE CONTINGENCIA Y DIRECCIÓN GENERAL.
CORREO ELECTRÓNICO	X			ITEM 12, ANEXO 6. SERVICIOS DE COLOCACION - SITIO PRINCIPAL.
COBOL, SOLARIS + COBOL	X			SOLO CONSULTA
INTERNET (SERVICIO RED)			X	NUMERAL 9.I. TELECOMUNICACIONES CENTRO DE CÓMPUTO PRINCIPAL, DE CONTINGENCIA Y DIRECCIÓN GENERAL.
DOCMANAGER			X	ITEM 14, ANEXO 6. SERVICIOS DE COLOCACION - SITIO PRINCIPAL



SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

ANEXO 17.

**CONDICIONES MINIMAS REQUERIDAS PARA LOS CENTRO DE CÓMPUTO PRINCIPAL Y DE CONTINGENCIA OFRECIDOS POR LOS CONTRATISTAS**

El CONTRATISTA debe entregar las siguientes instalaciones que hacen parte integral de la solución ofrecida:

**AIRE ACONDICIONADO Y SISTEMA ELÉCTRICO REGULADO.**

- Sistema de aires acondicionados de precisión que permite tener un medio ambiente que cumple con los estándares de temperatura y humedad que garanticen un correcto funcionamiento de los servidores y equipos de comunicación.
- Sistema de *backup* para Energía AC regulada por medio de *UPS* de última generación, que soporta la operación en caso de suspensión temporal del servicio eléctrico. Adicionalmente, se debe tener una planta eléctrica o similar en el edificio. En caso de daños eléctricos extremos, El CONTRATISTA debe informar de manera inmediata a ICETEX y la autonomía de los sistemas anteriormente descritos debe permitir por lo menos media hora para proceder con un apagado normal de los equipos mientras se normaliza el servicio de fluido eléctrico.

**ÁREAS CERRADAS SEGURAS**

Para un grado de privacidad y seguridad aún mayor, EL CONTRATISTA debe contar con seguridad propia (según características de racks y equipos del ICETEX) con accesos privados al personal técnico de operadores y demás que mantienen la operación por parte del CONTRATISTA y al personal autorizado de ICETEX que requiera ingresar a las instalaciones en donde se encuentren los servidores.

**SEGURIDAD ELECTRÓNICA**

- Sistema de Control de Acceso compuesto por varios niveles de seguridad que permita la restricción de acceso al Internet Centro de Cómputo ubicado en las instalaciones de EL CONTRATISTA.
- Sistema de video digital compuesto por cámaras con capacidad de reconstrucción secuencial de eventos, y detección de movimiento por áreas. La información debe ser almacenada en formato de video digital (MPEG4) con copias de seguridad periódicas, las cuales deben estar disponibles permanentemente para ser consultadas por ICETEX en caso de requerirse.

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

- Sistema de control de incendios basados con detectores de humo.

### Seguridad Lógica

Con el propósito de proteger el portal [www.icetex.gov.co](http://www.icetex.gov.co) en el *Centro de Cómputo* de EL CONTRATISTA, se debe contar con *firewall* dedicado e independiente para ICETEX. Este servicio es personalizado para ICETEX, de tal manera que cada granja de servidores cuenta con sus propias reglas de protección y características de seguridad a nivel de usuarios y sesiones. Se requiere:

- ✓ Instalación del Sistema Operativo y aplicaciones siguiendo un *checklist* estricto que deberá ser aprobado por ICETEX y aplicando los últimos *services pack*.
- ✓ Aplicación de un *check list* de seguridad para Sistema Operativo y servidor de Web.
- ✓ Apoyo especializado para asegurar las bases de datos, aplicativos y desarrollos propios.
- ✓ Utilización de *software* proactivo de seguridad para detección de vulnerabilidades para verificación del correcto aseguramiento del Sistema Operativo y aplicaciones. Se incluye la instalación, configuración y administración del HIPS e IPS por parte del CONTRATISTA.

### Ambiente LAN

Todos los servidores compartidos o dedicados que sean proporcionados por el CONTRATISTA deben contar con tarjetas de red duales físicamente conectadas a un *Switch* multinivel capas 2, 3 y 4 con redundancia en procesador y fuente de poder.

ICETEX cuenta actualmente en Centro de Cómputo Principal (Santa Bárbara) con dos switches cisco catalyst 2960g series, mediante los cuales se interconectan los servidores de misión crítica con el resto de la red WAN. Es responsabilidad del CONTRATISTA la operación, soporte, mantenimiento y gestión de garantías relacionadas con estos elementos activos de red. Cualquier cambio que se requiera sobre la plataforma será realizado por el personal en sitio descrito en el numeral 9.4.4. "Gestion VoIP Y Networking en Sitio".

Todos los servidores a nivel LAN se comunican con el *switch* a una velocidad de 1000 Mbps *Full-Dúplex*, siguiendo el estándar *Gigabit Ethernet*.

### Conectividad con Internet

El CONTRATISTA debe entregar enlaces redundantes y balanceados a nivel



#### SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

internacional y nacional en anchos de banda de  $n \times 64K$  y con conexión directa y redundante con el NAP Colombia que permite manejar todo el tráfico local de manera óptima y eficiente. En el caso particular del ICETEX, se ofrece un acceso a Internet para su hosting a 15 Mbps 1:1, una capacidad de almacenamiento de 1TB en cada uno de los servidores y una dirección IP para los dominios <http://www.icetex.gov.co> e <http://www.icetex.edu.co>.

Los anchos de banda propuestos "garantizan" un manejo de tráfico independiente por cada dirección IP sin importar si la solicitud viene desde el *backbone* de Internet o del NAP Colombia, esta funcionalidad se implementa utilizando dispositivos administradores de ancho de banda inteligentes.

#### COPIAS DE RESPALDO Y PRUEBAS DE RESTAURACIONES

De acuerdo con las condiciones definidas en el anexo ANEXO 9. "POLITICA DE BACKUP – RESTAURACIONES ICETEXEL CONTRATISTA", se requiere un sistema de respaldo: full mensual, incremental semanal y diario, los cuales deben estar disponibles para ser restaurados en el evento en que sean requeridos por ICETEX durante la duración del contrato. Se requiere acuerdo de nivel de servicio superior al 99,8% y con los costos detallados del valor del servicio, así como de las multas por mora en los casos de incumplir dichos acuerdos. Se requiere un claro procedimiento en labores de recuperación de desastres y/o restauración de copias de respaldo.

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

### ANEXO No. 18 ACUERDOS DE NIVELES DE SERVICIO (ANS)

ANS	DESCRIPCION	MEDICION	META	PERIODO	DESCUENTO (PENALIZACION)												
TELECOMUNICACIONES																	
Cumplimiento de la Etapa de Transición dentro del Plazo Establecido	El supervisor del Contrato por parte de ICETEX recibe en producción a satisfacción, antes del 30 de junio de 2015, todos los servicios de telecomunicaciones a nivel nacional (Integración de las Oficinas Regionales de ICETEX con el Sistema Central mediante WAN, Centro de Computo Principal y De Contingencia Integrado a la WAN para los servicios de Voz y Datos propios de ICETEX), servicios de Centro de Computo Principal y De Contingencia, y Servicios de Colocación Portal ICETEX tal como se solicita en los ANEXO 2 al ANEXO 7.	Porcentaje de Servicios en Producción	100%	ETAPA DE TRANSICION	<p>1% DEL VALOR TOTAL DEL CONTRATO POR CADA DIA DE INDISPONIBILIDAD TOTAL DEL CENTRO DE CÓMPUTO PRINCIPAL POR LA NO ENTREGA OPERATIVA OPORTUNA DEL MISMO.</p> <p>10% DEL VALOR TOTAL MENSUAL DEL SERVICIO POR CADA DIA DE INDISPONIBILIDAD TOTAL DE CADA CANAL DE TELECOMUNICACIONES PRINCIPAL (FILAS 35, 36 Y 27 A LA 31 DEL ANEXO 3)</p> <p>10% DEL VALOR DEL SERVICIO MENSUAL ASOCIADO POR CADA DIA DE INDISPONIBILIDAD DE CADA CANAL DE TELECOMUNICACIONES NO PRINCIPAL Y/O CADA SERVICIO AFECTADO.</p>												
Disponibilidad de canal de telecomunicaciones.	Todos los canales deben estar disponibles por lo menos el 99.8% del tiempo al mes, 24 horas al día durante todos los días del mes.	<p>NHD = Número de horas disponibles</p> <p>NHOC = Número de horas del mes que debería estar operando cada canal</p> <p>% = (NHD/NHOC)*100</p>	99.8% para todos los enlaces excepto para Mocoa, San Andrés, Barranca bermeja, Leticia y San Gil cuyos descuentos se hacen a partir del 99.6%		<p>Los descuentos asociados a esta Medición por indisponibilidad de servicio por cada canal, son:</p> <table><tr><th>Valor del Descuento(%)</th><th>% Disponibilidad (D)</th></tr><tr><td>0%</td><td>100 &gt;= X &gt;= P</td></tr><tr><td>5%</td><td>P &gt; X &gt;= 95.0</td></tr><tr><td>10%</td><td>95.0 &gt; X &gt;= 90.0</td></tr><tr><td>15%</td><td>90.0 &gt; X &gt;= 80.0</td></tr><tr><td>100%</td><td>X &lt; 80</td></tr></table> <p>Donde P=99.8% para todos los enlaces excepto Mocoa, San Andrés, Barrancabermeja, Leticia y San Gil y P=99.6 para estas ciudades.</p> <p>De acuerdo con esta tabla, ICETEX descantara de la factura mensual por canal un porcentaje (Valor) del valor del(os) canal(es) afectado(s).</p>	Valor del Descuento(%)	% Disponibilidad (D)	0%	100 >= X >= P	5%	P > X >= 95.0	10%	95.0 > X >= 90.0	15%	90.0 > X >= 80.0	100%	X < 80
Valor del Descuento(%)	% Disponibilidad (D)																
0%	100 >= X >= P																
5%	P > X >= 95.0																
10%	95.0 > X >= 90.0																
15%	90.0 > X >= 80.0																
100%	X < 80																
Disponibilidad del servicio de Video conferencia	Video conferencia oficinas Barranquilla, Bogotá, Bucaramanga, Cali y Medellín.	La disponibilidad del servicio de videoconferencia en cada sede, es medida de manera independiente para cada una	99.8%	MES	Los descuentos asociados a esta Medición por indisponibilidad de servicio por cada sede, son:												

