ICETEX Inversiones en el talento de los colombianos

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN

MEMORANDO

OCI 2600 – 147

Bogotá, Agosto 3 de 2016

PARA: **Dr. GERARDO GUTIERREZ CASTRO**
Jefe Oficina de Riesgos (E)

DE: **JEFE OFICINA DE CONTROL INTERNO**

ASUNTO: **SEGUIMIENTO CIRCULAR 029 de 2014**

La Oficina de Control Interno en cumplimiento de sus funciones, dentro de las cuales se encuentra la de evaluación y seguimiento a lo que compete, respecto de la Circular Externa 029 de 2014 de la Superintendencia Financiera de Colombia, realizó el seguimiento a la implementación de la citada Circular en relación a los requerimientos de seguridad.

Por lo anterior atentamente remito el documento con el resultado del seguimiento, con el fin de analizar y realizar los correctivos necesarios por parte de la firma Asesora de Seguridad de la Información, en coordinación con la Vicepresidencia de Operaciones y Tecnología, señalando las acciones y el plazo de su implementación, para lo cual se solicita enviarlo a ésta Oficina a más tardar el 17 de agosto de 2016, en el formato F263.

Cordialmente

LUZ ALBA SANCHEZ SANCHEZ

Anexo. Informe de seguimiento (9) folios
Plan de mejoramiento (7) folios

Copia. ING. MAURICIO GOMEZ MURCIA. Vicepresidente de Operaciones y Tecnología (E)

REQUERIMIENTOS MINIMOS DE SEGURIDAD					
Numeral Circular	Actividad	Aplica?	Respuesta Oficina de Riesgos	Estado implementado	Verificación Oficina de Control Interno
Obligaciones Generales					
Seguridad y Calidad					
3.1.1	Disponer de hardware, software y equipos de telecomunicaciones, así como de los procedimientos y controles necesarios, que permitan prestar los servicios y manejar la información en condiciones de seguridad y calidad.	SI	El Icetex cuenta con dispositivos (appliances) de seguridad perimetral como son: firewall (4), Monitoreo de trafico, proxy, IPS, Web Filter y WAF; se cuenta con seguridad a profundidad con la solución Endpoint de McAfee que, entre otros, tiene un analizador de vulnerabilidades y dos anti spam. La entidad cuenta con una red MPLS . Se ha establecido conexión VPN con los aliados comerciales (Serlefin, Data File, Deceval, Banco República); de manera adicional, con los proveedores Serlefin y Datafile existe un canal dedicado con **Contact Center Americas** (Sede Cobranzas) para establecer comunicaciones y se cuenta con un servicio SFTP con las entidades financieras para transmisión de información. Existe documentación del esquema de red actualizado al año 2015 por el contratista Level 3, documentación del servicio SFTP, de las reglas de. firewall, los diagnósticos de las soluciones de McAfee. Sin embargo, se requiere actualizar la documentación existente y documentar algunos procedimientos. Los procedimientos de la Dirección de Tecnología reposan en la herramienta In Process del instituto.	80%	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. La Direccción de Tecnología no suministró la documentación relacionada con las reglas del firewall.
3.1.2	Gestionar la seguridad de la información, para lo cual podrán tener como referencia el estándar ISO 27000, o el que lo sustituya	SI	Icetex ha adoptado la norma ISO 27001 como un estándar para la gestión de la seguridad de la información, para lo cual se encuentra en proceso de implementación desde del año 2014 y se han efectuado las principales actividades: Política de seguridad de la información, Inventario y Clasificación de Activos de Información, Gestión de Riesgos, Análisis de Vulnerabilidades.	37%	Se observó que el Icetex suscribió los contratos 2015-0074 y 2016-051 - cuyo objeto es el de implementar el modelo de seguridad y privacidad de la información de la estrategia de gobierno en línea el cual esta alienado con la norma ISO 27001, a la fecha se evidenciaron las siguientes actividades: • Planeación de modelo de seguridad y privacidad de la información de la Estrategia de Gobierno en línea. • Gestión de riesgos de seguridad de la información (50% de ejecución) . • Inventario y clasificación de activos de información (100 %). Es de señalar que el ICETEX no ha implementado la transición del protocolo IPv4 IPv6, requerido para dar cumplimiento a la etapa de DIAGNOSTICO – PLANIFICACION del Modelo de seguridad y privacidad de la Estrategia de Gobierno en Línea (GEL).
3.1.3	Disponer que el envío de información confidencial y de los instrumentos para la realización de operaciones a sus clientes, se haga en condiciones de seguridad. Cuando dicha información se envíe como parte de, o adjunta a un correo electrónico, ésta deberá estar cifrada	SI	Se envía información a los clientes sin cifrar, sin embargo la información de los clientes que se intercambia con terceros va cifrada mediante la plataforma Go any where (software de encripción de información). Los bancos envían información de clientes en archivos por medio del servicio SFTP, en donde el canal y el archivo son cifrados. A su vez, PSE (Pagos Seguros en Línea) envía un archivo de recaudos.	20%	El área de Tecnología mediante el contrato de prestación de servicios 004-2015 con la firma Level 3 implementa los mecanismos de seguridad del Instituto (Ej. Tesoreria - Recaudos), sin embargo NO se evidenció un procedimiento formal para realizar dicha actividad, ni los activos de información que se encuentran protegidos.
3.1.4	Dotar de seguridad la información confidencial de los clientes que se maneja en los equipos y redes de la entidad	SI	La entidad cuenta con una suite McAfee para asegurar los Endpoints (equipos de computo). Se han establecido controles de acceso a las unidades de CD y DVD de las estaciones de trabajo que se encuentran dentro del dominio "Icetex". Existe un antivirus corporativo McAfee y HPIS (host IPS a nivel local) y WAF (Protección portal Web); hay protección a nivel de GPO (Group Policy Management). Se encuentra implementado un appliance (dispositivo de seguridad) de control de contenido BARRACUDA , que controla el acceso a sitios Web y aplicaciones autorizadas.	80%	La Dirección de Tecnología informa que se realiza aseguramiento a nivel del servidor de bases de datos mediante la reducción de vulnerabilidades. Se evidenció reporte de escaneo de vulnerabilidades (verificación de seguridad a los recursos informáticos, mediante el análisis de los puertos abiertos en toda la red, que permite identificar los riesgos de seguridad, además identifica las debilidades del sistema operativo o de software de aplicación- Procedimiento Pruebas de Vulnerabilidad en el sistema de gestión de calidad.), se observó acta de comite de vulnerabilidades en la cual se realiza análisis y tratamiento de las mismas, sin embargo los reportes evidencian que existen vulnerabilidades que siguen sin resolverse desde el año 2014 .

REQUERIMIENTOS MINIMOS DE SEGURIDAD					
Numeral Circular	Actividad	Aplica?	Respuesta Oficina de Riesgos	Estado implementado	Verificación Oficina de Control Interno
3.1.5	Velar porque la información enviada a los clientes esté libre de software malicioso	SI	Como parte de la suite de McAfee se cuenta con servicios de antivirus y anti spam de entrada y salida, el cual hace las veces de antimalware. Sobre el correo electrónico (Exchange) se tiene un aplicativo contra malware y anti spam y a nivel de salida se tiene otro anti spam de McAfee. Se cuenta en las estaciones de trabajo con software de antivirus Endpoint. Así mismo, se cuenta con un IPS. La documentación del proceso de operación del antivirus puede estar desactualizada y la documentación de la actualización del antispam no se ha realizado.	50%	Se verificó la instalación de la suite de McAfee (Contrato 2014-0148) en los equipos de computo 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.no se evidencio la actualización ni documentación de la plataforma teniendo en cuenta que el contrato fue suscrito con fecha 24 de enero de 2014.
3.1.6	Proteger las claves de acceso a los sistemas de información. En desarrollo de esta obligación, las entidades deberán evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en los dispositivos y sistemas de cómputo de las entidades deberá ser única y personalizada	SI	Existe la Política de Contraseñas en la Política de Seguridad de la Información y se aplica en la Guía de contraseñas seguras dentro del proceso de Gestión de Servicios que contienen las contraseñas de acceso al Directorio Activo y los servicios de red obedecen a directrices de seguridad como son: vencimiento a los 30 días, control histórico de 5 contraseñas, complejidad y longitud mínima. En los aplicativos hay políticas de contraseñas, particulares en cada caso y de manera general hay tipos de usuarios y perfiles; en C&CTEX el usuario administrador es personalizado, en Apoteosys los administradores son personalizados. en Bizagi hay un perfil administrador genérico el cual no es compartido. Así mismo, existen usuarios por defecto en algunos componentes como dominio, bases de datos así como usuarios locales; se cuenta con actas de justificación de esas excepciones, debido a que se requiere que estén activos por que algunas aplicaciones funcionan con ellos. Para la creación de usuarios se requiere el diligenciamiento de un formato que debe contar con aval del jefe de la persona solicitante y la autorización de la Oficina de Riesgos. Las depuraciones se manejan automáticas; para C&CTEX se diligencia un formato de desvinculación; así mismo, se generan inactivaciones en el dominio y correo. Por su parte C&CTEX y Apoteosys tienen activa la política de 30 días antes que se produzca la inactivación de la cuenta por no utilización. Se crean usuarios personalizados. Todos los usuarios administradores entregan sus contraseñas en sobre sellado al Director de Tecnología para su custodia, debido a que están cobijados por las políticas de cambio periódico de contraseñas. En la herramienta In Process existe documentado el procedimiento de control de accesos, el cual es aplicado para la gestión de los accesos lógicos; de igual manera, existen guías de contraseñas seguras.	70%	Se observaron políticas de contraseñas en los sistemas de información críticos del ICETEX (Complejidad, longitud minima , caducidad, etc.). Sin embargo se evidencio una aplicacion que **No** tiene cifradas las contraseñas en el módulo de admisnitración de ususarios. Se observó que existen procedimientos y guias relacionados a los accesos a los sistemas de información: MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN • Numeral 11.2.1. Normas de administración de acceso de usuarios • Numeral 11.3.1. Normas de responsabilidades de acceso de los usuarios • Numeral 11.4.1. Normas de uso de altos privilegios y utilitarios de administración SISTEMA DE GESTIÓN DE CALIDAD – In Process • Procedimiento Asignación/Retiro de accesos a sistemas de información • Procedimiento Asignación/Retiro de accesos a sistemas de información IES e IES-ORI • Guía de contraseñas seguras
3.1.7	Dotar a sus terminales, equipos de cómputo y redes locales de los elementos necesarios que eviten la instalación de programas o dispositivos que capturen la información de sus clientes y de sus operaciones	SI	La entidad cuenta con una suite McAfee para asegurar los Endpoints (equipos de computo). Se han establecido controles de acceso a las unidades de CD y DVD de las estaciones de trabajo que se encuentran dentro del dominio "Icetex".	60%	Se evidencio que la instalación de software requiere de privlegios de usuario Administrador (Soporte mesa de ayuda). Se evidencio que existe un formato de actualización de software, autorizado por la Oficna de Riesgos y el lider del proceso. Se evidenció que permite la descarga de archivos lo que constituye un riesgo de seguridad .

