MINEDUCACIÓN

ICETEX

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

MEMORANDO
ICETEX
AL CONTESTAR CITE ESTE NÚMERO 2018006932-I
Remitente: OFICINA DE CONTROL INTERNO
Tipo Doc: MEMORANDO

Fecha: 18/05/2018 16:51:42.0

OCI 2600 – 111
Bogotá, Mayo 18 de 2018

PARA: ING. OSCAR YOVANI BAQUERO MORENO
Vicepresidente de Operaciones y Tecnología

ING. CARLOS ARIEL USEDA GÓMEZ
Director de Tecnología

DE: JEFE OFICINA DE CONTROL INTERNO

ASUNTO: Auditoría de seguimiento a los controles del Mapa de Riesgos de la Dirección de Tecnología

La Oficina de Control Interno, en cumplimiento de sus funciones, llevo a cabo la Auditoría de seguimiento a los controles del Mapa de Riesgos de la Dirección de Tecnología. La Auditoría fue desarrollada cumpliendo los criterios de independencia y objetividad atribuibles a la actividad de Auditoría Interna, con un enfoque de seguridad, concebida para agregar valor y mejora a los procesos de la Entidad.

El presente informe fue socializado con los Ingenieros Oscar Yovani Baquero Moreno y Carlos Ariel Useda Gómez el 7 de mayo de 2018.

Por lo anterior se anexa el informe con el resultado de la auditoria, por lo cual se solicita desarrollar las acciones de mejoramiento y remitirlas a esta Oficina en el formato F263 Plan de Mejoramiento Auditorías sistemas de Gestión, a más tardar el 31 de mayo del presente, sobre las cuales se efectuará seguimiento y control.

Cordialmente,

LUZ ALBA SANCHEZ SANCHEZ

Anexo. Informe en catorce (14) folios
Plan de mejoramiento

FECHA DE EMISIÓN DEL INFORME	***11/04/2018***

PROCESO, PROCEDIMIENTO O ACTIVIDAD A AUDITAR	Auditoría de seguimiento a los controles del Mapa de Riesgos de la Dirección de Tecnología
OBJETIVO DE LA AUDITORIA:	Analizar, verificar y evaluar en forma aleatoria la efectividad de los controles del mapa de riesgos de la Dirección de Tecnología
ALCANCE DE LA AUDITORIA:	Realizar el análisis y verificación de manera aleatoria del mapa de riesgos de la Dirección de Tecnología que se encuentra en el sistema de información VIGIA para el segundo semestre del 2017
CRITERIOS DE LA AUDITORIA:	Ley 87 de 1993, por la cual se establecen normas para el ejercicio del Control Interno en las entidades y organismos del Estado y se dictan otras disposiciones. Decreto 1499 de 2017 modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015 Capítulo XXIII de la circular externa 100 de 10995 – Reglas relativas a la Administración del Riesgo Operativo

OBSERVACIONES Y RECOMENDACIONES

Criterio de auditoría			*Observación OCI*	*Recomendación OCI*
1	**Riesgo**	**Pérdida de información crítica.**		
1.1	Descripción del control	"Administración, monitoreo y soporte de los servidores que soportan los sistemas de información".	La administración monitoreo y soporte lo realiza el contratista Level 3, se evidenciaron lo siguientes informes: Informe Administración BD, Informe Administración de red, Informe Administración Seguridad, Informe Administración WEB. Se observó que los informes presentan recomendaciones del contratista respecto a las incidencias que se presentan y actas de reuniones de seguimiento; sin embargo, no se evidencio la documentación con las acciones de mejora implementadas.	Se recomienda a la Dirección de Tecnología documentar las acciones de mejora propuestas por el contratista Level3.
	Detalle de la evidencia	"Informes de monitoreo. informes de gestión de incidentes, informes de análisis de rendimiento".		
1.2	Descripción del control	"La configuración de los discos de los servidores se encuentra en alta disponibilidad, es decir, un disco es espejo del otro de modo tal, que, si uno falla, el otro disco garantiza la disponibilidad del servicio".	Se observó que el detalle de la evidencia no soporta la descripción del control. No obstante, se evidenció que mediante contrato 2014-0298 se adquirió un sistema de servidores y almacenamiento que incluye las características mencionadas en la descripción del control. Se observó reporte del sistema de la configuración de los discos. Se evidenció que las hojas de vida de los servidores se encuentran en un repositorio en un servidor del Data Center en formato Excel, no obstante, se observó que estos archivos no se actualizan desde 2016, lo cual debería se periódicamente.	Se recomienda a la Dirección de Tecnología, implementar procedimientos para administrar la Infraestructura de Hardware y Software, los sistemas de información y la gestión de actualización de los sistemas operativos (Parches).
	Detalle de la evidencia	"Hojas de vida de cada uno de los servidores - contrato con el proveedor de		