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

		<p>de las sedes en las cuales se presta el servicio y se calcula mediante la siguiente fórmula:</p> $\% = 100 - (T_s - T_{ind}) / T_s$ <p>En donde: T(ind) es el tiempo de indisponibilidad en minutos desde el momento de haber sido detectada, ya sea proactiva o reactivamente el funcionamiento Ts: es el tiempo de servicio medido en minutos. Este tiempo mide la cantidad de minutos en el mes en el cual se realiza la medición</p>			<table><tr><th>Valor del Descuento(%)</th><th>% Disponibilidad (D)</th></tr><tr><td>0%</td><td>100 &gt;= X &gt;= 99.8 *</td></tr><tr><td>5%</td><td>99.8 &gt; X &gt;= 95.0 *</td></tr><tr><td>10%</td><td>95.0 &gt; X &gt;= 90.0</td></tr><tr><td>15%</td><td>90.0 &gt; X &gt;= 80.0</td></tr><tr><td>100%</td><td>X &lt; 80</td></tr></table> <p>De acuerdo con esta tabla, ICETEX descontara de la factura mensual un porcentaje (Valor) del valor del(os) sede(es) afectado(s).</p>	Valor del Descuento(%)	% Disponibilidad (D)	0%	100 >= X >= 99.8 *	5%	99.8 > X >= 95.0 *	10%	95.0 > X >= 90.0	15%	90.0 > X >= 80.0	100%	X < 80
Valor del Descuento(%)	% Disponibilidad (D)																
0%	100 >= X >= 99.8 *																
5%	99.8 > X >= 95.0 *																
10%	95.0 > X >= 90.0																
15%	90.0 > X >= 80.0																
100%	X < 80																
Disponibilidad de la herramienta de monitoreo	Herramienta(s) de monitoreo de servicio de red contra el cumplimiento de ANS	<p>NHO = Número de horas disponibles NHOC = Número de horas del mes que debería estar disponible % = (NHO/NHOC)*100</p>	99.6%	MES	<p>5% DEL VALOR MENSUAL CORRESPONDIENTE AL SERVICIO DE MONITOREO. SI SE SOBRE PASAN TRES DIAS, SE DESCONTARA EL 100% DEL VALOR DE ESTE SERVICIO ASOCIADO DE LA FACTURA MENSUAL.</p>												
Disponibilidad de la herramienta de tickets	Herramienta(s) de apertura de tickets o casos de problemas de red	<p>La disponibilidad de la herramienta se calcula bajo la siguiente formula:</p> $\%DHG = \frac{NHDM}{ND} * 100$ <p>Donde las distintas variables representan: o DHG= Disponibilidad Herramienta de Gestión o ND= Número de horas que debería estar Mensualmente disponible el sistema o NHDM= Número de horas disponibles en el mes o Frecuencia de Medición: Mensual</p>	Se alcanza el nivel de servicio en un porcentaje mayor o igual al 99.8%	MES	<p>Los descuentos asociados a esta Medición por indisponibilidad de servicio por son:</p> <table><tr><th>Valor del Descuento(%)</th><th>% Disponibilidad (D)</th></tr><tr><td>0%</td><td>100 &gt;= X &gt;= 99.8 *</td></tr><tr><td>5%</td><td>99.8 &gt; X &gt;= 95.0 *</td></tr><tr><td>10%</td><td>95.0 &gt; X &gt;= 90.0</td></tr><tr><td>15%</td><td>90.0 &gt; X &gt;= 80.0</td></tr><tr><td>100%</td><td>X &lt; 80</td></tr></table> <p>De acuerdo con esta tabla, ICETEX descontara de la factura mensual un porcentaje (Valor) del valor correspondiente a éste servicio</p>	Valor del Descuento(%)	% Disponibilidad (D)	0%	100 >= X >= 99.8 *	5%	99.8 > X >= 95.0 *	10%	95.0 > X >= 90.0	15%	90.0 > X >= 80.0	100%	X < 80
Valor del Descuento(%)	% Disponibilidad (D)																
0%	100 >= X >= 99.8 *																
5%	99.8 > X >= 95.0 *																
10%	95.0 > X >= 90.0																
15%	90.0 > X >= 80.0																
100%	X < 80																
Cumplimiento de tiempo de traslados	Traslado de último kilómetro en menos de 30 días hábiles dentro de la misma ciudad y sin costos adicionales, en caso de ser necesario.	Días Efectivos de Traslado empleados por el CONTRATISTA, después de la solicitud formal (notificación del interventor) realizada por ICETEX.	30	DIAS	<p>5% DEL VALOR MENSUAL DEL CANAL OBJETIVO DEL TRASLADO POR CADA DIA DE RETRASO EN EL MISMO</p>												
Disponibilidad de la herramienta de Gestión de Red.	Herramientas de gestión de red. Se requiere gestión de infraestructura convergente que ofrezca posibilidades de análisis de rendimiento sobre aplicaciones web del portal <a href="http://www.icetex.gov.co">www.icetex.gov.co</a> y aplicaciones cliente servidor propias adaptadas a requerimientos propios de ICETEX y sobre la que se puede tomar acciones preventivas y/o correctivas. Permitir que los administradores de sistemas realicen monitoreo del tiempo de respuesta de la aplicación de principio a fin para posteriormente,	Día de indisponibilidad	0	MES	<p>5% DEL VALOR DEL SERVICIO MENSUAL POR CADA DIA DE INDISPONIBILIDAD DE LA HERRAMIENTA. SI SE SOBRE PASAN TRES DIAS, SE DESCONTARA EL 100% DEL VALOR DE ESTE SERVICIO (GESTION RED) DE LA FACTURA MENSUAL.</p>												