REQUERIMIENTOS MINIMOS DE SEGURIDAD					
Numeral Circular	Actividad	Aplica?	Respuesta Oficina de Riesgos	Estado implementado	Verificación Oficina de Control Interno
3.1.8	Velar porque los niveles de seguridad de los elementos usados en los canales no se vean disminuidos durante toda su vida útil.	SI	Se realiza el uso de protocolos seguros tales como HTTPS y SSL para todas las transacciones generadas en el portal web del Icetex, se cuenta con un gestor de contenidos con niveles de seguridad establecidos. Cada uno de los aplicativos accedidos desde el portal tienen controles de autenticación. A nivel de plataforma se cuenta con firewall (4), proxy, WAF e IPS y los servidores donde funciona el portal web, administrados por un tercero, deben cumplir con los lineamientos de configuración segura establecidos por el Icetex.	80%	La Dirección de Tecnología cuenta en el Portal del ICETEX con Firewall y WAF (Web application Filter), que identifica cadenas de ataques (exploit sobre inyección de cadenas) o conexiones.
3.1.10	Ofrecer la posibilidad de manejar contraseñas diferentes para los instrumentos o canales, en caso de que éstos lo requieran y/o lo permitan.	SI	Los sistemas de información y sistemas operativos cuentan con la opción de cambio de contraseña .	80%	Se observó que los sistemas de información y el servidor de dominio tienen implementadas políticas de cambio de contraseña. Adicionalmente existen políticas y procedimientos relacionados a los accesos a los sistemas de información: MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN • Numeral 11.2.1. Normas de administración de acceso de usuarios • Numeral 11.3.1. Normas de responsabilidades de acceso de los usuarios • Numeral 11.4.1. Normas de uso de altos privilegios y utilitarios de administración SISTEMA DE GESTIÓN DE CALIDAD – In Process • Procedimiento Asignación/Retiro de accesos a sistemas de información • Procedimiento Asignación/Retiro de accesos a sistemas de información IES e IES-ORI • Guía de contraseñas seguras.
3.1.11	Establecer los mecanismos necesarios para que el mantenimiento y la instalación o desinstalación de programas o dispositivos en las terminales o equipos de cómputo sólo pueda ser realizado por personal debidamente autorizado	SI	Se verificó que existen restricciones por perfil de usuario para instalar o desinstalar software de los equipos de computo que soportan los servicios prestados a ICETEX.	40%	En la verificación realizada en los equipos de computo, se observó que la instalación de cualquier tipo de software requiere del privilegio de administrador del sistema, que permiten instalar o desinstalar software y/o aplicativos en general. Sin embargo es posible realizar la descarga de los archivos instaladores o ejecutables, lo que constituye un riesgo de seguridad. Mediante el software Aranda se identifica la instalación no autorizada de programas y el administrador de dominio realiza el proceso de desinstalación de software no autorizado, sin embargo no se evidenció que dicho procedimiento se encuentra documentado.
3.1.12	Establecer procedimientos para el bloqueo de canales o de instrumentos para la realización de operaciones, cuando existan situaciones o hechos que lo ameriten o después de un número de intentos de accesos fallidos por parte de un cliente, así como las medidas operativas y de seguridad para la reactivación de los mismos.	SI	Los aplicativos tienen política de numero de intentos fallidos de acceso y desconexión por inactividad (C&CETEX)	60%	El servidor de dominio y el sistema de información C&CETEX tienen implementadas políticas que bloquean los usuarios después de un número determinado de intentos fallidos de autenticación (3) y tiempo de desconexión por inactividad a los 5 minutos. Se evidenciaron aplicativos que no tienen implementadas las políticas mencionadas (TAE)
3.1.14	Realizar una adecuada segregación de funciones del personal que administre, opere, mantenga y, en general, tenga la posibilidad de acceder a los dispositivos y sistemas usados en los distintos canales e instrumentos para la realización de operaciones. En desarrollo de lo anterior, las entidades deberán establecer los procedimientos y controles para el alistamiento, transporte, instalación y mantenimiento de los dispositivos usados en los canales de distribución de servicios	SI	La entidad tiene una segregación de funciones para controlar dispositivos y sistemas	40%	Se observó que los sistemas de información de misión crítica presentan perfiles de acceso por tipo de usuario y registro de auditoría de las transacciones sensibles. Sin embargo se evidenciaron aplicativos que no tienen definidos perfiles y no generan registros de auditoría.
3.1.15	Definir los procedimientos y medidas que se deberán ejecutar cuando se encuentre evidencia de la alteración de los dispositivos usados en los canales de distribución de servicios financieros	SI	Se cuenta con la herramienta Aranda la cual genera y mantiene el inventario sobre los equipos de cómputo y se realizan comités de revisión de logs con una periodicidad establecida; sin embargo, la entidad no cuenta con procedimientos para la gestión de incidentes de seguridad.	40%	Se evidenció el registro de incidentes de seguridad, asi mismo se evidenció acta de comite de revisión de logs de auditoría de los aplicativos de misión crítica. Se observó que no se encuentra implementado registro de auditoría en todas las transacciones sensibles que se relizan a traves de aplicativos de misión crítica.

REQUERIMIENTOS MINIMOS DE SEGURIDAD					
Numeral Circular	Actividad	Aplica?	Respuesta Oficina de Riesgos	Estado implementado	Verificación Oficina de Control Interno
3.1.16	Sincronizar todos los relojes de los sistemas de información de la entidad involucrados en los canales de distribución. Se deberá tener como referencia la hora oficial suministrada por la Superintendencia de Industria y Comercio	SI	Actualmente se esta sincronizando la plataforma tecnológica con el servidor de tiempo de la Superintendencia de Industria y Comercio (SIC); el servidor de dominio sincroniza con la SIC y contra el se sincronizan los demás servidores y equipos. No obstante, los servidores con sistemas operativos Linux sincronizan contra un servidor estándar en internet y dicho servidor se encuentra alineado con la hora de la Superintendencia de Industria y Comercio (SIC).	80%	La Dirección de Tecnología informa que la sincronización se realiza con el servidor de la Superintendencia de Industria y Comercio , sin embargo se evidenció que la pagina del Instituto Nacional de Metrología reporta que esta entidad es la encargada de mantener, coordinar y difundir la hora legal de la República de Colombia. Se cotejó la hora configurada en el equipo de computo contra la hora registrada en la pagina web del instituno Nacional de Metrologia (www.inm.gov.co) , observándose diferencia contra el sistema de telefonía IP.
3.1.17	Tener en operación sólo los protocolos, servicios, aplicaciones, usuarios, equipos, entre otros, necesarios para el desarrollo de su actividad.	SI	Los protocolos, puertos y servicios en los equipos de computo son restringidos de acuerdo a las necesades y desarrollo de las actividades laborales.	100%	Se evidenció que la Dirección de Tecnología tiene implementadas políticas en los dispositivos de seguridad instalados en la entidad (firewall, IPS, Barracuda de navegación TCP servicio HTTP) que controlan las conexiones servicio y protocolos disponibles para los usuarios autorizados acorde a la características de los servicios.
Tercerización - Outsourcing					
3.2.1	Definir los criterios y procedimientos a partir de los cuales se seleccionarán los terceros y los servicios que serán atendidos por ellos.	SI	Se acogen los procesos de selección publica, los cuales establecen los criterios y procedimientos que deben cumplir los proveedores, teniendo en cuenta parámetros técnicos, económicos y operativos para la selección.	100%	Se observó que el Manual de Contratación y el Manual de Políticas de Seguridad de la Información incluyen los aspectos mencionados en los literales a, b, c, d y e en los numerales señalados a continuación. MANUAL DE CONTRATACION Numeral 10. ACUERDOS POR NIVELES DE SERVICIO Numeral 5.2.1 Determinación del objeto, alcance, clase de contrato y cláusulas.
3.2.2	Incluir en los contratos que se celebren con terceros o en aquellos que se prorroguen a partir de la entrada en vigencia del presente Capitulo, por lo menos, los siguientes aspectos: a) Niveles de servicio y operación. b) Acuerdos de confidencialidad sobre la información manejada y sobre las actividades desarrolladas. c) Propiedad de la información. d) Restricciones sobre el software empleado. e) Normas de seguridad informática y física a ser aplicadas. f) Procedimientos a seguir cuando se encuentre evidencia de alteración o manipulación de dispositivos o información. g) Procedimientos y controles para la entrega de la información manejada y la destrucción de la misma por parte del tercero una vez finalizado el servicio. Las entidades contarán con los procedimientos necesarios para verificar el cumplimiento de las obligaciones señaladas en el presente numeral, los cuales deberán ser informados previamente a la auditoría interna o quien ejerza sus funciones	SI	En los contratos celebrados con terceros se establecen niveles de servicio y operación, acuerdos de confidencialidad, propiedad de la información, restricciones sobre el software empleado, normas de seguridad informática y física. Sin embargo, no se tiene claridad del establecimiento de procedimientos a seguir cuando se encuentre evidencia de alteración o manipulación de dispositivos o información, ni de procedimientos y controles para la entrega de información al tercero y la destrucción de la misma, una vez finalizado el servicio.	70%	Se observó que el Manual de Contratación y el Manual de Políticas de Seguridad de la Información incluyen los aspectos mencionados en los literales a, b, c, d y e en los numerales señalados a continuación. **MANUAL DE CONTRATACION** Numeral 10. ACUERDOS POR NIVELES DE SERVICIO Numeral 5.2.1 Determinación del objeto, alcance, clase de contrato y cláusulas. **MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN** Numeral 9.1.1. Normas relacionadas con la vinculación de funcionarios Numeral 9.3.1. Normas para la desvinculación, licencias, vacaciones o cambios de labores de los funcionarios y personal provisto por terceros Numeral 15.4.1. Normas de intercambio de información Numeral 17.1. POLÍTICA DE INCLUSION DE CONDICIONES DE SEGURIDAD EN LA RELACIÓN CON TERCERAS PARTES Numeral 17.1.1. Normas de inclusión de condiciones de seguridad en la relación con terceras partes Numeral 17.2.1. Normas de gestión de la prestación de servicios de terceras partes" Sin embargo en los manuales no se evidenciaron normas para incluir en los contratos aspectos relacionados con el numeral f) Procedimientos a seguir cuando se encuentre evidencia de alteración o manipulación de dispositivos o información, y g) Procedimientos y controles para la entrega de la información manejada y la destrucción de la misma por parte del tercero una vez finalizado el servicio.
3.2.3	Exigir que los terceros contratados dispongan de planes de contingencia y continuidad debidamente documentados. Las entidades deberán verificar que los planes, en lo que corresponde a los servicios convenidos, funcionen en las condiciones pactadas	SI	Los contratos exigen que los terceros proveedores de servicios cuenten con un plan de continuidad de negocios. Icetex realiza pruebas periódicas de su plan de continuidad de negocios que incluyen pruebas de los planes de continuidad de los proveedores o se realizan pruebas compartidas; se solicitan los resultados de las pruebas efectuadas por los proveedores.	80%	Se evidencio que le ICETEX incluye en los contratos con terceros un plan de continuidad de negocios. Sin embargo no existen políticas relacionadas al plan de continuidad de negocio en el Manual de seguridad de la información en las políticas que rigen de la relación con terceras partes.
3.2.4	Establecer procedimientos que permitan identificar físicamente, de manera inequívoca, a los funcionarios de los terceros contratados	SI	Los funcionarios de terceros cuentan con carné que los identifica como proveedores, indicando el nombre de la compañía a la que pertenecen y, de acuerdo, con el tipo de servicio provisto, algunos proveedores están identificados por algún tipo de uniforme (chalecos). Sin embargo, se observó que no todos los funcionarios provistos por terceros portan su carné de identificación con ellos.	100%	Se evidencio el documento GUIA DE CARNETIZACION, en el sistema de Gestión de Calidad -In Process- . Se observó que los visitantes le expiden una escarapela para su identificación. Igualemente se solicita la presentación del carné al ingreso de la Entidad y se remiten correos electrónicos solicitando el uso obligatorio del carné.