		centro de cómputo"		
1.3	Descripción del control Detalle de la evidencia	"Método por el cual se garantiza la copia de la información en un medio diferente sobre el que normalmente consultada (sic)" "Informe mensual del proveedor por gestión de backups"	Esta auditoria considera que la descripción del control no es explicita. Se observó que el proceso de backup lo realiza el contratista Level3 con un procedimiento propio. Se revisaron reportes de ejecución de los backups, los cuales indican que algunos se efectuaron parcialmente, es decir que no se realizaron exitosamente, no se evidenció relanzamiento del backup	Se recomienda documentar el relanzamiento del backup en caso de falla de la ejecución, teniendo en cuenta el procedimiento de administración de backup del contratista.
1.4	Descripción del control Detalle de la evidencia	"Centro de datos donde se encuentran alojados los sistemas Core en un estado offline y a la espera de una puesta en servicio para recuperar operación / servicio en caso de desastre" "Centro de datos ante desastres"	El Icetex no cuenta con un centro de cómputo alterno que cuente con todos los servicios del centro de cómputo principal. No se evidenció la realización de pruebas a todos los aplicativos y a toda la infraestructura del plan de continuidad. Se evidencio que para la puesta en servicio del Data center alterno se requiere de operaciones manuales que no garantizan los tiempos de recuperación establecidos en el Análisis de Impacto de Negocio del ICETEX. Se presento el evento de riesgo numero 7540 el 25 de julio de 2017 "*...incidente de falla e indisponibilidad en los servicios tecnológicos de correo electrónico, carpetas compartidas y la aplicación apoteosys...*"	Se recomienda en el mediano plazo, disponer de un centro de cómputo e infraestructura alterno con las especificaciones técnicas que soporten la continuidad de la operación de acuerdo con lo establecido en el Manual de Administración del Plan de continuidad de negocio.

1.5	Descripción del control Detalle de la evidencia	"Asignación de acceso a los sistemas de información con la revisión y aprobación del jefe de área usuaria solicitante, el oficial de seguridad de la información o a quien haga sus veces y el apoyo de la Dirección de Tecnología." "Procedimientos de asignación / retiro de accesos a sistemas de información evidenciados en los formatos F121 y procedimiento de asignación / retiro de accesos a sistemas IES - IES ORI formato F247 debidamente diligenciados y firmados."	Se evidenciaron los formatos mencionados, los cuales son verificados por la Oficina de Riesgos	No aplica
1.6	Descripción del control Detalle de la evidencia	"Sistemas de seguridad perimetral los cuales aparte de controlar los accesos protegen la institución de intrusiones potenciales o software mal intencionado." "Procedimiento de pruebas de vulnerabilidades, informes de vulnerabilidades	El detalle de la evidencia no soporta la descripción del control. La Oficina de Control Interno evidenció reporte de escaneo de vulnerabilidades, Se observó acta de comité de vulnerabilidades en la cual se realiza análisis y tratamiento de estas, sin embargo, los reportes evidencian que existen vulnerabilidades internas medias que siguen sin resolverse.	Se recomienda incluir en el detalle de la evidencia información relacionada con los dispositivos de Hardware y software que hacen parte de los sistemas de seguridad perimetral. Se recomienda cerrar las vulnerabilidades pendientes de resolver.