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

	analizar el rendimiento de la aplicación en toda la infraestructura de la red.																
Disponibilidad de la herramienta de Gestión de Ancho de Banda.	Servicios de Gestión de ancho de banda (DoS)	Día de indisponibilidad	0	MES	5% DEL VALOR DEL SERVICIO MENSUAL POR CADA DIA DE INDISPONIBILIDAD DE LA HERRAMIENTA. SI SE SOBRE PASAN TRES DIAS, SE DESCONTARA EL 100% DEL VALOR DE ESTE SERVICIO (GESTION ANCHO BANDA) DE LA FACTURA MENSUAL.												
Atención Oportuna de Requerimientos de Integración	Servicios de integración con aliados estratégicos o similares requeridos por el ICETEX, por ejemplo, configuración y puesta en producción del enlace dedicado de 1024 Kbps, entre ICETEX Dirección General y Call Center Externo de Atención al Ciudadano.	Días Efectivos de atención después de la solicitud formal (correo del interventor) realizada por ICETEX empleados por el CONTRATISTA.	3	DIAS HABILES	5% DEL VALOR MENSUAL DEL SERVICIO OBJETO DE LA SOLICITUD POR CADA 1 DIA DE DEMORA EN LA ATENCIÓN SOLICITADA.												
Atención Oportuna de Requerimientos de Seguridad FireWall.	Gestión de FireWall Físico o virtual dedicado al servicio de salida del portal web www.icetex.gov.co en Centro de Cómputo Principal y demás cambios de seguridad gestionada solicitados por ICETEX.	Días Efectivos de atención de cambios después de la solicitud formal (correo del interventor) realizada por ICETEX empleados por el CONTRATISTA.	3	DIAS	5% DEL VALOR MENSUAL DEL SERVICIO OBJETO DE LA SOLICITUD POR CADA 1 DIA DE DEMORA EN LA ATENCIÓN SOLICITADA.												
Atención Oportuna de Requerimientos de Seguridad WAF.	Gestión de FireWall de Aplicación Web (WAF) dedicado al portal www.icetex.gov.co de acuerdo con los requerimientos propios del portal de ICETEX.	Días Efectivos de atención de cambios después de la solicitud formal (correo del interventor) realizada por ICETEX empleados por el CONTRATISTA.	3	DIAS	5% DEL VALOR MENSUAL DEL SERVICIO OBJETO DE LA SOLICITUD POR CADA 1 DIA DE DEMORA EN LA ATENCIÓN SOLICITADA.												
Atención Oportuna de Requerimientos de Seguridad Parches, Hardening y relacionados.	Instalación, actualización de parches de seguridad y hardening sobre todos los servidores dados en colocación y ofrecidos en hosting por el CONTRATISTA.	Días Efectivos de atención de cambios después de la solicitud formal (correo del interventor) realizada por ICETEX empleados por el CONTRATISTA.	3	DIAS	5% DEL VALOR MENSUAL DEL SERVICIO OBJETO DE LA SOLICITUD POR CADA 1 DIA DE DEMORA EN LA ATENCIÓN SOLICITADA.												
Atención Oportuna de Requerimientos de corrección de fallas por rendimiento de los servidores.	El CONTRATISTA debe ofrecer Herramientas proactivas de monitoreo de servidores de aplicaciones y bases de datos incluidos en la solución. En casos de que ICETEX detecte fallas en esta infraestructura, solicitará al CONTRATISTA la solución inmediata del evento.	Días Efectivos de atención de cambios después de la solicitud formal (correo del interventor) realizada por ICETEX empleados por el CONTRATISTA.	3	DIAS	5% DEL VALOR MENSUAL DEL SERVICIO OBJETO DE LA SOLICITUD POR CADA 1 DIA DE DEMORA EN LA ATENCIÓN SOLICITADA.												
HOSTING (incluye portal www.icetex.gov.co)																	
Disponibilidad Servidores Ofrecidos en Hosting en Centro de Cómputo Principal	Todos los recursos físicos (conexiones eléctricas y red de datos, memoria, disco, etc.), lógicos (Sistema Operativo, IIS, etc.), y de seguridad responsabilidad del CONTRATISTA deben estar disponibles por lo menos 99.8% del tiempo para la correcta operación de los servidores ofrecidos en calidad de hosting.	NHD = Número de horas disponibles NHOC = Número de horas del mes que debería estar disponible % = (NHD/NHOC)*100  Horas Disponibles / Horas que debería estar disponible.	99.8%	MES	Los descuentos asociados a esta Medición por indisponibilidad de servicio por cada servidor que se caiga de operación, son: <table><tr><th>Valor del Descuento(%)</th><th>% Disponibilidad (D)</th></tr><tr><td>0%</td><td>100 &gt;= X &gt;= 99.8 *</td></tr><tr><td>5%</td><td>99.8 &gt; X &gt;= 95.0 *</td></tr><tr><td>10%</td><td>95.0 &gt; X &gt;= 90.0</td></tr><tr><td>15%</td><td>90.0 &gt; X &gt;= 80.0</td></tr><tr><td>100%</td><td>X &lt; 80</td></tr></table> De acuerdo con esta tabla, ICETEX descontará de la factura mensual	Valor del Descuento(%)	% Disponibilidad (D)	0%	100 >= X >= 99.8 *	5%	99.8 > X >= 95.0 *	10%	95.0 > X >= 90.0	15%	90.0 > X >= 80.0	100%	X < 80
Valor del Descuento(%)	% Disponibilidad (D)																
0%	100 >= X >= 99.8 *																
5%	99.8 > X >= 95.0 *																
10%	95.0 > X >= 90.0																
15%	90.0 > X >= 80.0																
100%	X < 80																

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

					un porcentaje (Valor) del valor del(os) servicio por el servidor(es) afectado(s).												
Atención Oportuna de Requerimientos de Seguridad FireWall.	Gestión de FireWall Físico o virtual dedicado al servicio de salida del portal web <a href="http://www.icetex.gov.co">www.icetex.gov.co</a> en Centro de Cómputo Principal y demás cambios de seguridad gestionada solicitados por ICETEX.	Días Efectivos de atención de solicitud de cambios después de la solicitud formal (correo del interventor) realizada por ICETEX empleados por el CONTRATISTA.	0	DÍAS	5% DEL VALOR MENSUAL DEL SERVICIO OBJETO DE LA SOLICITUD POR CADA 1 DÍA DE DEMORA EN LA ATENCIÓN SOLICITADA.												
Atención Oportuna de Requerimientos de Seguridad WAF.	Gestión de FireWall de Aplicación Web (WAF) dedicado al portal <a href="http://www.icetex.gov.co">www.icetex.gov.co</a> de acuerdo con los requerimientos propios del portal de ICETEX.	Días Efectivos de Implementación de cambios después de la solicitud formal (correo del interventor) realizada por ICETEX empleados por el CONTRATISTA.	0	DÍAS	5% DEL VALOR MENSUAL DEL SERVICIO OBJETO DE LA SOLICITUD POR CADA 1 DÍA DE DEMORA EN LA ATENCIÓN SOLICITADA.												
Atención Oportuna de Requerimientos de Seguridad Parches, Hardening y relacionados.	Instalación, actualización de parches de seguridad y hardening sobre todos los servidores dados en colocación y ofrecidos en hosting por el CONTRATISTA.	Días Efectivos de Implementación de cambios después de la solicitud formal (correo del interventor) realizada por ICETEX empleados por el CONTRATISTA.	0	DÍAS	5% DEL VALOR MENSUAL DEL SERVICIO OBJETO DE LA SOLICITUD POR CADA 1 DÍA DE DEMORA EN LA ATENCIÓN SOLICITADA.												
Atención Oportuna de Requerimientos de corrección de fallas por rendimiento de los servidores.	El CONTRATISTA debe ofrecer Herramientas proactivas de monitoreo de servidores de aplicaciones y bases de datos incluidos en la solución. En casos de que ICETEX detecte fallas en esta infraestructura, solicitará al CONTRATISTA la solución inmediata del evento.	Días Efectivos de Implementación de cambios después de la solicitud formal (correo del interventor) realizada por ICETEX empleados por el CONTRATISTA.	0	DÍAS	5% DEL VALOR MENSUAL DEL SERVICIO OBJETO DE LA SOLICITUD POR CADA 1 DÍA DE DEMORA EN LA ATENCIÓN SOLICITADA.												
COLOCACION CENTRO DE CÓMPUTO PRINCIPAL																	
Disponibilidad Servicios Portal <a href="http://www.icetex.gov.co">www.icetex.gov.co</a>	Todos los recursos físicos (conexiones eléctricas y red de datos, memoria, disco, etc.), lógicos (Sistema Operativo, IIS, etc.), y de seguridad responsabilidad del CONTRATISTA descritas en el ANEXO 5. "REQUERIMIENTOS DE INFRAESTRUCTURA COMO SERVICIO PARA EL PORTAL <a href="http://WWW.ICETEX.GOV.CO">WWW.ICETEX.GOV.CO</a> " deben estar disponibles por lo menos 99.8% del tiempo para la correcta operación de los servidores que soporten el portal.	NHO = Número de horas disponibles NHOC = Número de horas del mes que debería estar disponible % = (NHO/NHOC)*100	99.8%	MES	<div>Los descuentos asociados a esta Medición por indisponibilidad de servicio por cada servidor que se caiga de operación, son:</div> <table><tr><th>Valor del Descuento(%)</th><th>% Disponibilidad (D)</th></tr><tr><td>0%</td><td>100 &gt;= X &gt;= 99.8 *</td></tr><tr><td>5%</td><td>99.8 &gt; X &gt;= 95.0 *</td></tr><tr><td>10%</td><td>95.0 &gt; X &gt;= 90.0</td></tr><tr><td>15%</td><td>90.0 &gt; X &gt;= 80.0</td></tr><tr><td>100%</td><td>X &lt; 80</td></tr></table> <div>De acuerdo con esta tabla, ICETEX descontará de la factura mensual un porcentaje (Valor) del valor del(os) canal(es) afectado(s).</div>	Valor del Descuento(%)	% Disponibilidad (D)	0%	100 >= X >= 99.8 *	5%	99.8 > X >= 95.0 *	10%	95.0 > X >= 90.0	15%	90.0 > X >= 80.0	100%	X < 80
Valor del Descuento(%)	% Disponibilidad (D)																
0%	100 >= X >= 99.8 *																
5%	99.8 > X >= 95.0 *																
10%	95.0 > X >= 90.0																
15%	90.0 > X >= 80.0																
100%	X < 80																
Disponibilidad Servicios Centro de Cómputo Principal Modalidad de Colocación	Todos los recursos físicos (conexiones eléctricas y red de datos), lógicos, de seguridad responsabilidad del CONTRATISTA descritas en los ANEXO 6. REQUERIMIENTOS DE SERVICIOS DE COLOCACION CENTRO DE CÓMPUTO PRINCIPAL para la correcta operación de cada uno de los servidores puestos en colocación.	NHO = Número de horas disponibles NHOC = Número de horas del mes que debería estar disponible % = (NHO/NHOC)*100  Horas Disponibles / Horas	99.8%	MES	<div>Los descuentos asociados a esta Medición por indisponibilidad de servicio por cada servidor que se caiga de operación, son:</div> <table><tr><th>Valor del Descuento(%)</th><th>% Disponibilidad (D)</th></tr><tr><td>0%</td><td>100 &gt;= X &gt;= 99.8 *</td></tr><tr><td>5%</td><td>99.8 &gt; X &gt;= 95.0 *</td></tr><tr><td>10%</td><td>95.0 &gt; X &gt;= 90.0</td></tr><tr><td>15%</td><td>90.0 &gt; X &gt;= 80.0</td></tr><tr><td>100%</td><td>X &lt; 80</td></tr></table>	Valor del Descuento(%)	% Disponibilidad (D)	0%	100 >= X >= 99.8 *	5%	99.8 > X >= 95.0 *	10%	95.0 > X >= 90.0	15%	90.0 > X >= 80.0	100%	X < 80
Valor del Descuento(%)	% Disponibilidad (D)																
0%	100 >= X >= 99.8 *																
5%	99.8 > X >= 95.0 *																
10%	95.0 > X >= 90.0																
15%	90.0 > X >= 80.0																
100%	X < 80																