REQUERIMIENTOS MINIMOS DE SEGURIDAD					
Numeral Circular	Actividad	Aplica?	Respuesta Oficina de Riesgos	Estado implementado	Verificación Oficina de Control Interno
3.2.5	Implementar mecanismos de cifrado fuerte para el envío y recepción de información confidencial con los terceros contratados.	SI	Hay conexiones directas (VPN site to site) con las casas de cobranza y con algunas entidades financieras. Con los demás aliados hay un protocolo de transferencia seguro (SFTP). El proveedor Serlefin cuenta con canal dedicado para establecer comunicación con ellos. Sin embargo, el envío de información por medio del correo electrónico no se cifra.	60%	El área de Tecnología mediante el contrato de prestación de servicios 004-2015 con la firma Level 3 implementa los mecanismos de seguridad de conformidad a los requerimientos puntuales de las dependencias del Instituto (Ej. Tesoreria - Recaudos), sin embargo NO se evidenció un procedimiento formal para realizar dicha actividad, ni los activos de información que se encuentran protegidos.
	Documentación				
3.3.1	Dejar constancia de todas las operaciones que se realicen a través de los distintos canales, la cual deberá contener cuando menos lo siguiente: fecha, hora, código del dispositivo (para operaciones realizadas a través de IVR: el número del teléfono desde el cual se hizo la llamada; para operaciones por Internet: la dirección IP desde la cual se hizo la misma; para operaciones con dispositivos móviles, el número desde el cual se hizo la conexión), cuenta(s), número de la operación y costo de la misma para el cliente o usuario.	SI	En el caso del portal web del Icetex queda registro de la última fecha de acceso, mas no de la transaccionalidad; en C&CTEX queda un log de accesos y actividades para los usuarios, registrado en tablas del aplicativo. Existe un perfil de consulta de logs y se lleva a cabo un comité de logs, cada dos meses dejando acta de su realización; en dicho comité se hace análisis de estos logs de manera muestral. En otros sistemas hay tablas de logs (accesos y transacciones). Se definieron los eventos sobre los cuales se generan logs de auditoria de C&CETEX como son: usuario, fecha, dirección IP, valores anteriores y valores nuevos. Estos logs se revisan en comité de logs. La Oficina de Comercial y Mercadeo envía mensualmente a la Dirección de Tecnología copia en medio removible con un resumen de las operaciones realizadas a través de los diferentes canales; este medio es enviado a custodia externa.	100%	Se observó que los dispositivos de seguridad que protegen el portal del ICETEX almacenan registros de las direcciones IP que realizan conexiones teniendo en cuenta que el portal redirecciona al portal transaccional PSE . La plataforma la administra el contratista Level 3.
3.3.5	Conservar todos los soportes y documentos donde se hayan establecido los compromisos, tanto de las entidades como de sus clientes y las condiciones bajo las cuales éstas prestarán sus servicios. Se debe dejar evidencia documentada de que los clientes las han conocido y aceptado. Esta información deberá ser conservada por lo menos por dos (2) años, contados a partir de la fecha de terminación de la relación contractual o en caso de que la información sea objeto o soporte de una reclamación o queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.	SI	En las carpetas de beneficiarios se almacena la información de los compromisos y condiciones de prestación de servicios. Para los créditos se registra información de: solicitud, recibo de pago de servicio público, afiliación al Sisben, deudores solidarios, pagaré, solicitud de renovación, certificados de notas. Cuando el crédito se otorga por medio de un fondo y se condona la deuda, debe haber información del trabajo de grado y una carta para condonación. Existe un sistema de gestión documental (Mercurio), que tiene modulo de archivo (gestión, central, títulos valores y carpetas de beneficiarios). En el modulo de títulos valor hay información de créditos educativos, los cuales están digitalizados a partir del año 2008; se busca digitalizar los créditos vigentes. El archivo central y los títulos valores están en custodia de un tercero (Datafile), certificado en las normas de calidad (ISO 9001) y seguridad de la información (ISO 27001) con presencia en todas las regionales, garantizando el traslado de información a Bogotá; el supervisor de dicho contrato hace visitas trimestrales a las instalaciones del outsourcing y se genera un informe que reposa en expediente único de contratista. El proveedor recoge la documentación utilizando tulas y precintos de seguridad, se pronuncia por audio y video la relación de la documentación recogida y la grabación se guarda por un mes. Data File es usuario del sistema C&CTEX e Icetex es usuario de sistema envío a custodia de Datafile en donde se relacionan los títulos.	100%	Se evidencio que el Icetex cuenta con el contrato de prestación de servicios 2014-0325 que comprende la administración del archivo central, los archivos de gestión y la administración y custodia de los títulos valores derivados de las operaciones de crédito educativo que otorgue el ICETEX, así mismo la administración de las carpetas de beneficiarios del ICETEX El ICETEX se rige por las normas que en materia archivística expide el Archivo General de la Nación quien es el ente regulador de la archivística del país. Para conservar la información el Icetex maneja las tablas de retención documental las cuales son listados de Grupos de Documentos que tienen características similares con sus respectivos tiempos de retención en cada una de las fases de archivo.
3.3.6	Llevar un registro de las consultas realizadas por los funcionarios de la entidad sobre la información confidencial de los clientes, que contenga al menos lo siguiente: identificación del funcionario que realizó la consulta, canal utilizado, identificación del equipo, fecha y hora. En desarrollo de lo anterior, se deberán establecer mecanismos que restrinjan el acceso a dicha información, para que solo pueda ser usada por el personal que lo requiera en función de su trabajo.	SI	La información confidencial de clientes está en las bases de datos y varios de los perfiles pueden consultar información confidencial de los clientes (beneficiarios).	40%	No se evidenció registro de consultas sobre la información confidencial de los beneficiarios. Respecto a los mecanismos de restricción al acceso de la información, se observó el procedimiento Asignación / Retiro de accesos a sistemas de información que tiene como objetivo administrar de manera segura la asignación o retiro de los diferentes usuarios a las diferentes aplicaciones y sistemas de información con que cuenta el ICETEX
3.3.7	Llevar el registro de las actividades adelantadas sobre los dispositivos finales a cargo de la entidad, usados en los canales de distribución de servicios, cuando se realice su alistamiento, transporte, mantenimiento, instalación y activación.	SI	Se evidenciaron los formatos relacionados con el acta de salida de equipo y el check list de alistamiento de equipo, pero no se logro evidenciar su aplicación.	30%	No se evidenció registro de acceso al Data Center por cuanto se encuentra en las instalaciones del contratista Level3. El contratista incluye los reportes de acceso en los informes mensuales de gestión (bitácoras, planillas de control de acceso).