		periódicos, configuración actual de la herramienta para intrusos, políticas actuales de configuración."		
1.7	Descripción del control	"Cada área funcional cuenta con una carpeta en el servidor de archivos, en la cual se debe almacenar la información sensible del área. estas carpetas están incluidas dentro de la política de backup."	Se evidenciaron las carpetas asignadas a las diferentes áreas del Instituto en el servidor identificado "ictxsrvfs" (192.168.51.120) se verifico en el reporte de backup que lo incluye en la copia. Se observaron reporte de backups los cuales indican que se ejecutaron parcialmente, no se evidenció relanzamiento del backup. El control no es efectivo por cuanto se evidenció el evento de riesgo número 5913 del 21 de noviembre de 2016: *"…. carpeta compartida grupoconciliaciones (\\ictxsrvfs)(z:), dentro de la cual se tiene una carpeta de ¿cuentas abandonadas¿, ...observamos que la información ha sido eliminada, ...se llama a soporte y se nos informa que no se evidencian las carpetas en el momento de realizar el remoto....."* No existen políticas ni controles para la retención de información en el manejo de las carpetas.	Se recomienda a la Vicepresidencia de Operaciones y Tecnología y la Dirección de Tecnología, revisar y establecer nuevos controles, dado que los señalados en el mapa de riesgos no son efectivos. Se recomienda implementar políticas de retención de información para las carpetas compartidas. De la misma manera identificar la información sensible de los computadores de las diferentes dependencias. Se recomienda documentar el relanzamiento del backup en caso de falla de la ejecución, teniendo en cuenta el procedimiento de administración de backup del contratista.
	Detalle de la evidencia	"Procedimiento publicado de gestión de backups"		
1.8	Descripción del control	"Restauración periódica de backups por parte del proveedor del servicio - por demanda"	Se observó registro de restauración por demanda, realizado por la administradora de Base de Datos del Contratista Level 3	No aplica
	Detalle de la evidencia	"Restauración periódica de backups por parte del proveedor del servicio - por demanda"		

1,9	Descripción del control Detalle de la evidencia	"Aplicación del sistema de antivirus." "Consola actualizada y archivos de definiciones de virus que este actualizada. en los equipos de cómputo se puede ver la fecha de actualización del software de antivirus y su ejecución."	Se verificó la instalación de la suite de McAfee (Contrato 2014-0148) en los equipos de cómputo de la Entidad, la cual incluye antivirus, analizador de vulnerabilidades, control de acceso a la red, Gateway de correo y es administrada por el contratista de seguridad de la firma Level 3. Se evidencio la actualización de la plataforma mediante contrato 2017-0462 con Softsequrity Ltda.	No aplica
1.10	Descripción del control Detalle de la evidencia	"Filtro web - se cuenta con un filtro de la página web que impide que el usuario ingrese a una página que este reportada como potencialmente peligrosa según una base de datos que se actualiza constantemente" "Reporte de navegación de las paginas a ingresar por usuario por la herramienta de gestión"	Se observó reporte del dispositivo de seguridad (appliance) implementado de control de contenido BARRACUDA, que controla el acceso a sitios Web y aplicaciones autorizadas.	No aplica
1.11	Descripción del control	"Elaboración de restricciones acordes a la parametrización de la herramienta con el fin de establecer	Se evidenció que la entidad cuenta con una suite McAfee para asegurar equipos de cómputo, así mismo se ha restringido acceso a las unidades de CD y DVD de las estaciones de trabajo que se encuentran dentro del dominio "Icetex". Sin embargo, se observó que es posible realizar la descarga de	Se recomienda a la Dirección de Tecnología definir el alcance del control con el propósito de validar el bloqueo de descargas potencialmente peligrosas para la entidad.