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

		que debería estar disponible.			<table><tr><td>0%</td><td>100 &gt;= X &gt;= 99.8 *</td></tr><tr><td>5%</td><td>99.8 &gt; X &gt;= 95.0 *</td></tr><tr><td>10%</td><td>95.0 &gt; X &gt;= 90.0</td></tr><tr><td>15%</td><td>90.0 &gt; X &gt;= 80.0</td></tr><tr><td>100%</td><td>X &lt; 80</td></tr></table> <p>De acuerdo con esta tabla, ICETEX descontara de la factura mensual un porcentaje (Valor) del valor del(os) canal(es) afectado(s).</p>	0%	100 >= X >= 99.8 *	5%	99.8 > X >= 95.0 *	10%	95.0 > X >= 90.0	15%	90.0 > X >= 80.0	100%	X < 80		
0%	100 >= X >= 99.8 *																
5%	99.8 > X >= 95.0 *																
10%	95.0 > X >= 90.0																
15%	90.0 > X >= 80.0																
100%	X < 80																
Cantidad de pruebas exitosas de copia y restauración.	Gestión de Backups, Pruebas y Restauraciones de acuerdo con las políticas de backups propias de ICETEX.	NCNR/NCR Donde, NCNR = Número Copias/Restauraciones No Realizadas; NCR = Número Copias /Restauraciones Solicitadas, según políticas definidas con ICETEX.	0	MES	5% DEL VALOR DEL SERVICIO MENSUAL ASOCIADO POR CADA INTENTO FALLIDO PARA USAR EL SERVICIO.												
Cantidad de copia enviadas a Custodia Externa	Custodia externa de acuerdo con las políticas propias de ICETEX.	Número Copias NO enviadas a custodia.	0	MES	5% DEL VALOR DEL SERVICIO MENSUAL ASOCIADO POR CADA SOLICITUD DE ENVIO NO REALIZADA, SEGÚN POLÍTICAS ESTABLECIDAS CON ICETEX.												
Cantidad de Solicitudes Gestionadas de Ingreso a Centro de Cómputo.	De acuerdo con los requerimientos de la operación propia de ICETEX, se solicitará ingreso al Centro de Cómputo para personal por parte del Instituto.	Número Ingresos NO gestionados dentro de los tiempos acordados.	0	MES	5% DEL VALOR MENSUAL DEL SERVICIO OBJETO DE LA SOLICITUD POR CADA 1 DIA DE DEMORA EN LA ATENCIÓN SOLICITADA.												
COLOCACION CENTRO DE CÓMPUTO DE CONTINGENCIA																	
Disponibilidad Servicios Centro de Cómputo De Contingencia Modalidad de Colocación	Todos los recursos físicos (conexiones eléctricas y red de datos), lógicos, de seguridad responsabilidad del CONTRATISTA descritas en los ANEXO 7. REQUERIMIENTOS DE SERVICIOS DE COLOCACION CENTRO DE CÓMPUTO DE CONTINGENCIA para la correcta operación de cada uno de los servidores puestos en colocación.	HD = Horas Disponibles HTD = Horas que debería estar disponible % = (HD/HTD)*100	99.8%	MES	<p>Los descuentos asociados a esta Medición por indisponibilidad de servicio por cada servidor físico que se caiga de operación, son:</p> <table><tr><td>Valor del Descuento(%)</td><td>% Disponibilidad (D)</td></tr><tr><td>0%</td><td>100 &gt;= X &gt;= 99.8 *</td></tr><tr><td>5%</td><td>99.8 &gt; X &gt;= 95.0 *</td></tr><tr><td>10%</td><td>95.0 &gt; X &gt;= 90.0</td></tr><tr><td>15%</td><td>90.0 &gt; X &gt;= 80.0</td></tr><tr><td>100%</td><td>X &lt; 80</td></tr></table> <p>De acuerdo con esta tabla, ICETEX descontara de la factura mensual un porcentaje (Valor) del valor del(os) canal(es) afectado(s).</p>	Valor del Descuento(%)	% Disponibilidad (D)	0%	100 >= X >= 99.8 *	5%	99.8 > X >= 95.0 *	10%	95.0 > X >= 90.0	15%	90.0 > X >= 80.0	100%	X < 80
Valor del Descuento(%)	% Disponibilidad (D)																
0%	100 >= X >= 99.8 *																
5%	99.8 > X >= 95.0 *																
10%	95.0 > X >= 90.0																
15%	90.0 > X >= 80.0																
100%	X < 80																
Cantidad de pruebas exitosas de copia y restauración.	Gestión de Backups, Pruebas y Restauraciones de acuerdo con las políticas de backups propias de ICETEX.	Número Copias o Restauraciones NO realizadas.	0	MES	5% DEL VALOR DEL SERVICIO MENSUAL ASOCIADO POR CADA INTENTO FALLIDO PARA USAR EL SERVICIO												
Cantidad de copia enviadas a Custodia Externa	Custodia externa de acuerdo con las políticas propias de ICETEX.	Número Copias NO enviadas a custodia.	0	MES	5% DEL VALOR DEL SERVICIO MENSUAL ASOCIADO POR CADA SOLICITUD DE ENVIO NO REALIZADA, SEGÚN POLÍTICAS ESTABLECIDAS CON ICETEX.												



## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

Cantidad de Solicitudes Gestionadas de Ingreso a Centro de Cómputo.	De acuerdo con los requerimientos de la operación propia de ICETEX, se solicitará ingreso al Centro de Cómputo para personal por parte del Instituto.	Número Ingresos NO gestionados dentro de los tiempos acordados.	0	MES	5% DEL VALOR MENSUAL DEL SERVICIO OBJETO DE LA SOLICITUD POR CADA 1 DIA DE DEMORA EN LA ATENCIÓN SOLICITADA.
<b>PROFESIONALES</b>					
Disponibilidad del servicio de DBA	DBA CERTIFICADO ORACLE 11G TIEMPO COMPLETO EN SITIO. El horario normal es de 8:00 a.m. a 5:30 p.m. con una hora de almuerzo en el edificio Dirección General Cra 3ª. No.18-32 de lunes a viernes.	Número de días no disponibles por parte del recurso humano en sitio.	0	MES	3.5 % DEL VALOR DEL SERVICIO de DBA MENSUAL POR CADA DIA DE INDISPONIBILIDAD DE DEL SERVICIO SIN JUSTIFICACIÓN VALIDA. SI SE SOBRE PASAN TRES DIAS, SE DESCONTARA EL VALOR TOTAL DE ESTE SERVICIO DE LA FACTURA MENSUAL.
Disponibilidad del servicio de Web Master.	WEB MASTER EN SITIO HORARIO DE 8:0AM A 5:30PM	Número de días no disponibles por parte del recurso humano en sitio	0	MES	3.5% DEL VALOR DEL SERVICIO DE WEB MASTER MENSUAL POR CADA DIA DE INDISPONIBILIDAD DE DEL SERVICIO SIN JUSTIFICACIÓN VALIDA. SI SE SOBRE PASAN TRES DIAS, SE DESCONTARA EL VALOR TOTAL DE ESTE SERVICIO DE LA FACTURA MENSUAL.
Disponibilidad del Servicio de Gestión de Seguridad.	GESTION SEGURIDAD INFORMACION EN SITIO 8AM A 5:45 PM	Número de días no disponibles por parte del recurso humano en sitio	0	MES	3.5% DEL VALOR DEL SERVICIO GESTION DE SEGURIDAD MENSUAL POR CADA DIA DE INDISPONIBILIDAD DE DEL SERVICIO SIN JUSTIFICACIÓN VALIDA. SI SE SOBRE PASAN TRES DIAS, SE DESCONTARA EL VALOR TOTAL DE ESTE SERVICIO DE LA FACTURA MENSUAL.
Disponibilidad del Servicio de Gestión de Voip y Networking.	GESTION VOIP Y NETWORKING EN SITIO 8AM A 5:45 PM	Número de días no disponibles por parte del recurso humano en sitio	0	MES	3.5% DEL VALOR DEL SERVICIO GESTION DE Voip Y NETWORKING MENSUAL POR CADA DIA DE INDISPONIBILIDAD DE DEL SERVICIO SIN JUSTIFICACIÓN VALIDA. SI SE SOBRE PASAN TRES DIAS, SE DESCONTARA EL VALOR TOTAL DE ESTE SERVICIO DE LA FACTURA MENSUAL.
<b>SERVICIOS DE DRP</b>					
Pruebas periódicas RPO/RTD	Los Sistemas Operativos y demás servicios descritos en ANEXO 15. CONTINGENCIA TECNOLÓGICA EQUERIDA DRP (BIA ICETEX TIEMPOS RPD) deben entrar en operación cuando sea requerido por la operación de ICETEX para lo cual mínimo se realiza una prueba de entrada en contingencia según tiempos descritos en anexo 15..	Número de Pruebas Fallidas.	0	mensual	Se aplicará un descuento de 5% del valor mensual del servicio asociado por cada prueba fallida.
Documentación de Planes y Ejecución de Pruebas de DRP.	Todos los Planes de Ejecución periódica de pruebas sobre la plataforma de contingencia deben estar documentadas.	Número Pruebas No Documentadas.	0	MES	Se aplicará un descuento de 5% del valor mensual del servicio asociado por cada prueba no documentada
<p><b>Nota:</b></p> <p>En General, ningún servicio podrá ser facturado si no es recibido a completa satisfacción por parte del interventor del contrato. Las penalizaciones por servicios no prestados adecuadamente se realizan sobre las tarifas ofertadas por cada servicio, en cumplimiento del acuerdo de disponibilidad definido y no por promedios del cumplimiento de todos los ANS pactados.</p>					

SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

ANEXO 19.

REQUERIMIENTOS MINIMOS DEL CENTRO DE CÓMPUTO  
PRINCIPAL Y DE CONTINGENCIA  
Generalidades.

El CONTRATISTA debe suministrar y administrar una herramienta de monitoreo que permita identificar la disponibilidad, desempeño, alertas **a toda la plataforma teleinformática relacionada con servicios propios de ICETEX (Servidores de Aplicaciones, Servidores de Bases de Datos, Appliance de Seguridad, Switches, Routers, entre otros)**. Adicionalmente debe contar con un software de acceso remoto seguro que contenga autenticación y encriptación del canal de comunicación, SSL.

Backup

El contratista debe contar con una herramienta WEB para el registro de casos y apertura de tickets de tal manera que se garantice el cumplimiento de los ANS pactados (CENTRO DE CÓMPUTO Principal y De Contingencia, como los servicios de canales dedicados descritos en los anexos 3, 6 y 7). Así mismo se deben garantizar los canales de comunicación a través de la mesa de servicio.

El CONTRATISTA debe realizar las copias de seguridad de todas las aplicaciones e información puesta en el CENTRO DE CÓMPUTO. Para tal efecto, el CONTRATISTA debe utilizar herramientas de backup las cuales deben ser compatibles con el sistema con el que cuenta actualmente ICETEX (Librería LOT5 - TIVOLI). El CONTRATISTA debe configurar esta herramienta y administrar de acuerdo con las políticas de copia propias de ICETEX, las cuales son presentadas en el ANEXO 9. "POLITICA DE BACKUP – RESTAURACIONES ICETEX" del presente Pliego de Condiciones. Igualmente, será responsabilidad del CONTRATISTA operar y gestionar garantías de la herramienta de backup e igualmente mantener actualizado el licenciamiento correspondiente.

El sistema de copias de respaldo suministrado por El CONTRATISTA debe cumplir mínimo con los siguientes requisitos:

- a) Implementar, actualizar y ejecutar las políticas de backup y recuperación para servidores en los diferentes ambientes (desarrollo, pruebas, capacitación y producción) y mantener actualizada mensualmente esta información de acuerdo con las políticas internas definidas por el ICETEX.
- b) El contratista debe ejecutar el Backup con agentes de respaldo para SQL, Oracle, Open files y buzones de correo.
- c) Suministrar las cintas necesarias para realizar las copias de respaldo a los servidores, así como las cintas de respaldo y demás elementos

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

requeridos para el mantenimiento del sistema de backups, las cuales deberán ser proporcionadas desde el inicio del contrato de Outsourcing.

- d) Hacer gestión de backup sobre todos los servicios del ICETEX.
- e) Mantener actualizada la información de copias de respaldo, así como la gestión de custodia de las bases de datos del ICETEX.
- f) Ejecutar procedimientos de custodia y recepción/entrega de medios por demanda del software operacional, aplicativos y las copias de respaldo y contingencia de la información.
- g) Mantener copias de seguridad actuales en la Institución para tener acceso inmediato a la información, estas copias deben ser almacenadas en un repositorio SAN o NAS del ICETEX, bajo administración adecuada de accesos.
- h) Las cintas magnéticas que contengan información son propiedad del ICETEX.
- i) Proveer y administrar el suministro de medios magnéticos para la ejecución de las copias de respaldo para servidores y así mismo la custodia de medios de acuerdo a las políticas del ICETEX y a los resultados del BIA.
- j) Proponer mejoras a las políticas de respaldo de información del ICETEX existentes.
- k) Efectuar la marcación de medios magnéticos de acuerdo con la nomenclatura y/o estándar del ICETEX.
- l) Mantener en un archivo en hoja electrónica o base de datos, por cada cinta, la siguiente información básica:
  - Label, marca o número de cinta, Tipo de copia: Full, Incremental, otro.
  - Periodicidad: Mensual, diaria, anual, otro.
  - Contenido: Correo electrónico, Bases de Datos Contabilidad, Bases de Datos Crédito y Cartera, Otros.

### Energía

Al presentarse una interrupción en la fuente de alimentación principal, el sistema UPS del CONTRATISTA, configurado en línea, debe cubrir inmediatamente las necesidades energéticas de todos los equipos que conformen la solución de ICETEX. Del mismo modo, en caso de daños extremos de energía, se debe garantizar como mínimo de 30 minutos de autonomía a fin de tener un tiempo de apagado normal de todos los equipos que conforman la solución.

Las instalaciones del CONTRATISTA deben estar equipadas con generadores industriales (tipo diésel o similares), con capacidad para soportar toda nuestra infraestructura incluida en los CENTRO DE CÓMPUTO, en el evento de presentarse una interrupción prolongada de Energía.

**SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015****Control Climático**

La Temperatura y humedad deben ser constantemente monitoreadas y vigiladas por sistemas de precisión de control de clima localizado en los Centro de Cómputo Principal y De Contingencia para el funcionamiento óptimo de los equipos y su protección.

- Unidades de aire acondicionado de precisión dedicada a los equipos de cómputo de ICETEX.
- Detectores de humedad distribuidos en las salas de servidores.

En general, el CONTRATISTA debe garantizar las condiciones de calor y humedad para todos los servidores propiedad de ICETEX y puestos en calidad de COLOCACION y HOSTING. En caso de que se presentaren indisponibilidades o daños sobre estos equipos, las reparaciones de los equipos deben ser completa responsabilidad del CONTRATISTA, así como los descuentos por indisponibilidades (ANS 99,8%) de los servicios que puedan estar relacionados.

**Puerta delantera:** Con área ventilada que facilite la eficiente ventilación de los equipos. Con sistema de puesta a tierra.

**Puerta trasera:** De fácil apertura, con chapa y llave. Con sistema de puesta a tierra.

**Prevención de Incendios**

EL CONTRATISTA debe utilizar sistemas de detección de humo, dispositivos de la detección del calor, como también sistemas de la supresión de incendios. Los Centro de Cómputo deben ser entregados con capacidad de aislamiento, detección de fuego, centralización y control de incendios sin causar daño al resto de las instalaciones. Así mismo, se debe contar por lo menos con un Sistema de aviso visual y sonoro en caso de incendios, sistemas de descarga automática con sistema de aborto manual y Monitoreo de alarmas 7 x 24 x 365.