REQUERIMIENTOS MINIMOS DE SEGURIDAD					
Numeral Circular	Actividad	Aplica?	Respuesta Oficina de Riesgos	Estado implementado	Verificación Oficina de Control Interno
3.3.9	Grabar las llamadas realizadas por los clientes a los centros de atención telefónica cuando consulten o actualicen su información.	SI	Se evidencio el archivo de audio el cual corresponde al registro del servicio prestado al cliente por medio telefónico; además, se observo el archivo de relación de llamadas el cual corresponde al registro documental del archivo de audio generado en la atención al cliente.	50%	Se evidenció que las grabaciones son entregadas en la factura del contratista SERLEFIN para su verificación. No se evidenció la grabación de llamadas con el contratista Contact Center Americas en la sede de cobranzas. Se observó que mediante contrato 2012-0467 con la firma SERLEFIN dentro de los requerimiento mínimos de atención Contact Center el contratista realiza la grabación y registro del 97% de las llamadas atendidas o realizadas Este registro incluye toda la información relacionada con la llamada, como hora, fecha, duración, ANI y DNI entre otras.
3.3.10	La información a que se refieren los numerales 3.3.1, 3.3.6 y 3.3.9 deberá ser conservada por lo menos por dos (2) años. En el caso en que la información respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto	SI	Los logs del aplicativo C&CTEX se conservan en su totalidad desde que fueron implementados en el año 2012. Se ha efectuado un plan de capacidad sobre la base de datos, previendo el crecimiento de la operación y el mantenimiento de los logs. De manera adicional, se envían a custodia externa los medios que contienen el resumen generado mensualmente con las operaciones realizadas a través de los diferentes canales que el ICETEX pone a disposición de los usuarios.	100%	Se evidencio que el Icetex cuenta con el contrato de prestación de servicios 2014-0325 que comprende la administración del archivo central, los archivos de gestión y la administración y custodia de los títulos valores derivados de las operaciones de crédito educativo que otorgue el ICETEX, así mismo la administración de las carpetas de beneficiarios del ICETEX El ICETEX se rige por las normas que en materia archivística expide el Archivo General de la Nación quien es el ente regulador de la archivística del país. Para conservar la información el Icetex maneja las tablas de retención documental las cuales son listados de Grupos de Documentos que tienen características similares con sus respectivos tiempos de retención en cada una de las fases de archivo.
Divulgación de Información					
Obligaciones por Tipo de Canal					
Oficinas					
4.1.1	Los sistemas informáticos empleados para la prestación de servicios en las oficinas deben contar con soporte por parte del fabricante o proveedor	SI	No se logro evidenciar el requisito del numeral.	60%	La Dirección de Tecnología informa que los sistemas informáticos están soportados por contratos de soporte y mantenimiento por parte de los proveedores, sin embargo no fue posible evidenciarlos.
4.1.2	Los sistemas operacionales de los equipos empleados en las oficinas deben cumplir con niveles de seguridad adecuados que garanticen protección de acceso controlado.	SI	El Icetex cuenta con la herramienta WSUS (Gestor de parches) para hacer las actualizaciones del sistema operativo Windows; la Dirección de Tecnología lleva a cabo 2 brigadas al año en las cuales se revisan equipos. De manera adicional, la herramienta Aranda reporta el inventario de software instalado. Cada dos (2) meses se hace escaneo de vulnerabilidades a los equipos de escritorio, con la herramienta McAfee Vulnerabiliy manager y, de manera paralela, existe un comité de análisis de vulnerabilidades que sesiona cada dos meses, dejando actas de comité y cifras de remediación de vulnerabilidades.	40%	Se evidenció que se encuentran implementadas políticas de seguridad a nivel de dominio, antivirus, ips(cliente), WSUS (Gestor de parches) actualización de vulnerabilidades de Windows. Actualmente se hacen escaneo de vulnerabilidad a una muestra de los distintos activos de información. Se verifico el reporte de vulnerabilidades, sin embargo se evidenciaron vulnerabilidades identificadas que a la fecha no se han cerrado.
4.1.3	Contar con cámaras de video, las cuales deben cubrir al menos el acceso principal y las áreas de atención al público. Las imágenes deberán ser conservadas por lo menos ocho (8) meses o en el caso en que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto	SI	En las instalaciones del Icetex en Bogotá hay un centro de monitoreo en donde se tiene control de cámaras y se realiza la grabación de las mismas. Un contratista hace mantenimiento del sistema y hace el monitoreo. Así mismo atiende el acceso a la Dirección de Tesorería. El sistema almacena 6 meses de grabaciones. A nivel nacional, algunas sedes cuentan con cámaras de los servicios de vigilancia prestado en cada edificio donde funcionan sus instalaciones. Se ha propuesto un proyecto para establecer este tipo de controles en todas las regionales, junto con puntos de alarma.	40%	En visita realizada al cuarto de monitoreo en la sede principal, se evidenció que el ICETEX cuenta con un sistema de vigilancia que abarca 4 Dispositivos de grabación (DVR) cada uno con 16 cámaras de las cuales 3 cubren el área de atención al público y 2 el área de recepción, este sistema es monitoreado constantemente por personal especializado (Contrato 2016-107). Se observó que el DVR que soporta las cámaras del área de atención al usuario realiza grabaciones durante 314 días, tiempo en el cual se sobrescribirá la información por cuanto no se evidencio un procedimiento de copia de seguridad. De la misma manera se observó que el sistema de monitoreo no cubre la sala de conferencias, la sede alterna de cobranza ni los puntos de atención a nivel nacional.
4.1.4	Disponer de los mecanismos necesarios para evitar que personas no autorizadas atiendan a los clientes o usuarios en nombre de la entidad	SI	Para evitar que personas no autorizadas atiendan a los clientes se cuenta con controles de acceso físico a las instalaciones de atención, controles de acceso lógico a los equipos de computo y controles de acceso lógico a las aplicaciones relacionadas con la atención directa al cliente.	100%	El ICETEX tiene contratado por outsorcing, la prestación de servicios para la atención del usuario a nivel nacional el cual comprende los siguientes canales: Atención Contact Center, Atención Virtual, Atención Chat, Atención personalizada, Atención escrita, Atención PBX y Atención de grandes clientes.

REQUERIMIENTOS MINIMOS DE SEGURIDAD					
Numeral Circular	Actividad	Aplica?	Respuesta Oficina de Riesgos	Estado Implementado	Verificación Oficina de Control Interno
4.1.5	La información que viaja entre las oficinas y los sitios centrales de las entidades deberá estar cifrada usando hardware de propósito específico, o software, o una combinación de los anteriores. Para los Establecimientos de Crédito el hardware o software empleados deberán ser totalmente separados e independientes de cualquier otro dispositivo o elemento de procesamiento de información, de seguridad informática, de transmisión y/o recepción de datos, de comunicaciones, de conmutación, de enrutamiento, de gateways, servidores de acceso remoto (RAS) y/o de concentradores. En cualquiera de los casos anteriores se deberá emplear cifrado fuerte. Las entidades deberán evaluar con regularidad la efectividad y vigencia de los mecanismos de cifrado adoptados	SI	La red nacional del Icetex es un canal MPLS; hay canales principales y backups (provistos por un tercero). Los servicios son provistos en Bogotá y las regionales se conectan. Sin embargo, no se han establecido las condiciones de cifrado con los terceros.	80%	Se observó que el Icetex cuenta con hardware y software de propósito especifico para proteger la información, se evidencio la configuración de redes privadas virtuales con terceros. Para transferencia de archivos la herramienta Go Anywhere automatización de recaudos y transferencia segura de información según requerimiento de las áreas. No se evidenció documentación.
4.1.6	Establecer procedimientos necesarios para atender de manera segura y eficiente a sus clientes en todo momento, en particular cuando se presenten situaciones especiales tales como: fallas en los sistemas, restricciones en los servicios, fechas y horas de mayor congestión, posible alteración del orden público, entre otras, así como para el retorno a la normalidad. Las medidas adoptadas deberán ser informadas oportunamente a los clientes y usuarios	SI	Existe un procedimiento de recuperación ante desastres, el cual se encuentra en revisión. Actualmente se cuenta con replicación de las bases de datos entre el Datacenter principal y un servidor en las instalaciones del Icetex y se espera tener contar con un Datacenter alterno, con el cual haya replicación con el Datacenter principal. Este procedimiento pretender cumplir con los tiempos que establece el BIA realizado para los procesos misionales de la entidad. Así mismo, existen políticas y procedimiento de backups; los medios se envían a custodia externa (MTI). El procedimiento de gestión de backups contempla pruebas de restauración, de las cuales se han definido unas básicas y algunas aleatorias; queda registro de resultados de las pruebas de recuperación las cuales son registradas en el informe mensual del Datacenter externo. De manera adicional, se cuenta con un servicio de mesa de ayuda para atender casos de soporte, a nivel nacional. Existe un procedimiento de soporte de infraestructura que los contratistas deben acoger, el cual contempla ANS de cumplimiento. En las regionales hay atención remota y personas en sitio; el segundo y tercer nivel de atención se lleva a cabo en Bogotá. Para la atención remota se requiere la aprobación del usuario, quien puede retomar control de su equipo, cuando lo desee. En Bogotá se cuenta con planta eléctrica con los mantenimientos y revisiones establecidos; sin embargo, en las otras ciudades, donde se hace presente el Icetex se esta revisando la contingencia a nivel físico.	40%	Se observó que el ICETEX tiene implementado un Plan de Continuidad de Negocio para responder a eventos que interrumpan la operación normal y que pueden llegar a generar impactos en el logro de los objetivos. De la misma manera los terceros contratados deben garantizar planes de recuperación de desastres (DRP) y planes de contingencia para los servicios ofrecidos. Sin embargo las oficinas territoriales no se encuentran incluidas dentro del plan de continuidad.
4.6.2	Permitir transferir la llamada a un operador, al menos en los horarios hábiles de atención al público	SI	Se efectúan la transferencia de llamada del PBX al Contact Center; de igual manera, los correos electrónicos de usuarios donde piden información se transfieren al proveedor (Serlefin) para que sean respondidos.	100%	Dentro de las actividades de prestación de servicios para el correcto desarrollo de la operación de atención del usuario se encuentra la transferencia de llamadas.
4.7.1	Destinar un área dedicada exclusivamente para la operación de los recursos necesarios en la prestación del servicio, la cual deberá contar con los controles físicos y lógicos que impidan el ingreso de personas no autorizadas, así como la extracción de la información manejada	SI	El proveedor de servicios de atención al usuario (Serlefin) indica que ha destinado un área dedicada para la operación del servicio de Contac Center, ubicada en una de sus instalaciones con los controles de acceso físicos y lógicos para evitar el ingreso de personas no autorizadas a las instalaciones y a la infraestructura tecnológica desde la cual se presta el servicio, así como la divulgación de la información manejada. Se realizará una verificación de estas condiciones.	100%	Se verificó que el ousorcing de atención al usuario tiene un espacio dedicado en sus instalaciones para el servicio de Contact Center
Internet Icetex					

REQUERIMIENTOS MINIMOS DE SEGURIDAD					
Numeral Circular	Actividad	Aplica?	Respuesta Oficina de Riesgos	Estado Implementado	Verificación Oficina de Control Interno
4.9.1	Implementar los algoritmos y protocolos necesarios para brindar una comunicación segura	SI	En el módulo de autenticación para los clientes se utilizan los protocolos "HTTPS" y "SSL", se toma la información del saldo de la obligación y dicha información se entrega a PSE (Pagos Seguros en Línea) cifrada, utilizando un hash con un algoritmo provisto por la plataforma de pagos. La operación posterior es realizada por PSE y la entidad bancaria. De acuerdo con el paso en que vaya la operación, existe un sistema de actualización de estados. Durante la implementación del proyecto hubo revisión por parte de expertos de PSE y de Bancolombia. Se debe revisar la documentación correspondiente a la implementación del proyecto de pagos en línea.	80%	La Dirección de Tecnologia informa que el portal del Icetex cuenta con un certificado digital que expide la firma Certicamara S.A Este certificado asegura que ningún otro sitio web puede suplantar la identidad del servidor original. Constituye una modalidad e identificación electrónica que vincula a la entidad a claves que pueden utilizarse para el cifrado y rubrica de información digital. Adicionalmente se evidencio la renovación de certificados digitales así: Contrato 2015-041 Certificado digital que permite por un año validar el correo electrónico institucional al ingresar desde la página web del ICETEX como sitio seguro, permitiendo realizar transacciones por medio de protocolos https. Contrato 2015-042 Un certificado digital de SSL (Secure Site Pro con Ev) o servidor seguro tipo perdona jurídica por un periodo de dos (2) AÑOS Contrato 2015-0065 Renovación de 3 certificados digitales (Dispositivo Seguro Token) correspondientes a las firmas del Presidente, Vicepresidente Financiero y Director de Contabilidad para efectos de comunicación y envío de información a la SFC y demás entidades públicas que requieran transmisión de documentos con firma digital. Se evidencio que NO hay certificados digitales para las aplicaciones y no se encuentran activa la conexión segura (HTTPS) para algunas aplicaciones. De la misma manera se evidenciaron aplicaciones que tienen activas las conexiones seguras y no seguras.
4.9.4	Establecer el tiempo máximo de inactividad, después del cual se deberá dar por cancelada la sesión, exigiendo un nuevo proceso de autenticación para realizar otras operaciones.	SI	El tiempo de inactividad en el portal web del Icetex se ha establecido en 20 minutos, al cabo de los cuales el usuario debe autenticarse nuevamente.	100%	Se verificó que los enlaces a las aplicaciones que tiene disponibles en el Icetex tienen implementadas políticas de autenticación cuando se presenta inactividad
4.9.5	Informar al cliente, al inicio de cada sesión, la fecha y hora del último ingreso a este canal.	SI	Al inicio de cada sesión se informa al cliente la fecha y hora del último ingreso.	100%	Se verificó en el portal en la opción Consultar estado de cuenta la fecha y hora del ultimo ingreso
4.9.6	Implementar mecanismos que permitan a la entidad financiera verificar constantemente que no sean modificados los enlaces (links) de su sitio Web, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS.	SI	En la página web el sistema de monitoreo que informa las modificaciones a nivel de estructura del home de la pagina web; de manera adicional, el gestor de contenidos cuenta con logs de control de cambios. En relación con el certificado digital no se usan herramientas de verificación; sin embargo, se verifica su autenticidad de manera manual y el proveedor del certificado (Certicámara), por medio de un proveedor envía un informe periódico de escaneos del portal web donde se consideran los certificados digitales. El servicio de DNS público depende de un proveedor y no se tiene certeza de la validación que realiza sobre posibles modificaciones no autorizadas en la resolución de dichos DNS.	80%	La Dirección de Tecnologia informa que el portal del Icetex cuenta con un certificado digital que expide la firma Certicamara S.A Este certificado asegura que ningún otro sitio web puede suplantar la identidad del servidor original. Constituye una modalidad e identificación electrónica que vincula a la entidad a claves que pueden utilizarse para el cifrado y rubrica de información digital Adicionalmente se evidencio la renovación de certificados digitales así: Contrato 2015-041 Certificado digital que permite por un año validar el correo electrónico institucional al ingresar desde la página web del ICETEX como sitio seguro, permitiendo realizar transacciones por medio de protocolos https. Contrato 2015-042 Un certificado digital de SSL (Secure Site Pro con Ev) o servidor seguro tipo perdona jurídica por un periodo de dos (2) AÑOS Contrato 2015-0065 Renovación de 3 certificados digitales (Dispositivo Seguro Token) correspondientes a las firmas del Presidente, Vicepresidente Financiero y Director de Contabilidad para efectos de comunicación y envío de información a la SFC y demás entidades públicas que requieran transmisión de documentos con firma digital. Se evidencio que NO hay certificados digitales para las aplicaciones y no se encuentran activa la conexión segura (HTTPS) para algunas aplicaciones. De la misma manera se evidenciaron aplicaciones que tienen activas las conexiones seguras y no seguras.
4.9.7	Contar con mecanismos para incrementar la seguridad de los portales, protegiéndolos de ataques de negación de servicio, inyección de código malicioso u objetos maliciosos, que afecten la seguridad de la operación o su conclusión exitosa	SI	La entidad cuenta con IPS, firewall y un filtro tipo request en el servidor IIS 7.5. Se realizan revisiones manuales de logs del portal web dos (2) veces por semana y se verifican los comportamientos del software monitoreo, con el fin de verificar estos tipos de ataques. Para evitar la negación del servicio se cuenta con una política en el IPS, la cual aún no se ha puesto a prueba. El portal web se compone de dos (2) los cuales se encuentran fisicamente en otro Datacenter y son administrados y asegurados por un tercero, según lineamientos del Icetex. Se realizó un hacking ético externo sobre direcciones criticas del portal y se encontraron algunos hallazgos de las vulnerabilidades Cross Site Scripting - XSS y SQL Injection sobre aplicativos: se recomendó migrar estos aplicativos a tecnologías mas actuales.	80%	Se observó que la Dirección de Tecnología tiene implementado IPS, Firewall (4) y el servicio Web Application Firewall (WAF) el cual protege 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 ,Se evidenció que este servicio lo administra el contratista Level 3 (contrato de prestación de servicios No.004-2015).
Reglas sobre Actualización de Software					

REQUERIMIENTOS MINIMOS DE SEGURIDAD					
Numeral Circular	Actividad	Aplica?	Respuesta Oficina de Riesgos	Estado Implementado	Verificación Oficina de Control Interno
5.1	Mantener tres ambientes independientes: uno para el desarrollo de software, otro para la realización de pruebas, y un tercer ambiente para los sistemas en producción. En todo caso, el desempeño y la seguridad de un ambiente no podrá influir en los demás.	SI	Se cuenta con cuatro (4) ambientes para los aplicativos: el ambiente de desarrollo en el sitio de trabajo de los proveedores. En Icetex existen los ambientes de pruebas, contingencia y producción. Se accede con credenciales distintas a los ambientes; en casos aislados los desarrolladores acceden a ambientes de pruebas.	100%	Se verificó que la Dirección de Tecnología tiene implementados los ambientes de desarrollo prueba y producción el ambiente de desarrollo se encuentra a cargo del contratista (UT GGT INFORMATICA STEFANINI contrato 2015-0292). El ambiente de pruebas se encuentra en un servidor de la Entidad (10.1.4.51) en la sede principal. El ambiente de producción esta a cargo del contratista Level 3 (Contrato No.004-2015).
5.2	Implementar procedimientos que permitan verificar que las versiones de los programas del ambiente de producción corresponden a las versiones de programas fuentes catalogadas.	SI	Existe un procedimiento de control de versiones de programas fuentes para el aplicativo C&CTEX; existe también un formato de catalogaciones, tanto ordenes de catalogación para software nuevo como ajustes a la base de datos. La entidad cuenta con un tablero de control (administrado por el asistente de la Dirección de Tecnología), el cual se revisa periódicamente y se busca consistencia con la Oficina de Riesgos; el formato de catalogaciones significan un paso a producción.	70%	Se evidenció el Procedimiento Catalogación en el sistema de gestión de calidad. La Dirección de Tecnología informa que las versiones de los programas fuentes se realiza a traves de la aplicación Microsoft TEAM FOUNDATION SERVER. Se tiene un servidor exclusivo para la aplicacion y es administrada por un analista del área de tecnologia, sin embargo no se presento evidencia de documentación.
5.3	Cuando las entidades necesiten tomar copias de la información de sus clientes para la realización de pruebas, se deberán establecer los controles necesarios para garantizar su destrucción, una vez concluidas las mismas	SI	Se adquirió la herramienta de enmascaramiento de datos Oracle Datamasking dentro del contrato de renovación tecnológica de la entidad. La Dirección de Tecnología analizó la información de las bases de datos mas críticas que se debe enmascarar inicialmente y el proveedor va a apoyar la configuración de la herramienta y capacitará a los funcionarios designados del Icetex para administrar y ser usuarios de la herramienta.	70%	La Dirección de Tecnología informa que la destrucción de la información para la realización de pruebas se realiza cada 15 días, no obstante no se evidenció un procedimiento formal ni documentación relacionada. Se observó en el Manual de Políticas de Seguridad de la Información. "..POLÍTICA PARA LA PROTECCION DE LOS DATOS DE PRUEBA La Dirección de Tecnología del ICETEX protegerá los datos de prueba que se entregarán a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción. Numeral 16.3.1. Normas para la protección de los datos de prueba Normas dirigidas a: DIRECCION DE TECNOLOGIA v La Dirección de Tecnología debe certificar que la información a ser entregada a los desarrolladores para sus pruebas será enmascarada y no revelará información confidencial de los ambientes de producción. La Dirección de Tecnología debe eliminar la información de los ambientes de pruebas, una vez estas han concluido...."
5.4	Contar con procedimientos y controles para el paso de programas a producción. El software en operación deberá estar catalogado.	SI	Existe un procedimiento de control de cambios, soportado por un formato de solicitud de cambios, una orden de catalogación y acta de catalogación, cuando se trata de cambios sobre los aplicativos. En la Dirección de Tecnología se lleva a cabo un Comité de Cambios una vez los requerimientos han sido aprobados por la Oficina de Riesgos.	100%	Se evidenció en el sistema de gestión de calidad los procedimientos Control de cambios y Catalogación. En la Dirección de Tecnología se realiza un Comité de Cambios.
5.5	Contar con interfaces para los clientes o usuarios que cumplan con los criterios de seguridad y calidad, de tal manera que puedan hacer uso de ellas de una forma simple e intuitiva	SI	Los clientes de Icetex realizan sus solicitudes y efectúan sus tramites ante la entidad a través del portal web, entre ellos el proceso de inscripción y consulta de sus créditos. Las personas que acuden a otros canales lo hacen por situaciones específicas; aun así, en caso de tener dudas sobre el uso del portal web pueden solicitar soporte utilizando los canales dispuestos para tal fin.	100%	Se observó que los usuarios del Icetex realizan los tramites a traves del portal Web, y el canal de Contact Center
5.6	Mantener documentada y actualizada, al menos, la siguiente información: parámetros de los sistemas donde operan las aplicaciones en producción, incluido el ambiente de comunicaciones; versión de los programas y aplicativos en uso; soportes de las pruebas realizadas a los sistemas de información; y procedimientos de instalación del software.	SI	La entidad cuenta con la documentación del servidor web como manual de instalación y configuración del ambiente web (usuarios, permisos, variables, gestor de contenido, conexiones a bases de datos). La documentación de las versiones en producción no se encuentra actualizada, aunque se documentan los controles de cambios; se dispone de documentación de cambio de versión en el portal web del proveedor. Se realizan pruebas funcionales en cada uno de los módulos del gestor de contenidos; sin embargo, dichas pruebas no quedan documentadas formalmente. En el caso de los desarrollos web in-house (realizados por terceros) se cuenta con control de cambios, control de versiones, pruebas con su respectiva documentación y ordenes de catalogación (procedimiento de instalación). De manera adicional, el Icetex cuenta con un software de control de versiones, existen hojas de vida de los recursos tecnológicos, bases de datos y aplicaciones, se cuenta con manuales de instalación de plataforma.	40%	La Dirección de Tecnología informa que se encuentra documentada la información de todos los servidores, sin embargo no se evidenció dicha documentación. Se evidenció el Procedimiento Catalogación en el sistema de gestión de calidad. La Dirección de Tecnología informa que las versiones de los programas fuentes se realiza a través de la aplicación Microsoft TEAM FOUNDATION SERVER. Se tiene un servidor exclusivo para la aplicación y es administrada por un analista del área de Tecnología, sin embargo no se evidencio documentación.
Análisis de Vulnerabilidades					

REQUERIMIENTOS MINIMOS DE SEGURIDAD					
Numeral Circular	Actividad	Aplica?	Respuesta Oficina de Riesgos	Estado implementado	Verificación Oficina de Control Interno
7.1	Estar basado en un hardware de propósito específico (appliance) totalmente separado e independiente de cualquier dispositivo de procesamiento de información, de comunicaciones y/o de seguridad informática.	SI	El Icetex cuenta con el appliance McAfee Vulnerabiliy Manager, dedicado para la ejecución y escaneo de vulnerabilidades en la plataforma tecnológica de la entidad. Al interior de la Dirección de Tecnología se realizan alrededor de 5 o 6 pruebas de vulnerabilidades al año, cubriendo toda la red de datos. De manera adicional, se han hecho pruebas de hacking ético los dos últimos años con periodicidad anual, las ultimas de ellas en el año 2013, especificas para objetivos determinados. Existe un procedimiento y formato de plan de mejoramiento de auditorías en donde se registran los hallazgos de las pruebas de hacking; el plan de mejoramiento debe culminar el primer semestre del año en curso.	80%	La Dirección de Tecnología cuenta con una herramienta de escaneo de vulnerabilidades en los servidores y aplicaciones Web. Estos escaneos se realizan por el contratista de seguridad de la información (Level 3 contrato No.004-2015) y por el contratista de seguridad de la información (Digiware) Se evidenció un reporte de escaneo de vulnerabilidades sobre los equipos, y la gestión que realiza el contratista de seguridad. Se observó que se efectúa un comité de análisis de vulnerabilidades en el cual se efectúan actividades de identificación y mitigación de vulnerabilidades, con participación del contratista de seguridad y la Dirección de Tecnología de ICETEX. Sin embargo se evidenció que no se cierran oportunamente las vulnerabilidades.
7.2	Generar de manera automática por lo menos dos (2) veces al año un informe consolidado de las vulnerabilidades encontradas. Los informes de los últimos dos años deberán estar a disposición de la SFC.	SI	Se llevan a cabo mas de dos (2) escaneos de vulnerabilidades al año con el appliance McAfee Vulnerabiliy Manager y se cuenta con los informes de los últimos dos (2) años. Existe un Comité de Vulnerabilidades el cual sesiona bimensualmente y allí se evalúan los resultados de las pruebas de vulnerabilidad. Se conservan los registros de todas las pruebas y los informes generados por el appliance.	90%	Se evidenció un reporte de escaneo de vulnerabilidades de febrero de 2016 sobre los equipos, y la gestión que realiza el contratista de seguridad. Los informes se encuentran en custodia la Oficina de Riesgos y el area de Tecnología, sobre los cuales no tuvo acceso la Auditoría.
7.3	Las entidades deberán tomar las medidas necesarias para remediar las vulnerabilidades detectadas en sus análisis.	SI	El Comité de Vulnerabilidades define la prioridad de tratamiento de las vulnerabilidades y genera actas de comité y planes de mejoramiento para remediación de las vulnerabilidades detectadas durante los escaneos de vulnerabilidades; a cada plan se le hace seguimiento en el mismo comité. Cuando es necesario se generan controles de cambio como parte de los actividades de remediación. La Revisoría Fiscal evalúa la realización de pruebas de vulnerabilidades y piden documentación de la gestión de vulnerabilidades.	80%	Se observó un acta del comité de análisis de vulnerabilidades en el cual se realizan actividades de identificación y mitigación de vulnerabilidades en el cual participan el contratista de seguridad y la Dirección de Tecnología de ICETEX. Sin embargo se evidencio que no se cierran oportumnamente las vulnerabilidades. Se observó que la Oficina de Riesgos a través del contratista de seguridad de la información tiene un plan de monitoreo de vulnerabilidades el cual controla la resolución de vulnerabilidades
7.4	Realizar un análisis diferencial de vulnerabilidades, comparando el informe actual con respecto al inmediatamente anterior.	SI	El appliance McAfee Vulnerabiliy Manager genera varios informes y el Asesor de Seguridad Informática los consolida y, a partir de la información arrojada por éste genera un informe ejecutivo; apartes del informe ejecutivo quedan en el acta del Comité de Vulnerabilidades. En el informe ejecutivo se presenta el análisis diferencial.	40%	La Dirección de Tecnología informa que se genera un reporte para determinar las vulnerabilidades que permanecen y cuales estan mitigadas. Sin embargo no se evidencio soporte del diferencial. La Oficina de Riesgos a través del contratista Digiware tiene esta actividad asignada.
7.5	Las herramientas usadas en el análisis de vulnerabilidades deberán estar homologadas por el CVE (Common Vulnerabilities and Exposures) y actualizadas a la fecha de su utilización.	SI	El appliance utilizado para los análisis de vulnerabilidades actualiza sobre su base de datos las actualización de CVE (Common Vulnerabilities and Exposures) y CVSS (Common Vulnerabiliy Scoring System) y genera informes a partir de dichos códigos. Por parte de la firma que efectúa las pruebas de Ethical Hacking se usa la herramienta Nessus homologada por el CVE, información dada por el Consultor Dixon Camacho en dic de 2015	100%	Se evidenció que la herramienta de escaneo de vulnerabilidades se encuentra homolagada. Se verifico reporte del contratista de seguridad de la información de la Oficina de Riesgos.
7.6	Para la generación de los informes solicitados se deberá tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre (www.mitre.org)	SI	Se utilizan los nombres provistos por CVE y CVSS en los informes de las pruebas de vulnerabilidades. En la descripcion de cada vulberabilidad en el informe de Ethical Hacking está el CVE cuando aplica, información dada por el Consultor Dixon Camacho en dic de 2015	100%	Se evidenció que la herramienta de escaneo de vulnerabilidades se encuentra homologada. Se verifico reporte del contratista des seguridad de la información de la Oficina de Riesgos.

AREA : _____ FECHA DILIGENCIAMIENTO FORMATO: _____

PROCESO	HALLAZGO/OBSERVACION	ACCIONES DE MEJORAMIENTO	FECHA DE INICIO DE LA ACCIÓN	FECHA DE FINALIZACIÓN DE LA ACCIÓN	RESPONSABLE
	Numeral 3.1.2 Se observó que el Icetex suscribió los contratos 2015-0074 y 2016-051 - cuyo objeto es el de implementar el modelo de seguridad y privacidad de la información de la estrategia de gobierno en línea el cual esta alienado con la norma ISO 27001, a la fecha se evidenciaron las siguientes actividades: • Planeación de modelo de seguridad y privacidad de la información de la Estrategia de Gobierno en línea. • Gestión de riesgos de seguridad de la información (50% de ejecución) . • Inventario y clasificación de activos de información (100 %). Es de señalar que el ICETEX no ha implementado la transición del protocolo IPv4 IPv6, requerido para dar cumplimiento a la etapa de DIAGNOSTICO – PLANIFICACION del Modelo de seguridad y privacidad de la Estrategia de Gobierno en Línea (GEL).				
	Numeral 3.1.3 El área de Tecnología mediante el contrato de prestación de servicios 004 2015 con la firma Level 3 implementa los mecanismos de seguridad del Instituto (Ej. Tesoreria - Recaudos), sin embargo NO se evidenció un procedimiento formal para realizar dicha actividad, ni los activos de información que se encuentran protegidos.				
	Numeral 3.1.4 La Dirección de Tecnología informa que se realiza aseguramiento a nivel del servidor de bases de datos mediante la reducción de vulnerabilidades. Se evidenció reporte de escaneo de vulnerabilidades (verificación de seguridad a los recursos informáticos, mediante el análisis de los puertos abiertos en toda la red, que permite identificar los riesgos de seguridad, además identifica las debilidades del sistema operativo o de software de aplicación- Procedimiento Pruebas de Vulnerabilidad en el sistema de gestión de calidad.), se observó acta de comite de vulnerabilidades en la cual se realiza análisis y tratamiento de las mismas, sin embargo los reportes evidencian que existen vulnerabilidades que siguen sin resolverse desde el año 2014 .				
	Numeral 3.1.5 Se verificó la instalación de la suite de McAfee (Contrato 2014-0148) en los equipos de computo 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.no se evidencio la actualización ni documentación de la plataforma teniendo en cuenta que el contrato fue suscrito con fecha 24 de enero de 2014.				
	Numeral 3.1.6 Se observaron políticas de contraseñas en los sistemas de información críticos del ICETEX (Complejidad, longitud minima , caducidad, etc.). Sin embargo se evidencio una aplicacion que **No** tiene cifradas las contraseñas en el módulo de admisnitración de ususarios. Se observó que existen procedimientos y guias relacionados a los accesos a los sistemas de información: MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN • Numeral 11.2.1. Normas de administración de acceso de usuarios • Numeral 11.3.1. Normas de responsabilidades de acceso de los usuarios • Numeral 11.4.1. Normas de uso de altos privilegios y utilitarios de administración SISTEMA DE GESTIÓN DE CALIDAD – In Process • Procedimiento Asignación/Retiro de accesos a sistemas de información • Procedimiento Asignación/Retiro de accesos a sistemas de información IES e IES-ORI • Guía de contraseñas seguras				
	Numeral 3.1.7 Se evidencio que la instalación de software requiere de privlegios de usuario Administrador (Soporte mesa de ayuda). Se evidencio que existe un formato de actualización de software, autorizado por la Oficna de Riesgos y el lider del proceso. Se evidenció que permite la descarga de archivos lo que constituye un riesgo de seguridad .				
	Numeral 3.1.8 La Dirección de Tecnología cuenta en el Portal del ICETEX con Firewall y WAF (Web application Filter), que identifica cadenas de ataques (exploit sobre inyección de cadenas) o conexiones.				