		niveles de bloqueo de usuarios"	archivos lo que constituye un riesgo de seguridad.	
	Detalle de la evidencia	"Informe generado por la herramienta de gestión de seguridad - por demanda"		
2	**Riesgo**	**Fallas de software y hardware que afectan la operación del Instituto.**		
2.1	Descripción del control	"Contrato de soporte a los servidores de producción."	Esta auditoria considera que el contrato de soporte no es un control.	Se recomienda que la descripción del control determine las acciones preventivas y correctivas realizadas por el contratista con la supervisión y documentación de las acciones de mejora por parte de la Dirección de Tecnología.
	Detalle de la evidencia	"N/A"		
2.2	Descripción del control	"La infraestructura que soporta las bases de datos de producción se encuentra en alta disponibilidad."	Se observo reporte de la herramienta DATA GUARD donde se evidencia la configuración de la Base de datos en alta disponibilidad	No aplica
	Detalle de la evidencia	"N/A"		
2.3	Descripción del control	"Los mantenimientos de la entidad se realizan bajo un cronograma de trabajo los mantenimientos se realizan por personal especializado se realiza un análisis del impacto de la realización del mantenimiento	Esta auditoria considera que la descripción del control no es específica en la actividad a realizar. Se observó que el contratista realiza la programación de mantenimiento a los equipos de cómputo e informa mediante correo electrónico.	Se recomienda modificar la redacción del control en el cual se especifique la actividad para prevenir el riesgo de fallas de hardware y software

		(hardware y software)"		
	Detalle de la evidencia	"Correo electrónico informando los mantenimientos y actualización con fecha y hora. documentado en el acta de comité de cambios donde se informan los mantenimientos programados. informe de resultados y actualización de hojas de vida (cuando aplique) revisar análisis de impacto"		
2.4	Descripción del control	"Verificación periódica por parte del coordinador de infraestructura de la ejecución del cumplimiento del plan de administración del DBA verificar la calidad y completitud de los procedimientos y en general a la documentación de las bases de datos por parte del coordinador de infraestructura"	Se evidencio Informe del contratista con las actividades relacionadas con la Administración de Base de Datos.	Se recomienda documentar las acciones de mejoramiento a las observaciones realizadas por el administrador de Base de Datos
	Detalle de la evidencia	"Actas de comité de infraestructura"		

2.5	Descripción del control Detalle de la evidencia	"Los servidores de misión crítica del Icetex se encuentra en un data center tercerizado certificado tanto en sitio principal como sitio alterno que cumple con normativas internacionales para garantizar disponibilidad y seguridad" "Seguimiento al informe mensual que entrega el proveedor de data center (capitulo)- contrato con el proveedor del servicio"	Se evidencio que el contratista Level 3 cuenta con las certificaciones internacionales mencionadas en la descripción del control. Sin embargo se presentaron fallas en la disponibilidad de los servidores a nivel nacional como se evidencia en los incidentes presentados por la no disponibilidad de los servicios y los siguientes eventos de riesgo numero 7260 (23 junio de 2017) "*.....se reportó un error de almacenamiento en el servidor a nivel nacional, ...*" *Numero 7319:".....se presenta caída de la aplicación crm cosmos lo cual genera 15 minutos sin servicio de aplicación afectando los canales de atención de la entidad.....".*	Se recomienda a la Dirección de Tecnología documentar la topología y funcionalidad de todos los recursos y servicios de red con el fin de identificar y solucionar oportunamente las fallas presentadas.
3.	**Riesgo**	**Fallas en las telecomunicaciones que afectan la operación del Instituto.**		
3.1	Descripción del control Detalle de la evidencia	"Toma de respaldo del estado actual antes de la actualización para poder realizar roll back en caso de falla" "Actas de comité - procedimiento de control de cambios"	La descripción del control no es precisa, no indica a cuál componente de hardware y/o software se le realiza el respaldo. Se verificó que la Dirección de Tecnología tiene un repositorio con las plantillas de los dispositivos de red que corresponden a la configuración de los switch, sin embargo, se observó que esta documentación no se actualiza periódicamente.	Se recomienda ajustar la descripción del control con el fin de determinar a cuál componente de hardware y/o software de telecomunicaciones corresponde la actualización. Se recomienda a la Dirección de Tecnología, implementar procedimientos para administrar la Infraestructura de Hardware y Software de telecomunicaciones.
3.2	Descripción del control	"El coordinador de infraestructura realiza seguimiento al cumplimiento del contrato con respecto a los	Se evidencio reporte en formato Excel donde se indica el porcentaje de cumplimiento por cada servicio. No se evidencia en los indicadores las fallas en el servicio presentadas en el mes de julio de 2017, situación que incide en la facturación de los servicios prestados por el contratista	Se recomienda fortalecer los controles con el fin de reflejar en los indicadores las fallas presentadas en el servicio y aplicar las sanciones correspondientes.