**Diseño de Rack y cableado estructurado**

Cada rack debe estar claramente pre-alambrado y conectado bajo el sistema del cableado, suspendido sobre bandejas o escalerillas debidamente marcadas para identificar cada servicio y rack asignado a ICETEX. Además, se alimenta cada estante usando switches de alimentación independientes para asegurar redundancia de la energía. Para cada uno de los equipos que forman parte de la solución, se debe conectar a dos circuitos eléctricos diferentes que van a dos

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

UPS diferentes a fin de entregar redundancia eléctrica a los equipos que conforman la solución.

### NORMAS

Los Centro de Cómputo Principal y De Contingencia deben Cumplir por lo menos con las normas: EIA-TIA 310D; NEMA 250-1; NTC: ISO 9001:2000.

Todos los cables y tomas presentes en los Centro de Cómputo Principal y De Contingencia ofrecidos, deben cumplir con las siguientes normas:

- ✓ EIA/TIA-568B.1 Standard Commercial Building Telecommunications Wiring Standard.
- ✓ EIA/TIA-568B.2 100-ohm twisted-pair cabling standar.
- ✓ EIA/TIA-568B.2-1 Category 6.
- ✓ EIA/TIA-568B.3 Optical fiber cabling Standard.
- ✓ EIA/TIA-569A Commercial Building Standard for Telecommunications pathways and spaces.
- ✓ EIA/TIA 606 The Administration Standard for the Telecommunications Infrastructure of Commercial Buildings.
- ✓ EIA/TIA 607 Commercial Building and Bonding Requirements for Telecommunications última edición.
- ✓ ISO/IEC 11801 The international Organization for Standardization the International Electrotechnical Commission. Specifies generic cabling for use within commercial premises. Single or multiple buildings on a campus.

**Altura útil:** 42 unidades de rack.

La solución de firewall para el portal del ICETEX debe ser:

- ✓ De un fabricante posicionado como líder en el cuadrante mágico de gartner que garantice una completa protección al portal [www.icetex.gov.co](http://www.icetex.gov.co), a la LAN alojada en ese CENTRO DE DATOS y que debe estar separada lógicamente del servicio del portal web.
- ✓ Completamente compatible e integrado con las funcionalidades y características técnicas descritas en ANEXO 20. "CARACTERISTICAS TECNICAS FIRE WALL ACTUAL ICETEX" de los FireWall que posee actualmente ICETEX.
- ✓ Costos detallados en el anexo "ANEXO 5. REQUERIMIENTOS DE INFRAESTRUCTURA COMO SERVICIO PARA EL PORTAL WWW.ICETEX.GOV.CO" y excluidos de este ítem aunque el servicio como tal quede descrito en el presente numeral.

Diseñar, documentar y aplicar sobre el Firewall, las políticas de seguridad asociadas a la infraestructura tecnológica que se encuentran dentro del alcance y debe realizar como

**SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015**

mínimo las siguientes actividades:

- ✓ Suministrar y realizar la administración, mantenimiento y actualización de las políticas de seguridad en los firewalls de la red en coordinación y con autorización de la Dirección de Tecnología del ICETEX.
- ✓ Realizar administración, mantenimiento y actualizaciones a los equipos Hardware que soportan la operación de los firewalls.
- ✓ Debe configurar para ofrecer servicio de salida del portal web [www.icetex.gov.co](http://www.icetex.gov.co) en Centro de Cómputo De Contingencia.

**ANEXO 20.****CARACTERISTICAS TECNICAS FIRE WALL ACTUAL ICETEX  
ICETEX CENTRO DE CÓMPUTO**

- Un 1 cluster de firewall Check Point.
- La solución está compuesta por componentes de hardware y software necesarios para su completo funcionamiento, sin necesidad de instalar hardware y/o hardware en algún equipo de otra marca que no forme parte de la solución
- La solución está integrada a la red en modo Bridge (capa 2 del modelo OSI, las interfaces no requieren de una dirección)
- Los gateways y su administración permiten adicionar nuevas funcionalidades a través de plug-ins o blades, sin necesidad de realizar un upgrade completo del software o hardware
- La solución está avalada en el último reporte de Gartner Group, para firewalls Enterprise en el cuadrante de líderes.
- Entre las características actuales se encuentran:
  - Firewall con un throughput de 4.8 Gbps con :
    - ✓ Manejo de protocolos y aplicaciones seguras
    - ✓ Soporte para encriptación AES 128-256 bit, 3DES 56-168 bit
    - ✓ Métodos de autenticación Password, RADIUS, TACACS, X.509, scurrid, LDAP.
    - ✓ Autoridad de certificación
    - ✓ Soporte de agente VPN, IPSec, SSL
    - ✓ Con capa de protección de red
    - ✓ Con capa de protección de aplicaciones
    - ✓ Soporta mínimo 1.200.000 sesiones concurrentes
    - ✓ Manejo de Networking Avanzado
    - ✓ Manejo de redundancia ISP
    - ✓ Soporte en enrutamiento de vanguardia

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

- ✓ Calidad de servicio
- ✓ Manejo de aceleración y agrupamiento de datos
- ✓ Manejo de alta disponibilidad
- ✓ CoreXL
- ✓ SecureXL
- ✓ Alta Disponibilidad y balanceo de carga de gateways con sincronización de estados, incluyendo la licencia para Alta Disponibilidad.
- ✓ Características de firewall de Acceleration and Clustering
- ✓ Sincronización de estado para cluster
- ✓ Sincronización de miembros para cluster
- ✓ Notificaciones de dispositivos
- ✓ Agregación de links
- ✓ 12 puertos 10/100/1000 y un almacenamiento mayor o igual a 250 Gb. Memoria mínimo de 4GB con opción de crecimiento a mínimo 8GB y fuente de poder redundante
- ✓ Encriptación de toda la información confidencial para el ICETEX, enviada vía Internet desde y hacia terceros mediante comunicaciones seguras: VPNs
- ✓ Soporte a VPNs site-to-site y Client-to-site

### ANEXO 21

#### CARACTERISTICAS TECNICAS MINIMAS REQUERIDAS DEL SERVICIO WEB APPLICATION FIREWALL – WAF

Web Application Security es un conjunto de medidas destinadas a proteger las aplicaciones web y datos frente a ataques a las aplicaciones como SQL Injection (SQLi), Cross Site Scripting (XSS), Secuestro de sesión, y Cross Site Request Forgery (CSRF) entre otros, los cuales se utilizan para extraer información confidencial, como datos de tarjetas de crédito o detalles de los clientes o incluso producir indisponibilidad del servicio a través de servidores web públicos.

La solución propuesta debe ser de propósito específico y desarrollado para la función de Web Application Firewall de uso específico para este fin

La solución debe poder ser administrada vía interfaz gráfica (GUI) e interfaz de línea de comandos (CLI)

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

La solución debe ser capaz de:

Trabajar en modo Pasivo Snnifer, en modo En Línea (tipo bridge), en modo de Proxy reverso y en modo Proxy transparente

Los usuarios deberán poder autenticarse de diferentes formas a través del equipo

- Encabezado de autorización del protocolo HTTP/HTTPS, si la aplicación web no soporta autenticación HTTP del RFC 2617 entonces La solución propuesta deberá proveer esta función.
- Formas embebidas de HTML
- Certificados digitales personales
- Cuentas de usuario final locales en La solución
- Cuentas de usuarios finales remotas a través de LDAP, RADIUS y NTLM
- El equipo deberá ser capaz de generar grupos de usuarios para accesos similares
- La solución podrá aplicar los grupos de usuarios a un dominio de autorización.

### PROTECCIÓN DE SERVIDORES

La solución deberá proteger tanto por dirección IP como por nombre (DNS Domain Name)

La solución podrá verificar la salud de los equipos a través de los siguientes protocolos TCP, HTTP/HTTPS e ICMP

La solución podrá generar granjas de servidores para distribuir las conexiones de los usuarios, los métodos para distribuir estas sesiones deberán ser: Balanceo de Servidores, ruteo basado en contenido WSDL, ruteo basado en contenido HTML, ruteo basado en contenido XML

La solución deberá ser capaz de crear servidores virtuales para que los usuarios puedan tener acceso a los servicios reales y poder configurar mensajes de intercepción y de error

La solución deberá ser capaz de:

Funcionar como terminador de sesiones SSL para aceleración de tráfico

Ejecutar descifrado oculto de SSL usando claves privadas del servidor.

Soportar certificados tanto en modo pasivo como activo

Cifrar en ambos sentidos (Frontend y Backend)

Soportando:

- SSL 2.0
  - DES-EDE3-CBC-MD5 — 192-bit
  - DES-CBC-MD5 — 64-bit
- SSL 3.0
  - AES-SHA — 256-bit & 128-bit
  - DES-CBC3-SHA — 168-bit
- TLS 1.0
  - AES-SHA — 256-bit & 128-bit



## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

- DES-CBC3-SHA — 168-bit
- Triple DES (3DES)
- RSA
- Diffie-Helman
- Digital Signature Algorithm (DSA)
- Secure Hash Algorithm 1 (SHA-1) and Message-Digest 5 (MD5)
- SNMP v2

La solución deberá tener la capacidad de almacenar certificados digitales de CA's, así como la capacidad de poder generar CSR para su posterior envío y firmado por alguna CA.