AREA : _____ FECHA DILIGENCIAMIENTO FORMATO: _____

PROCESO	HALLAZGO/OBSERVACION	ACCIONES DE MEJORAMIENTO	FECHA DE INICIO DE LA ACCION	FECHA DE FINALIZACIÓN DE LA ACCIÓN	RESPONSABLE
	Numeral 3.1.10 Se observó que los sistemas de información y el servidor de dominio tienen implementadas políticas de cambio de contraseña. Adicionalmente existen políticas y procedimientos relacionados a los accesos a los sistemas de información: MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN • Numeral 11.2.1. Normas de administración de acceso de usuarios • Numeral 11.3.1. Normas de responsabilidades de acceso de los usuarios • Numeral 11.4.1. Normas de uso de altos privilegios y utilitarios de administración SISTEMA DE GESTIÓN DE CALIDAD – In Process • Procedimiento Asignación/Retiro de accesos a sistemas de información • Procedimiento Asignación/Retiro de accesos a sistemas de información IES e IES-ORI • Guía de contraseñas seguras.				
	Numeral 3.1.11 En la verificación realizada en los equipos de computo, se observó que la instalación de cualquier tipo de software requiere del privilegio de administrador del sistema, que permiten instalar o desinstalar software y/o aplicativos en general. Sin embargo es posible realizar la descarga de los archivos instaladores o ejecutables, lo que constituye un riesgo de seguridad. Mediante el software Aranda se identifica la instalación no autorizada de programas y el administrador de dominio realiza el proceso de desinstalación de software no autorizado, sin embargo no se evidenció que dicho procedimiento se encuentra documentado.				
	Numeral 3.1.12 El servidor de dominio y el sistema de información C&CETEX tienen implementadas políticas que bloquean los usuarios después de un número determinado de intentos fallidos de autenticación (3) y tiempo de desconexión por inactividad a los 5 minutos. Se evidenciaron aplicativos que no tienen implementadas las politicas mencionadas (TAE)				
	Numeral 3.1.14 Se observó que los sistemas de información de misión crítica presentan perfiles de acceso por tipo de usuario y registro de auditoría de las transacciones sensibles. Sin embargo se evidenciaron aplicativos que no tienen definidos perfiles y no generan registros de auditoría.				
	Numeral 3.1.15 Se evidenció el registro de incidentes de seguridad, asi mismo se evidenció acta de comite de revisión de logs de auditoría de los aplicativos de misión crítica. Se observó que no se encuentra implementado registro de auditoría en todas las transacciones sensibles que se relizan a traves de aplicativos de misión crítica.				
	Numeral 3.1.16 La Dirección de Tecnologia informa que la sincronización se realiza con el servidor de la Superintendencia de Industria y Comercio , sin embargo se evidenció que la pagina del instituto Nacional de Metrología reporta que esta entidad es la encargada de mantener, coordinar y difundir la hora legal de la República de Colombia. Se cotejó la hora configurada en el equipo de computo contra la hora registrada en la pagina web del instituno Nacional de Metrologia (www.inm.gov.co) , observándose diferencia contra el sistema de telefonía IP.				
	Numeral 3.1.17 Se evidenció que la Dirección de Tecnología tiene implementadas políticas en los dispositivos de seguridad instalados en la entidad (firewall, IPS, Barracuda de navegación TCP servicio HTTP) que controlan las conexiones servicio y protocolos disponibles para los usuarios autorizados acorde a la características de los servicios.				
	Numeral 3.2.1 Se observó que el Manual de Contratación y el Manual de Políticas de Seguridad de la Información incluyen los aspectos mencionados en los literales a, b, c, d y e en los numerales señalados a continuación. MANUAL DE CONTRATACION Numeral 10. ACUERDOS POR NIVELES DE SERVICIO Numeral 5.2.1 Determinación del objeto, alcance, clase de contrato y cláusulas.				

AREA : _____ FECHA DILIGENCIAMIENTO FORMATO: _____

PROCESO	HALLAZGO/OBSERVACION	ACCIONES DE MEJORAMIENTO	FECHA DE INICIO DE LA ACCIÓN	FECHA DE FINALIZACIÓN DE LA ACCIÓN	RESPONSABLE
	Numeral 3.2.2 Se observó que el Manual de Contratación y el Manual de Políticas de Seguridad de la Información incluyen los aspectos mencionados en los literales a, b, c, d y e en los numerales señalados a continuación. **MANUAL DE CONTRATACION** Numeral 10. ACUERDOS POR NIVELES DE SERVICIO Numeral 5.2.1 Determinación del objeto, alcance, clase de contrato y cláusulas. **MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN** Numeral 9.1.1. Normas relacionadas con la vinculación de funcionarios Numeral 9.3.1. Normas para la desvinculación, licencias, vacaciones o cambios de labores de los funcionarios y personal provisto por terceros Numeral 15.4.1. Normas de intercambio de información Numeral 17.1. POLÍTICA DE INCLUSION DE CONDICIONES DE SEGURIDAD EN LA RELACIÓN CON TERCERAS PARTES Numeral 17.1.1. Normas de inclusión de condiciones de seguridad en la relación con terceras partes Numeral 17.2.1. Normas de gestión de la prestación de servicios de terceras partes" Sin embargo en los manuales no se evidenciaron normas para incluir en los contratos aspectos relacionados con el numeral f) Procedimientos a seguir cuando se encuentre evidencia de alteración o manipulación de dispositivos o información, y g) Procedimientos y controles para la entrega de la información manejada y la destrucción de la misma por parte del tercero una vez finalizado el servicio.				
	Numeral 3.2.3 Se evidencio que le ICETEX incluye en los contratos con terceros un plan de continuidad de negocios. Sin embargo no existen políticas relacionadas al plan de continuidad de negocio en el Manual de seguridad de la información en las políticas que rigen de la relación con terceras partes.				
	Numeral 3.2.4 Se evidencio el documento GUIA DE CARNETIZACION, en el sistema de Gestión de Calidad -In Process- . Se observó que los visitantes le expiden una escarapela para su identificación. se remiten correos electrónicos solicitando el uso obligatorio del carné.				
	Numeral 3.2.5 El área de Tecnología mediante el contrato de prestación de servicios 2015 con la firma Level 3 implementa los mecanismos de seguridad de conformidad a los requerimientos puntuales de las dependencias del Instituto (Ej. Tesoreria - Recaudos), sin embargo NO se evidenció un procedimiento formal para realizar dicha actividad, ni los activos de información que se encuentran protegidos.				
	Numeral 3.3.1 Se observó que los dispositivos de seguridad que protegen el portal del ICETEX almacenan registros de las direcciones IP que realizan conexiones teniendo en cuenta que el portal redirecciona al portal transaccional PSE . La plataforma la administra el contratista Level 3.				
	Numeral 3.3.5 Se evidencio que el Icetex cuenta con el contrato de prestación de servicios 2014-0325 que comprende la administración del archivo central, los archivos de gestión y la administración y custodia de los títulos valores derivados de las operaciones de crédito educativo que otorgue el ICETEX, así mismo la administración de las carpetas de beneficiarios del ICETEX El ICETEX se rige por las normas que en materia archivística expide el Archivo General de la Nación quien es el ente regulador de la archivística del país. Para conservar la información el Icetex maneja las tablas de retención documental las cuales son listados de Grupos de Documentos que tienen características similares con sus respectivos tiempos de retención en cada una de las fases de archivo.				
	Numeral 3.3.6 los beneficiarios. Respecto a los mecanismos de restricción al acceso de la información, se observó el procedimiento Asignación / Retiro de accesos a sistemas de información que tiene como objetivo administrar de manera segura la asignación o retiro de los diferentes usuarios a las diferentes aplicaciones y sistemas de información con que cuenta el ICETEX				

AREA : _____ FECHA DILIGENCIAMIENTO FORMATO: _____

PROCESO	HALLAZGO/OBSERVACION	ACCIONES DE MEJORAMIENTO	FECHA DE INICIO DE LA ACCIÓN	FECHA DE FINALIZACIÓN DE LA ACCIÓN	RESPONSABLE
	Numeral 3.3.7 No se evidenció registro de acceso al Data Center por cuanto se encuentra en las instalaciones del contratista Level3. El contratista incluye los reportes de acceso en los informes mensuales de gestión (bitácoras, planillas de control de acceso).				
	Numeral 3.3.9 Se evidenció que las grabaciones son entregadas en la factura del contratista SERLEFIN para su verificación. No se evidenció la grabación de llamadas con el contratista Contact Center Americas en la sede de cobranzas. Se observó que mediante contrato 2012-0467 con la firma SERLEFIN dentro de los requerimiento mínimos de atención Contact Center el contratista realiza la grabación y registro del 97% de las llamadas atendidas o realizadas Este registro incluye toda la información relacionada con la llamada, como hora, fecha, duración, ANI y DNI entre otras.				
	Numeral 3.3.10 Se evidencio que el Icetex cuenta con el contrato de prestación de servicios 2014-0325 que comprende la administración del archivo central, los archivos de gestión y la administración y custodia de los títulos valores derivados de las operaciones de crédito educativo que otorgue el ICETEX, así mismo la administración de las carpetas de beneficiarios del ICETEX El ICETEX se rige por las normas que en materia archivística expide el Archivo General de la Nación quien es el ente regulador de la archivística del país. Para conservar la información el Icetex maneja las tablas de retención documental las cuales son listados de Grupos de Documentos que tienen características similares con sus respectivos tiempos de retención en cada una de las fases de archivo.				
	Numeral 4.1.1 La Dirección de Tecnología informa que los sistemas informáticos están soportados por contratos de soporte y mantenimiento por parte de los proveedores, sin embargo no fue posible evidenciarlos.				
	Numeral 4.1.2 Se evidenció que se encuentran implementadas políticas de seguridad a nivel de dominio, antivirus, ips(cliente), WSUS (Gestor de parches) actualización de vulnerabilidades de Windows. Actualmente se hacen escaneo de vulnerabilidad a una muestra de los distintos activos de información. Se verifico el reporte de vulnerabilidades, sin embargo se evidenciaron vulnerabilidades identificadas que a la fecha no se han cerrado.				
	Numeral 4.1.3 En visita realizada al cuarto de monitoreo en la sede principal, se evidenció que el ICETEX cuenta con un sistema de vigilancia que abarca 4 Dispositivos de grabación (DVR) cada uno con 16 cámaras de las cuales 3 cubren el área de atención al público y 2 el área de recepción, este sistema es monitoreado constantemente por personal especializado (Contrato 2016-107). Se observó que el DVR que soporta las cámaras del área de atención al usuario realiza grabaciones durante 314 días, tiempo en el cual se sobrescribirá la información por cuanto no se evidencio un procedimiento de copia de seguridad. De la misma manera se observó que el sistema de monitoreo no cubre la sala de conferencias, la sede alterna de cobranza ni los puntos de atención a nivel nacional.				
	Numeral 4.1.4 El ICETEX tiene contratado por outsorcing, la prestación de servicios para la atención del usuario a nivel nacional el cual comprende los siguientes canales: Atención Contact Center, Atención Virtual, Atención Chat, Atención personalizada, Atención escrita, Atención PBX y Atención de grandes clientes.				
	Numeral 4.1.5 Se observó que el Icetex cuenta con hardware y software de propósito especifico para proteger la información, se evidencio la configuración de redes privadas virtuales con terceros. Para transferencia de archivos la herramienta Go Anywhere automatización de recaudos y transferencia segura de información según requerimiento de las áreas. No se evidenció documentación.				
	Numeral 4.1.6 Se observó que el ICETEX tiene implementado un Plan de Continuidad de Negocio para responder a eventos que interrumpan la operación normal y que pueden llegar a generar impactos en el logro de los objetivos. De la misma manera los terceros contratados deben garantizar planes de recuperación de desastres (DRP) y planes de contingencia para los servicios ofrecidos. Sin embargo las oficinas territoriales no se encuentran incluidas dentro del plan de continuidad.				

AREA : _____ FECHA DILIGENCIAMIENTO FORMATO: _____

PROCESO	HALLAZGO/OBSERVACION	ACCIONES DE MEJORAMIENTO	FECHA DE INICIO DE LA ACCIÓN	FECHA DE FINALIZACIÓN DE LA ACCIÓN	RESPONSABLE
	Dentro de las actividades de prestación de servicios para el correcto desarrollo de la operación de atención del usuario se encuentra la				
	Numeral 4.7.1 Se verificó que el ousorcing de atención al usuario tiene un espacio dedicado en sus instalaciones para el servicio de Contact Center				
	ISE-DLP epo de mcafee ISE es una plataforma de control y gestión de				
	Numeral 4.9.1 La Dirección de Tecnologia informa que el portal del Icetex cuenta con un certificado digital que expide la firma Certicamara S.A Este certificado asegura que ningún otro sitio web puede suplantar la identidad del servidor original. Constituye una modalidad e identificación electrónica que vincula a la entidad a claves que pueden utilizarse para el cifrado y rubrica de información digital. Adicionalmente se evidencio la renovación de certificados digitales así: Contrato 2015-041 Certificado digital que permite por un año validar el como sitio seguro, permitiendo realizar transacciones por medio de protocolos https. Contrato 2015-042 Un certificado digital de SSL (Secure Site Pro con Ev) o servidor seguro tipo perdona jurídica por un periodo de dos (2) AÑOS Contrato 2015-0065 Renovación de 3 certificados digitales (Dispositivo Seguro Token) correspondientes a las firmas del Presidente, Vicepresidente Financiero y Director de Contabilidad para efectos de comunicación y envío de información a la SFC y demás entidades públicas que requieran transmisión de documentos con firma digital. Se evidencio que NO hay certificados digitales para las aplicaciones y no se encuentran activa la conexión segura (HTTPS) para algunas aplicaciones. De la misma manera se evidenciaron aplicaciones que tienen activas las conexiones seguras y no seguras.				
	Se verificó que los enlaces a las aplicaciones que tiene disponibles en el Icetex tienen implementadas politicas de autenticación cuando se				
	Se verificó en el portal en la opción Consultar estado de cuenta la fecha y				
	Numeral 4.9.6 La Dirección de Tecnologia informa que el portal del Icetex cuenta con un certificado digital que expide la firma Certicamara S.A Este certificado asegura que ningún otro sitio web puede suplantar la identidad del servidor original. Constituye una modalidad e identificación electrónica que vincula a la entidad a claves que pueden utilizarse para el cifrado y rubrica de información digital Adicionalmente se evidencio la renovación de certificados digitales así: Contrato 2015-041 Certificado digital que permite por un año validar el como sitio seguro, permitiendo realizar transacciones por medio de protocolos https. Contrato 2015-042 Un certificado digital de SSL (Secure Site Pro con Ev) o servidor seguro tipo perdona jurídica por un periodo de dos (2) AÑOS Contrato 2015-0065 Renovación de 3 certificados digitales (Dispositivo Seguro Token) correspondientes a las firmas del Presidente, Vicepresidente Financiero y Director de Contabilidad para efectos de comunicación y envío de información a la SFC y demás entidades públicas que requieran transmisión de documentos con firma digital. Se evidencio que NO hay certificados digitales para las aplicaciones y no se encuentran activa la conexión segura (HTTPS) para algunas aplicaciones. De la misma manera se evidenciaron aplicaciones que tienen activas las conexiones seguras y no seguras.				
	Numeral 5.1 Se verificó que la Dirección de Tecnología tiene implementados los ambientes de desarrollo prueba y producción el ambiente de desarrollo se encuentra a cargo del contratista (UT GGT INFORMATICA STEFANINI contrato 2015-0292). El ambiente de pruebas se encuentra en un servidor de la Entidad (10.1.4.51) en la sede principal. El ambiente de producción esta a cargo del contratista Level 3 (Contrato No.004-2015).				

AREA : _____ FECHA DILIGENCIAMIENTO FORMATO: _____

PROCESO	HALLAZGO/OBSERVACION	ACCIONES DE MEJORAMIENTO	FECHA DE INICIO DE LA ACCIÓN	FECHA DE FINALIZACIÓN DE LA ACCIÓN	RESPONSABLE
	Numeral 5.2 Se evidenció el Procedimiento Catalogación en el sistema de gestión de calidad. La Dirección de Tecnología informa que las versiones de los programas fuentes se realiza a traves de la aplicación Microsoft TEAM FOUNDATION SERVER. Se tiene un servidor exclusivo para la aplicacion y es administrada por un analista del área de tecnologia, sin embargo no se presento evidencia de documentación.				
	Numeral 5.3 La Dirección de Tecnología informa que la destrucción de la información para la realización de pruebas se realiza cada 15 días, no obstante no se evidenció un procedimiento formal ni documentación relacionada. Se observó en el Manual de Políticas de Seguridad de la Información. "..POLÍTICA PARA LA PROTECCION DE LOS DATOS DE PRUEBA La Dirección de Tecnología del ICETEX protegerá los datos de prueba que se entregarán a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción. Numeral 16.3.1. Normas para la protección de los datos de prueba Normas dirigidas a: DIRECCION DE TECNOLOGIA v La Dirección de Tecnología debe certificar que la información a ser entregada a los desarrolladores para sus pruebas será enmascarada y no revelará información confidencial de los ambientes de producción. La Dirección de Tecnología debe eliminar la información de los ambientes de pruebas, una vez estas han concluido...."				
	Se evidenció en el sistema de gestión de calidad los procedimientos Control de cambios y Catalogación. En la Dirección de Tecnología se				
	Numeral 5.5 Se observó que los usuarios del Icetex realizan los tramites a traves del portal Web, y el canal de Contact Center				
	Numeral 5.6 La Dirección de Tecnología informa que se encuentra documentada la información de todos los servidores, sin embargo no se evidenció dicha documentación. Se evidenció el Procedimiento Catalogación en el sistema de gestión de calidad. La Dirección de Tecnología informa que las versiones de los programas fuentes se realiza a través de la aplicación Microsoft TEAM FOUNDATION SERVER. Se tiene un servidor exclusivo para la aplicación y es administrada por un analista del área de Tecnología, sin embargo no se evidencio documentación.				
	Numeral 7.1 La Dirección de Tecnología cuenta con una herramienta de escaneo de vulnerabilidades en los servidores y aplicaciones Web. Estos escaneos se realizan por el contratista de seguridad de la información (Level 3 contrato No.004-2015) y por el contratista de seguridad de la información (Digiware) Se evidenció un reporte de escaneo de vulnerabilidades sobre los equipos, y la gestión que realiza el contratista de seguridad. Se observó que se efectúa un comité de análisis de vulnerabilidades en el cual se efectúan actividades de identificación y mitigación de vulnerabilidades, con participación del contratista de seguridad y la Dirección de Tecnología de ICETEX. Sin embargo se evidenció que no se cierran oportunamente las vulnerabilidades.				
	Numeral 7.2 Se evidenció un reporte de escaneo de vulnerabilidades de febrero de 2016 sobre los equipos, y la gestión que realiza el contratista de seguridad. Los informes se encuentran en custodia la Oficina de Riesgos y el area de Tecnología, sobre los cuales no tuvo acceso la Auditoría.				
	Numeral 7.3 Se observó un acta del comité de análisis de vulnerabilidades en el cual se realizan actividades de identificación y mitigación de vulnerabilidades en el cual participan el contratista de seguridad y la Dirección de Tecnología de ICETEX. Sin embargo se evidencio que no se cierran oportumnamente las vulnerabilidades. Se observó que la Oficina de Riesgos a través del contratista de seguridad de la información tiene un plan de monitoreo de vulnerabilidades el cual controla la resolución de vulnerabilidades				

AREA : _____ FECHA DILIGENCIAMIENTO FORMATO: _____

PROCESO	HALLAZGO/OBSERVACION	ACCIONES DE MEJORAMIENTO	FECHA DE INICIO DE LA ACCIÓN	FECHA DE FINALIZACIÓN DE LA ACCIÓN	RESPONSABLE
	Numeral 7.4 La Dirección de Tecnología informa que se genera un reporte para determinar las vulnerabilidades que permanecen y cuales estan mitigadas. Sin embargo no se evidencio soporte del diferencial. La Oficina de Riesgos a través del contratista Digiware tiene esta actividad asignada.				
	Numeral 7.5 Se evidenció que la herramienta de escaneo de vulnerabilidades se encuentra homolagada. Se verifico reporte del contratista de seguridad de la información de la Oficina de Riesgos.				
	Numeral 7.6 Se evidenció que la herramienta de escaneo de vulnerabilidades se encuentra homologada. Se verifico reporte del contratista des seguridad de la información de la Oficina de Riesgos.				
ELABORADO POR.	*NOMBRE* _____ *CARGO* _____				
APROBADO POR.	*NOMBRE* _____ *CARGO* _____				