	Detalle de la evidencia	acuerdos de niveles de servicio, aplica sanciones cuando fuere el caso (sobre la factura)." "Informe de indicadores de acuerdos de niveles de servicios de infraestructura"		
3.3	Descripción del control Detalle de la evidencia	"El acceso a estos dispositivos lo realizan funcionarios idóneos para esta actividad y es un área restringida." "Correo electrónico con los datos de los funcionarios autorizados que sirve de control de acceso a centro de cómputo"	La descripción no corresponde a un control, no indica si existen políticas y/o procedimientos de acceso al área donde se encuentran los dispositivos que tienen restricción	Se recomienda que la descripción del control determine las acciones preventivas tendientes a restringir el acceso físico y lógico a personal autorizado, al área donde operan los dispositivos de telecomunicaciones.
3.4	Descripción del control Detalle de la evidencia	"La entidad cuenta con un sistema de seguridad perimetral sobre la infraestructura tecnológica de Icetex" "Alertas dadas por los sistemas de seguridad de la entidad contar con antivirus instalado en las estaciones de trabajo"	Se evidenció que la Entidad dispone de una infraestructura tecnológica (telecomunicaciones, servidores y aplicaciones), la cual cuenta con los niveles requeridos de disponibilidad y seguridad, soportada a través del contrato de prestación de servicios No.004-2015 con la firma Level 3. se verificó Informe de Administración de seguridad de enero de 2018	Se recomienda implementar las acciones propuestas por el contratista respecto a la actualización de componentes de hardware y software, aplicación de controles y verificaciones de los servicios, mitigar los inconvenientes eléctricos en la sede Aguas, ejecutar adecuadamente el proceso de cambios de personal, asegurar el cierre de vulnerabilidades y clasificación de la información.

4 Riesgo	**No contar con un adecuado soporte a los usuarios que permita atender los requerimientos de los sistemas de información y de infraestructura.**			
4.1	Descripción del control	"Garantizar un proveedor de servicio técnico que soporte a nivel nacional la atención de requerimientos"	Se evidenció contrato 2017-02308 de prestación de servicios de esquema de servicio integral con soporte técnico preventivo y correctivo a la infraestructura de tecnología y los sistemas de información; soporte técnico a la infraestructura LAN; administración y soporte especializado a las plataformas de servicios virtualizados VMware y administración y soporte especializado a plataforma de servicios Microsoft del ICETEX. Se observaron los informes de gestión a todos los servicios incluidos en el contrato.	No aplica
	Detalle de la evidencia	"Seguimiento al informe mensual de la mesa de ayuda y la atención de requerimientos a nivel nacional dando cumplimiento a los acuerdos de niveles de servicio a nivel nacional"		
4.2	Descripción del control	"Se cuenta con canales (vía telefónica y correo electrónico) que les permite a los usuarios registrar sus solicitudes de atención a requerimientos."	Se evidencio que las solicitudes se realizan por vía telefónica y correo electrónico y se registran por parte del contratista en la aplicación ARANDA SERVICE DESK	No aplica
	Detalle de la evidencia	"Registro de los casos reportados por los funcionarios en la herramienta destinada para tal fin"		
5 Riesgo	**Proyectos que se desarrollan cumpliendo con los requerimientos de los usuarios, pero que no cumplen con las necesidades de la operación**			

5.1	Descripción del control	"Realizar por parte del ingeniero asignado por la coordinación de sistemas de información el cumplimiento de las etapas del desarrollo propuesto y el cumplimiento de las pruebas validadas por los funcionales para tal fin, anexando la debida documentación"	Se evidencio formato F60 y F80 y acta de comité de cambios	No aplica
	Detalle de la evidencia	"Formato F60 y formato F80, acta de comité de cambios"		
5.2	Descripción del control	"Para el procedimiento de desarrollo de software, se solicita que debe asociarse un Mantis de desarrollo avalado por el jefe del área, quien confirma la solicitud y el solicitante para llevar a cabo el desarrollo, confirmando la idoneidad del usuario funcional."	Se observa que en la herramienta Mantis no tiene control para la creación de usuarios	Se recomienda a la Dirección de Tecnología depurar los usuarios en la herramienta Mantis y establecer los controles necesarios en la asignación de usuarios.
	Detalle de la evidencia	"Formato F60 - Mantis de software asociado al requerimiento de desarrollo"		

5.3	Descripción del control	"Verificación de la ejecución de la validación de control de calidad de software por parte del líder de calidad y la certificación del gerente del proyecto de los controles de calidad para las pruebas del desarrollo."	Se observó que el desarrollo de software se realiza mediante la contratación de servicios profesionales de ingenieros para la codificación y generación de software por demanda y atención de emergencias. No se evidenció documentación con la planeación contractual respecto a los ingenieros contratados v/s los proyectos de desarrollo de la Entidad. No se evidenciaron controles para supervisar el cumplimiento de los proyectos de software asignados a los contratistas. No se evidenciaron controles que permitan determinar la repercusión del desarrollo de software sobre la información de los aplicativos de la Entidad. No se evidenciaron controles para dar continuidad a los proyectos de software de los contratistas que finalizan por anticipado el contrato.	Se recomienda a la Dirección de Tecnología implementar controles para validar la calidad del desarrollo de software de acuerdo con las necesidades de la Entidad. De la misma manera aplicar metodologías de gestión de proyectos de desarrollo de software.
	Detalle de la evidencia	"Certificación de pruebas de fabrica"		
6	**Riesgo**	**Modificaciones o extracciones no autorizadas de la información contenida en los diferentes medios informáticos de la entidad o pérdida definitiva de la misma**		
6.1	Descripción del control	"Remediación de vulnerabilidades por los administradores de acuerdo con el reporte de los escaneos por parte del administrador de seguridad realizados en la Dirección de Tecnología"	La Oficina de Control Interno evidenció reporte de escaneo de vulnerabilidades, se observó acta de comité de vulnerabilidades en la cual se realiza análisis y tratamiento de estas, sin embargo, los reportes evidencian que existen vulnerabilidades internas medias que siguen sin resolverse.	Se recomienda a la Dirección de Tecnología en coordinación con el contratista asegurar el cierre de vulnerabilidades teniendo en cuenta los informes de vulnerabilidades generados con el propósito de asegurar la red de la Entidad
	Detalle de la evidencia	"Actas comité vulnerabilidades"		

6.2	Descripción del control	"Se estableció logs de auditoria para todas las bases de datos y se realiza una revisión aleatoria periódica de los mismos en los comités de logs."	Se evidencio que la Dirección de Tecnología realiza comité de Logs de los sistemas de información críticos del ICETEX, sin embargo, no se evidenciaron actividades de seguimiento y control a los usuarios con altos privilegios sobre la base de datos que establece el manual de seguridad de la información (numeral 11.5.1 y 11.6)	• Se recomienda a la Vicepresidencia de Operaciones y Tecnología implementar registros de auditoria a las transacciones críticas del sistema a los usuarios con altos privilegios • Se recomienda implementar registro de auditoría a las modificaciones que se realizan mediante procesos masivos a la base de datos de los aplicativos de la Entidad dado que estos cambios se realizan sin hacer uso del software.
	Detalle de la evidencia	"Actas de comités de logs"		
7	**Riesgo**	**Falla en los procedimientos para mantener la capacidad de implementación de sistemas de información**		
7.1	Descripción del control	"Se realiza revisión a los logs de auditoria de los cambios realizados en las bases de datos."	Se evidencio que la Dirección de Tecnología realiza comité de Logs de los sistemas de información críticos del ICETEX, sin embargo, no se evidenciaron actividades de seguimiento y control a los usuarios con altos privilegios sobre la base de datos que establece el manual de seguridad de la información (numeral 11.5.1 y 11.6)	• Se recomienda a la Vicepresidencia de Operaciones y Tecnología implementar registros de auditoria a las transacciones críticas del sistema a los usuarios con altos privilegios • Se recomienda implementar registro de auditoría a las modificaciones que se realizan mediante procesos masivos a la base de datos del aplicativo C&CETEX dado que estos cambios se realizan sin hacer uso del software.
	Detalle de la evidencia	"Acta del comité de logs"		

Informe elaborado por: Carlos Eduardo Cruz González
Informe aprobado por: Luz Alba Sanchez Sanchez

Código: F263
Versión: 1
Fecha: 11/04/2013
Página 1 de 2

PLAN DE MEJORAMIENTO AUDITORIAS DE GESTIÓN

AREA : DIRECCIÓN DE TECNOLOGIA FECHA DILIGENCIAMIENTO FORMATO: _____

PROCESO	HALLAZGO/OBSERVACION	ACCIONES DE MEJORAMIENTO	FECHA DE INICIO DE LA ACCIÓN	FECHA DE FINALIZACIÓN DE LA ACCIÓN	RESPONSABLE
	Numeral 1.1 Se observó que los informes presentan recomendaciones del contratista respecto a las incidencias que se presentan y actas de reuniones de seguimiento; sin embargo, no se evidencio la documentación con las acciones de mejora implementadas.				
	Numeral 1.2 Se observó que el detalle de la evidencia no soporta la descripción del control. No obstante, se evidenció que mediante contrato 2014-0298 se adquirió un sistema de servidores y almacenamiento que incluye las características mencionadas en la descripción del control. Se observó reporte del sistema de la configuración de los discos. Se evidenció que las hojas de vida de los servidores se encuentran en un repositorio en un servidor del Data Center en formato Excel, no obstante, se observó que estos archivos no se actualizan desde 2016, lo cual debería se periódicamente.				
	Numeral 1.3 Esta auditoria considera que la descripción del control no es explicita. Se observó que el proceso de backup lo realiza el contratista Level3 con un procedimiento propio. Se revisaron reportes de ejecución de los backups, los cuales indican que algunos se efectuaron parcialmente, es decir que no se realizaron exitosamente, no se evidenció relanzamiento del backup				
	Numeral 1.4 El Icetex no cuenta con un centro de cómputo alterno que cuente con todos los servicios del centro de cómputo principal. No se evidenció la realización de pruebas a todos los aplicativos y a toda la infraestructura del plan de continuidad. Se evidencio que para la puesta en servicio del Data center alterno se requiere de operaciones manuales que no garantizan los tiempos de recuperación establecidos en el Análisis de Impacto de Negocio del ICETEX. Se presento el evento de riesgo numero 7540 el 25 de julio de 2017 "...incidente de falla e indisponibilidad en los servicios tecnológicos de correo electrónico, carpetas compartidas y la aplicación apoteosys..."				
	Numeral 1.6 El detalle de la evidencia no soporta la descripción del control. La Oficina de Control Interno evidenció reporte de escaneo de vulnerabilidades, Se observó acta de comité de vulnerabilidades en la cual se realiza análisis y tratamiento de estas, sin embargo, los reportes evidencian que existen vulnerabilidades internas medias que siguen sin resolverse.				
	Numeral 1.7 Se evidenciaron las carpetas asignadas a las diferentes áreas del Instituto en el servidor identificado "ictxsrvfs" (192.168.51.120) se verifica en el reporte de backup que lo incluye en la copia				
	Numeral 1.11 Se evidenció que la entidad cuenta con una suite McAfee para asegurar equipos de cómputo, así mismo se ha restringido acceso a las unidades de CD y DVD de las estaciones de trabajo que se encuentran dentro del dominio "Icetex". Sin embargo, se observó que es posible realizar la descarga de archivos lo que constituye un riesgo de seguridad.				
	Numeral 2.1 Esta auditoria considera que el contrato de soporte no es un control.				
	Numeral 2.3 Esta auditoria considera que la descripción del control no es específica en la actividad a realizar.				
	Numeral 2.4 Se evidencio Informe del contratista con las actividades relacionadas con la Administración de Base de Datos. Se recomienda documentar las acciones de mejoramiento a las observaciones realizadas por el administrador de Base de Datos				
	Numeral 2.5 Se evidencio que el contratista Level 3 cuenta con las certificaciones internacionales mencionadas en la descripción del control. Sin embargo se presentaron fallas en la disponibilidad de los servidores a nivel nacional como se evidencia en los incidentes presentados por la no disponibilidad de los servicios y los siguientes eventos de riesgo numero 7260 (23 junio de 2017) "*.....se reportó un error de almacenamiento en el servidor a nivel nacional, ...*" *Numero 7319:".....se presenta caída de la aplicación crm cosmos lo cual genera 15 minutos sin servicio de aplicación afectando los canales de atención de la entidad.....".*				
	Numeral 3.1 La descripción del control no es precisa, no indica a cuál componente de hardware y/o software se le realiza el respaldo. Se verificó que la Dirección de Tecnología tiene un repositorio con las plantillas de los dispositivos de red que corresponden a la configuración de los switch, sin embargo, se observó que esta documentación no se actualiza periódicamente.				

AREA : DIRECCIÓN DE TECNOLOGIA FECHA DILIGENCIAMIENTO FORMATO: _____

			FECHA DE INICIO	FECHA DE	
	Numeral 3.2 Se evidencio reporte en formato Excel donde se indica el porcentaje de cumplimiento por cada servicio. No se evidencia en los indicadores las fallas en el servicio presentadas en el mes de julio de 2017, situación que incide en la facturación de los servicios prestados por el contratista				
	Numeral 3.3 La descripción no corresponde a un control, no indica si existen políticas y/o procedimientos de acceso al área donde se encuentran los dispositivos que tienen restricción				
	Numeral 3.4 Se evidenció que la Entidad dispone de una infraestructura tecnológica (telecomunicaciones, servidores y aplicaciones), la cual cuenta con los niveles requeridos de disponibilidad y seguridad, soportada a través del contrato de prestación de servicios No.004-2015 con la firma Level 3. se verificó Informe de Administración de seguridad de enero de 2018. Se recomienda implementar las acciones propuestas por el contratista respecto a la actualización de componentes de hardware y software, aplicación de controles y verificaciones de los servicios, mitigar los inconvenientes eléctricos en la sede Aguas, ejecutar adecuadamente el proceso de cambios de personal, asegurar el cierre de vulnerabilidades y clasificación de la información.				
	Numeral 5.2 Se observa que en la herramienta Mantis no tiene control para la creación de usuarios				
	Numeral 5.3 Se observó que el desarrollo de software se realiza mediante la contratación de servicios profesionales de ingenieros para la codificación y generación de software por demanda y atención de emergencias. No se evidenció documentación con la planeación contractual respecto a los ingenieros contratados v/s los proyectos de desarrollo de la Entidad. No se evidenciaron controles que permitan determinar la repercusión del desarrollo de software sobre la información de los aplicativos de la Entidad. No se evidenciaron controles para supervisar el cumplimiento de los proyectos de software asignados a los contratistas. No se evidenciaron controles para dar continuidad a los proyectos de software de los contratistas que finalizan por anticipado el contrato.				
	Numeral 6.1 La Oficina de Control Interno evidenció reporte de escaneo de vulnerabilidades, se observó acta de comité de vulnerabilidades en la cual se realiza análisis y tratamiento de estas, sin embargo, los reportes evidencian que existen vulnerabilidades internas medias que siguen sin resolverse.				
	Numeral 6.2 Se evidencio que la Dirección de Tecnología realiza comité de Logs de los sistemas de información críticos del ICETEX, sin embargo, no se evidenciaron actividades de seguimiento y control a los usuarios con altos privilegios sobre la base de datos que establece el manual de seguridad de la información (numeral 11.5.1 y 11.6)				
	Numeral 7.1 Se evidencio que la Dirección de Tecnología realiza comité de Logs de los sistemas de información críticos del ICETEX, sin embargo, no se evidenciaron actividades de seguimiento y control a los usuarios con altos privilegios sobre la base de datos que establece el manual de seguridad de la información (numeral 11.5.1 y 11.6)				
ELABORADO POR.	***NOMBRE*** ***CARGO***				
APROBADO POR.	***NOMBRE*** ***CARGO***				