Si los clientes se van a conectar al sitio web usando HTTPS La solución se deberá poder configurar para solicitar a los clientes que presenten su certificado personal durante el establecimiento de la sesión para confirmar sus identidades, autenticación PKI

La solución deberá ser capaz de validar que los certificados sean válidos y que no hayan sido revocados a través de una lista de revocación de certificados (CRL) o a través de una búsqueda de OCSP. La solución será capaz de respaldar los certificados.

### CONTROL DE ACCESO A LAS APLICACIONES

La solución deberá soportar reglas para definir si las peticiones de HTTP serán aceptadas basándose en el hostname el URL así como el origen de la petición, y si es necesario aplicar una tasa de transferencia específica (rate limiting)

La solución deberá contar con una base de datos actualizable de forma automática para la generación de blacklist y whitelist con la facultad de realizar bloqueos de forma geográfica o de asignar niveles de severidad.

La solución deberá contener firmas de los robots conocidos como link checkers, search engine indexers, spiders y web crawlers que se podrán colocar en los perfiles de control de acceso, así como resetear las conexiones.

La solución deberá contar con un sistema de reputación de direcciones IP públicas para detectar y calificar las direcciones IP que tienen acceso al sistema de tal forma que si una IP ha sido partícipe de un ataque informático no se le permita el acceso a los servidores de aplicaciones, esta calificación se deberá hacer y actualizar de forma automática.

La solución deberá poder limitar el número de HTTP request por segundo por dirección IP, de la misma forma se podrá limitar el número de conexiones TCP por sesión de HTTP además de limitar las peticiones desde una misma dirección ip

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

La solución podrá aceptar firmas personalizadas las cuales podrán ser contra ataques o de prevención de fuga de información (DLP)

La solución podrá reescribir o redireccionar HTTP requests y HTTP responses. Para reescribir el URL podrá seleccionar qué parte de la petición se buscará igualar en base a: HTTP Host, HTTP Request URL, HTTP Referer, HTTP Body, HTTP Location y la expresión regular que se haya definido

La solución también podrá tener la capacidad de definir excepciones a las políticas de seguridad y Validar protocolos y restricción de métodos , Validar encoding URL, Validar el formato no estándar, Validar el tamaño de header, contenido y cuerpo

Validar parámetros adicionales con reglas para ataques desconocidos y Proteger contra la detección de campos ocultos.

### 1 BLOQUEO DE ATAQUES

La solución podrá generar reglas para el orden en que las páginas deben de ser accesadas y al especificar este orden se asegura el correcto funcionamiento de la aplicación web y se previenen ataques como cross-site request forgery (CSRF)

La solución podrá fijar puntos legítimos de entrada a las aplicaciones web para evitar ataques state-based

La solución podrá limitar el protocolo HTTP/HTTPS para prevenir ataques como buffer over flow, estas limitantes incluyen: Host Name ilegal, HTTP Versión ilegal, HTTP Request Method ilegal , HTTP Request Length, Content Length, Body Length, Header Length, Header Line Length, Number of Header Lines In Request, Total URL and Body Parameters Length, Total URL Parameters Length, Number of URL Parameters, Number of Cookies In Request, Number of ranges in Range Header, Malformed Request

La solución deberá contener por lo menos los siguientes ataques:

- Ataques HTTP/HTTPS
  - Adobe Flash binary (AMF) protocol attacks
  - Botnet
  - Browser Exploit Against SSL/TLS (BEAST)
  - Brute force login attack
  - Clickjacking
  - Cookie tampering
  - Credit card theft

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

- Cross-site request forgery (CSRF)
- Cross-site scripting (XSS)
- Denial of service (DoS)
- HTTP header overflow
- Local file inclusion (LFI)
- Malicious robots
- Remote file inclusion (RFI)
- Server information leakage
- SQL injection
- Malformed XML
- HTTP request flood
- Ataques DoS
  - Botnet
  - Low-rate DoS
  - Slow POST attack
  - Slowloris
  - SYN flood
- Ataques SOAP/XML
  - Ataques Dia cero (Zero-Day)
  - Element overflow
  - External entity
  - Inadvertent XML DoS
  - Recursive payload
  - Schema poisoning
  - XML parameter tampering
  - WSDL scanning

La solución podrá limitar la carga de archivos hacia los servidores basándose en el tipo de archivo y en su tamaño, la detección y la restricción se realizará escaneando los encabezados de Content-Type y Content-Lenght

La solución podrá realizar la compresión y descompresión de los archivos para liberar recursos en los servidores web

La solución deberá contar con perfiles de protección que contengan características que actúen cuando se encuentren peticiones de HTTP con contenido XML como RSS o servicios web SOAP. Cada política de protección XML deberá contar con al menos los siguiente parámetros: WSDL Verify, WSDL verify action, Web Service, XML SIG, XML SIG action, XML ENC, XML ENC action, Key Info, XML reverse SIG, XML reverse SIG key, XML reverse SIG XPath, XML reverse ENC, XML reverse ENC Key, XML reverse ENC XPath, SQL Injection Prevention, SQL Injection Prevention Action, Non-XML traffic

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

La solución deberá contar con horarios de protección para eventos de una sola ocasión o para eventos recurrentes.

Los perfiles de protección con las que deberá contar La solución deberán combinar una serie de reglas, perfiles y políticas en un grupo completo que podrá ser aplicado cuando el equipo se encuentre en línea. Cada perfil de protección podrá contener las siguientes funcionalidades de seguridad: Session Timeout, X-Forwarded-For, Cookie Poisoning Detection, Signatures, Enable AMF3 Protocol Detection, Enable XML Protocol Detection, Illegal XML Format, Custom Access, Parameter Validation, Hidden Fields Protection, File Upload Restriction, HTTP Protocol Constraints, Brute Force Login, URL Access, Page Access, Start Pages, Allow Method, Robot Control, IP List, Geo IP, DoS Protection, IP Intelligence, URL Rewriting, HTTP Authentication, File Compress, File Uncompress, Redirect URL, Redirect URL With Reason, Data Analytics

La solución deberá contar con una herramienta contra modificación de páginas web (Anti-Defacement) la cual estará verificando de forma constante el contenido de las páginas y en caso de existir alguna modificación automáticamente regresar el archivo original y/o alertar sobre este evento.

La solución deberá contar con una herramienta de escaneo de vulnerabilidades en los servidores y aplicaciones Web. Estos escaneos se podrán programar por el Administrador. Estos escaneos deberán encontrar las vulnerabilidades comunes de los servidores como software caduco o con fugas conocidas de memoria o posibles buffer Overflows, o vulnerabilidades más avanzadas para detectar al menos XSS, SQL Injection, Source-code Disclosure, OS Commanding, al terminar el escaneo deberá generar un reporte en los siguientes formatos HTML, PDF, MIME HTML, PDF, RTF y TXT y tener la posibilidad de mandarlo por correo electrónico.

La solución deberá ser capaz de ejecutar análisis de vulnerabilidades

Los análisis de vulnerabilidades ejecutados por la solución deben ser de tipo no intrusivo  
Los análisis de vulnerabilidades ejecutados por la solución deben ser en modo autenticado

La solución debe permitir la programación de análisis de vulnerabilidades automáticos

La solución debe permitir la exclusión de URLs dentro del análisis de vulnerabilidades

La solución deberá contener una funcionalidad de auto aprendizaje para que el equipo entienda cómo funciona la estructura Web de las aplicaciones y permita implementar políticas de seguridad con la información recopilada. Este aprendizaje debe de descubrir los URL y otras características de las sesiones de HTTP/HTTPS mediante la observación del tráfico que pasa a través dLa solución

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

Si La solución propuesta fuera un appliance éste deberá contener un sistema de protección fail-to-wire el cual permitirá el paso del tráfico sin filtrar en caso de que el equipo se apague o se encuentre en proceso de encendido.

La solución deberá contener una base de datos actualizable de manera automática sin la intervención del usuario administrador, también tendrá la opción de escoger entre utilizar la base de datos completa o solamente la de los virus más recientes y peligrosos.

La solución deberá contar con una administración web en la cual se cuente con un panel de control con la información relevante como: Información La solución, Versión de la base de datos de Antivirus, Acceso a la línea de comandos de la solución, Recursos Disponibles de la solución, Consola de Bitácora de ataques, Resumen de Políticas de Seguridad, Consola de Bitácora de Eventos, Estado de los Servidores, Sesiones que están usando las políticas.

En el caso de que se oferte una solución con equipo físico este deberá tener un esquema de discos en RAID 1 para redundancia.

Para diagnosticar problemas o rastrear alguna acción La solución deberá almacenar los logs al mismo tiempo que procese el tráfico, estos logs deberán ser de Ataques, tráfico, Eventos, Utilización de CPU y Memoria y se podrá configurar los métodos de almacenamiento hacia el disco duro, a la memoria, a un servidor de Syslog o algún otro equipo para la generación de reportes.

La solución deberá contar con el servicio de envío de correos electrónicos para la notificación de algún ataque, eventos de falla.

La solución deberá soportar el estándar SNMP y contar con un esquema de generación de reportes para mostrar la información obtenida en base al auto-aprendizaje, a las estadísticas y tráfico recolectados por las políticas, reportes de ataques, eventos y reportes de escaneo de vulnerabilidades para fines de cumplimiento de alguna normativa. Estos reportes podrán ser calendarizados.

Adicionalmente a los reportes La solución deberá contar con análisis de los datos (Data analytics) para ayuda en el rastreo del uso de los servidores web

La solución deberá contar con la facilidad de proveer alta disponibilidad en donde dos dispositivos pueden actuar en forma activo-pasivo de forma tal que, si el equipo principal fallara el pasivo podrá continuar procesando el tráfico.

Para la solución de problemas La solución debe de contar con la funcionalidad de captura de paquetes también conocida como Sniffer. Mediante esta funcionalidad se permite la

**SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015**

captura de todo o parte del tráfico que pase a través de una interface en particular, permitiendo rastrear los estados de la conexión para un mejor diagnostico en caso de alguna falla.

**ANEXO 22****REQUERIMIENTOS TECNICOS MINIMOS SISTEMA VIDEO CONFERENCIA****SISTEMA DE VIDEO CONFERENCIA PARA CINCO SEDES DE ICETEX**

Es factible que se ofrezca un sistema virtual o en la nube siempre y cuando se cumpla con la misma calidad y disponibilidad que se tiene con los equipos descritos en el presente anexo.

Las especificaciones técnicas mínimas en cuanto a videoconferencia, son las siguientes:

**SISTEMA CENTRAL MULTIPUNTO****Estándares**

El equipo debe instalarse en el punto central de ICETEX (Bogotá)

- Debe ser completamente compatible con los estándares H.323, H.320 y SIP.
- Debe tener compatibilidad con Estándares ITU: H.221, H.242, H.243, H.224/H.281 FECC (por lo menos para el codec de videoconferencia), H.225 (opcional), H.245, H.239, T.120 (opcional).
- Protocolos de red: TELNET, HTTP, FTP, SNMP (todos los dispositivos deben ser administrables), DNS, DHCP, RTP/RTCP o su equivalente, TCP/UDP o su equivalente, IP, IPv6, ARP.
- Deben Incorporar mecanismos de seguridad (contraseñas de administración, encriptación, etc.)

**Sistema de video**

- Debe incluir Estándares y protocolos de video: H.261, H.263, H.263+, H.263++, H.264 y/o MPEG4.
- La codificación y decodificación será realizada por hardware en dispositivos dedicados.
- Especificaciones de las cámaras: Cámaras a color con funcionalidad PTZ, Rango Pan (+/- 95°), Rango Tilt (+15°/- 20°), Zoom óptico mínimo, autoenfoco, balance automático de brillo y blancos, controlable remotamente.
- Se deben incluir líneas de salida tipo VCR o RCA o una tecnología más actualizada para este tipo de salidas.
- Por lo menos 60 cuadros por segundo.
- La solución del sistema de videoconferencia incluye los formatos de video (NTSC, PAL, VGA, SVGA, XGA W-XGA o SXGA).

**Sistema de audio**

- Debe Cumplir Estándares y protocolos de audio: G.711, G.722, G.722.1, G.728, G.722.1
- La codificación y decodificación será realizada por hardware en dispositivos dedicados.
- Capacidad de audio digital full-duplex a 7 KHz o superior.
- Debe Incorporar mecanismos para cancelación de eco y supresión de ruido.
- Se deben incluir líneas de salida estéreo tipo VCR o RCA o una tecnología más actualizada para

## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

este tipo de salidas.

### Unidad multipunto – MCU

Indicar marca y modelo del equipo, con las siguientes características principales:

- Alta definición sin compromiso. Debe actuar como puente de conferencia multimedia con la facultad de entregar una verdadera alta definición (HD), sin compromiso ni límites, el equipo soporta la más alta resolución de video, en velocidad de transmisión, velocidad en cuadros por segundo y permitiendo al códec proporcionar los últimos criterios de valoración para HD.
- Debe incluir una comunicación plena en presencia continua de todas las conferencias, incluidos los que tienen una mezcla de ambos HD y de definición estándar (SD).
- Debe soportar aplicaciones que exigen para sus comunicaciones de audio y vídeo la mejor calidad, tales como reuniones y capacitación empresarial.

- Alta Capacidad Constante (incluyendo más de 50 layout de presencia continua) en cualquier puerto, sin pérdida de capacidad.

- Rendimiento de Alta Definición Debe proporcionar una imagen clara, a todo movimiento (full-motion), la solución debe proveer Alta definición a todos los puertos. 720p H.264, mínimo a 60 cuadros por segundo en presencia continua con una perfecta calidad y limitado únicamente por la capacidad en la red y del endpoint. Debe soportar Multi- Standart HD de audio y presentaciones en Videoconferencia.

Debe proporcionar una transmisión de video con mínimo 4x de resolución.

- Rendimiento de vídeo de hasta 720p H.263 60fps presencia continua junto con soporte de audio de Alta definición.
- Protección de inversiones
- Estándares Básicos y Compatibles
- Debe permitir interoperabilidad con redes IP y RDSI y demostrar la compatibilidad con todos los principales proveedores.
- Debe soportar Streaming de vídeo y contenido en cualquier navegador WEB, sin ningún software o hardware adicional.

Debe permitir programar, administrar y controlar individualmente las distintas conferencias independientemente de seleccionar el layout de presencia continua para cada usuario, sin necesidad de instalar ningún software adicional.

- Tecnología Paquete Seguro

Se debe asegurar que la pérdida de paquetes en cualquier parte de la red tenga un impacto mínimo sobre la calidad de la conferencia.

Es deseable que dentro de las opciones de Conferencia por Web, se pueda añadir datos, como diapositivas, chat, anotaciones y streaming de video estándar y de voz.

Es deseable tener un segundo puerto Ethernet que permita que llamen desde dentro y fuera de la red para cumplir en el puente, dejando el firewall y sus niveles de seguridad sin cambios.



## SELECCIÓN PÚBLICA DEL CONTRATISTA N°004-2015

### CARACTERÍSTICAS DE LOS EQUIPOS

Es deseable que los equipos estén diseñados con las siguientes características técnicas y funcionales:

- Códec con cámara integrada
- Control remoto inalámbrico
- Micrófono de mesa
- Cables necesarios para su operación
- Manual de usuario en formato electrónico (PDF)

Debe admitir las siguientes visualizaciones del contenido a proyectar.

- Capacidad para establecer conexiones de audio y video (video y audio conferencia) simultáneas mínimo con 9 sitios, incluido el sistema local.
- Soporta los estándares H.320, H.323 y SIP. En su defecto se deben entregar los mecanismos que permitan la integración con estos estándares en caso de requerirse.
- Características de seguridad: Contraseñas de administración IP, contraseña de protección de conferencia, administración vía https, encriptación embebida.
- Capacidad para soportar anchos de banda diferentes para cada sitio de videoconferencia. Es decir, si por ejemplo, 2 usuarios se conectan a 384kbps y uno a 128kbps, la MCU debe permitir la conexión de los 3 con sus respectivos anchos de banda, sin degenerar la calidad de conferencia de los usuarios a 384kbps y permitiendo a la vez que el usuario a 128 kbps permanezca en la videoconferencia (*transrating y/o transcoding*)
- Interfaces: Ethernet 10/100/1000 Mbps.
- Capacidad de crecimiento para manejo de ancho banda.

El proveedor debe garantizar el debido crecimiento y escalabilidad de la red WAN de acuerdo con las necesidades que a futuro pueda requerir el ICETEX.

"Como mínimo los equipos del nivel central de la WAN entregada por el contratista deben soportar IPV6. Esto se refiere a los router de Centro de Datos y de la Dirección General ubicada en el sector de Aguas".

"El contratista debe presentar un Plan de Trabajo en el que se indiquen los recursos humanos y técnicos, así como las fechas de entrega de la implementación parcial y total, teniendo en cuenta que el actual contrato termina el 30 de junio de 2015 y que de ningún modo se pueden efectuar pagos referentes a implementaciones fuera de los considerados en los presentes Términos de Referencia."

**POR EL ICETEX**

**NELSON DARÍO MEJÍA FAJARDO**

Vicepresidente de Operaciones y Tecnología

**EL CONTRATISTA**

**GERMÁN DE JESÚS GARCÍA SALAZAR**

Representante Legal

**LEVEL 3 COLOMBIA S.A**

Revisó Técnicamente:

Ing. Mauricio Gómez Murcia, Director de Tecnología  
Ing. Víctor Bautista, Coordinador de Infraestructura  
Juan Guillermo Muriel Tobón/Abogado Grupo Contratos

Elaboró: