

OFICINA DE CONTROL INTERNO ICETEX - SEGUIMIENTO MAPA DE RIESGOS DE CORRUPCIÓN PRIMER CUATRIMESTRE DE 2022

Nombre Proceso	Riesgo	Causa	Controles	Resultado de la calificación del diseño del control	Resultado de la Calificación de la ejecución del control	Observación y recomendaciones - Seguimiento Oficina de Control Interno
Gestión de Riesgo lavado de activos y financiación del terrorismo	La Posibilidad de materialización de eventos de corrupción, soborno y/o fraude al solicitar o recibir cualquier dádiva o beneficio a nombre propio o de terceros, con el fin de omitir algún potencial cliente activo que se encuentre relacionado con temas de LAFT.	Procesos ejecutados de forma manual	La herramienta de listas de control cuando realiza una consulta que genera una coincidencia, envía de forma automática un correo de notificación al Oficial de Cumplimiento como administrador de la misma, En caso de que no se genere automáticamente la notificación se puede generar el reporte manual o solicitar por correo al proveedor la generación de este con los campos de usuario, fecha y hora de las consultas realizadas. Evidencias: Se guardan los correos de notificaciones automáticas y los reportes generados mensualmente en la carpeta compartida Consultas Risk Consulting(Presidencia/Sarlaft)	Fuerte	Fuerte	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, se evidencian notificaciones automáticas de coincidencia en consultas de listas restrictivas. Recomendación: Seguimiento periódico del control con el fin de actualizar según los cambios operacionales y normativos.
Gestión Comunicación Externa	La Posibilidad de materialización de eventos de corrupción, soborno y/o fraude al solicitar o recibir cualquier lucro o beneficio para el uso inapropiado de la marca ICETEX.	Uso inapropiado de marca por parte de un tercero sin tener un vínculo contractual o convenio con el Icetex, con fines de estafa, engaños y uso diferente a lo establecido.	El profesional de la oficina recibe diariamente el reporte por parte del proveedor que monitorea a medios de comunicación tradicionales y redes sociales a nivel nacional para poder identificar cualquier anomalía con respecto al manejo de la marca ICETEX a través de correo enviado por el proveedor, el profesional si identifica alguna anomalía la reporta a jefe del área. En caso de no recibirse el reporte diariamente, el jefe de área o profesional puede solicitar el reporte al proveedor. Evidencias: Reporte diario, correo electrónico por parte del proveedor.	Moderado	Fuerte	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, teniendo en cuenta que se realiza manualmente la búsqueda y para el reporte diario de las noticias a finales del mes de mayo se contará con el servicio del proveedor para el monitoreo de medio y redes sociales. Recomendación: Se recomienda efectuar verificación de la estructuración del control respecto a la relación con el riesgo y la causa.
Gestión Comunicación Externa	La Posibilidad de materialización de eventos de corrupción, soborno y/o fraude al solicitar o recibir cualquier lucro o beneficio para el uso inapropiado de la marca ICETEX.	Uso inapropiado de marca por parte de un tercero sin tener un vínculo contractual o convenio con el Icetex, con fines de estafa, engaños y uso diferente a lo establecido.	Un colaborador de la oficina de comunicaciones realiza diariamente un monitoreo aleatorio en las redes sociales del Icetex para identificar posibles riesgos reputacionales de la Entidad, revisa las menciones de Icetex en redes sociales y mediante plataforma se consulta si también existen estas, si encuentra alguna novedad la reporta al jefe del área. Los colaboradores de la Oficina de Comunicaciones están pendientes de cualquier novedad en caso de que el funcionario no pueda realizar la actividad. Evidencias: Reporte de funcionario con la identificación de novedades.	Moderado	Fuerte	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos por cuanto los profesionales de la oficina realizan el monitoreo en redes sociales, ayudados de plataformas digitales para el monitoreo y seguimiento de comentarios en las publicaciones e identifican posibles casos o comentarios que afecten la reputación de la Entidad. Recomendación: Seguimiento periodico del control con el fin de actualizar según los cambios operacionales y normativos.
Gestión Comunicación Externa	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros al divulgar información considerada reservada y clasificada.	3. Personas sin conocimiento o falta de capacitación llevan a cabo una inadecuada gestión de comunicación.	Los profesionales del área y/o líder del área cada vez que se publique una pieza comunicativa, validan la aprobación del contenido de la misma, mediante la revisión de los contenidos internos y externos de la comunicación con las dependencias involucradas aprobando el mismo por las partes mediante correo electrónico o en reuniones u otro medio oficial. En caso de tener diferencia en el contenido de la pieza se corrige el mismo según anotaciones de los interesados. Evidencia correo electrónico, actas, grabaciones de las reuniones.	El criterio no aplica para riesgos, causas y controles del sector.	Fuerte	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, en razón a que el profesional encargado de realizar el seguimiento a los requerimiento que las Áreas sobre la generación de contenidos externo o interno, valida la información y envía para aprobación por parte del área, por medio de correo electrónico, posterior a esto se realiza la publicación del contenido. Recomendación: Seguimiento periodico del control con el fin de actualizar según los cambios operacionales y normativos.

OFICINA DE CONTROL INTERNO ICETEX - SEGUIMIENTO MAPA DE RIESGOS DE CORRUPCIÓN PRIMER CUATRIMESTRE DE 2022

Nombre Proceso	Riesgo	Causa	Controles	Resultado de la calificación del diseño del control	Resultado de la Calificación de la ejecución del control	Observación y recomendaciones - Seguimiento Oficina de Control Interno
Representación Judicial y asesoría jurídica	Posibilidad de materialización de eventos de corrupción, soborno y/o fraude al incumplir los términos y acciones judiciales que se requieran, para favorecimiento propio o el de terceros.	Debilidad injustificada en la gestión de defensa judicial de la entidad	Cada abogado debe efectuar la calificación del riesgo de pérdida del proceso judicial asignado en el aplicativo EKOGUI (Aplicativo de gestión de procesos judiciales y conciliaciones) y esta actividad se debe realizar cuando menos cada seis meses para cada proceso.	Fuerte	Fuerte	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, para lo cual los apoderados validan en el aplicativo eKogui el respectivo registro y se efectuó un control dual de la Oficina Asesora Jurídica y la calificación del riesgo reportada a la Vicepresidencia Financiera. Recomendación: Se recomienda efectuar verificación de la estructuración del control respecto a la relación con el riesgo y la causa.
Atención al Cliente	Posibilidad de recibir cualquier dádiva, soborno o beneficio a nombre propio o de terceros por el uso indebido de privilegios otorgados en los sistemas de la entidad para aplicar novedades y alterar la información de los diferentes grupos de interés.	Control inadecuado de los diferentes perfiles de los funcionarios del outsourcing de atención al cliente que permita la manipulación de estados sobre las obligaciones de los beneficiarios por parte de un funcionario que no está autorizado para hacerlo.	El profesional o analista designado realiza un monitoreo de asignación de perfiles y realiza la validación en el sistema, cada vez que se hace necesario activar o dar de baja funcionarios del proveedor de atención al usuario, con el fin de prevenir accesos no autorizados a los sistemas de información de la Entidad. Evidencia del control: Correos electrónicos por parte del coordinador del grupo, profesional y/o analista designado.	Débil	Moderado	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, mediante monitoreos de calidad orientados al buen uso de los aplicativos, soportado por medio de matrices de calidad elaboradas con el fin de evidenciar oportunidades de mejora y buen manejo de los aplicativos, sin embargo, la Oficina ha emitido diferentes observaciones y alertas sobre el préstamo de claves y usuarios entre los colaboradores de atención al usuario. Recomendación: Adelantar las gestiones pertinentes para ejecutar los controles de forma adecuada y minimizar la posibilidad de materialización de riesgos.
Planeación estratégica	Posibilidad de recibir cualquier dádiva, soborno o beneficio a nombre propio o de terceros por la manipulación de los resultados de indicadores y planes de acción corporativos.	Concentración de funciones.	De acuerdo con el documento guía (G04) se establece que los líderes designados por cada dependencia en conformidad con la frecuencia de medición de sus metas, registran a través del aplicativo y/o herramienta para la administración de la planeación estratégica los resultados de los programas, planes e indicadores propios de su área. Si no se registran los resultados de los programas, planes e indicadores, los responsables asignados de la Oficina Asesora de Planeación remiten notificación por correo electrónico solicitando su respectivo reporte. Evidencias: Registro de resultados de los programas, planes e indicadores dentro del aplicativo y/o herramienta para la administración de la planeación estratégica. En el caso que se presente el no reporte de información se tendrá correo electrónico solicitando su reporte.	Débil	Fuerte	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, teniendo en cuenta que mediante la herramienta Plan View se realiza la parametrización, formulación y seguimiento de la planeación estratégica de la Entidad, sin embargo, de conformidad con la descripción del control referente a los responsables de la ejecución: "los responsables asignados de la Oficina Asesora de Planeación remiten notificación...", no asigna a un cargo específico, de conformidad con la directrices impartidas en la Guía para la administración del riesgo y el diseño de controles en entidades públicas Visión 4 del Departamento Administrativo de la Función Pública, igualmente el control debe iniciar con un cargo responsable o un sistema o aplicativo. Recomendación: Se recomienda efectuar verificación de la estructuración del control respecto a la relación con el riesgo y la causa.

OFICINA DE CONTROL INTERNO ICETEX - SEGUIMIENTO MAPA DE RIESGOS DE CORRUPCIÓN PRIMER CUATRIMESTRE DE 2022

Nombre Proceso	Riesgo	Causa	Controles	Resultado de la calificación del diseño del control	Resultado de la Calificación de la ejecución del control	Observación y recomendaciones - Seguimiento Oficina de Control Interno
Planeación estratégica	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros al formular proyectos y/o planes de acción direccionados que no respondan a ninguna necesidad.	Incumplimiento de los requisitos para poder definir una necesidad.	Los proyectos y/o planes de acción aprobados, que responden a las necesidades priorizadas por la Oficina Asesora de Planeación, tienen que estar soportados en la planeación estratégica de la Entidad y deberán ser socializados en plenaria (Comité de Presidencia) con los directivos.	El criterio no aplica para riesgos, causas y controles del sector.	Fuerte	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, teniendo en cuenta que el Líder del Proceso manifestó que durante la formulación de los proyectos estos pasan por varias instancias una de estas es la revisión en plenaria del Comité de Presidencia sobre la estructuración de los proyectos, sus objetivos, actividades y principales entregables. Recomendación: Seguimiento periódico del control con el fin de actualizar según los cambios operacionales y normativos.
Planeación estratégica	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros al formular proyectos y/o planes de acción direccionados que no respondan a ninguna necesidad.	Crear necesidades que no concuerdan con la realidad.	Las necesidades para justificar un proyecto y/o planes de acción deben estar definidas con los soportes, recursos y autorizaciones correspondientes.	El criterio no aplica para riesgos, causas y controles del sector.	Fuerte	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, teniendo en cuenta que el Líder del Proceso manifestó que durante la formulación de los proyectos estos pasan por varias instancias, la primera se realizan validaciones de recursos para su ejecución y su relación con el plan estratégico. Recomendación: Seguimiento periódico del control con el fin de actualizar según los cambios operacionales y normativos.
Planeación estratégica	Posibilidad de recibir dádivas o beneficios a nombre propio o de terceros por la manipulación del Plan Estratégico.	No hay un control de las modificaciones que se hacen al Plan.	Todas las modificaciones al documento deben ser socializadas con todos los directivos de la entidad y no se puede modificar el documento original. Así mismo, siempre debe quedar una copia de la modificación y se debe dejar evidencia de dicho documento aprobado por la Junta Directiva en plenaria.	El criterio no aplica para riesgos, causas y controles del sector.	Fuerte	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, teniendo en cuenta que el Líder del Proceso manifestó que durante las plenarios del Comité de Presidencia se revisan alertas y avances de los proyectos para validación y ajuste. Recomendación: Seguimiento periódico del control con el fin de actualizar según los cambios operacionales y normativos.
Planeación Financiera	Posibilidad de recibir cualquier dádiva, soborno o beneficio a nombre propio, de IES o de terceros por la manipulación de información para el cálculo de los aportes al Fondo de Sostenibilidad.	Concentración de funciones.	El analista de la Oficina Asesora de Planeación cada que se aplica la evaluación remite el documento con los resultados de dicha evaluación para revisión y aprobación del Jefe, a través de correo electrónico. De no efectuarse la aprobación se realizan las correcciones propuestas por el jefe de área. Evidencias: Cruces de correos electrónicos.	Fuerte	Fuerte	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, teniendo en cuenta que el Líder del Proceso manifestó que durante la última revisión del cálculo de aportes al Fondo de Sostenibilidad del Crédito Educativo realizada en 2020 se efectuó el control respectivo para evitar el riesgo de corrupción identificado en este proceso. Recomendación: Seguimiento periódico del control con el fin de actualizar según los cambios operacionales y normativos.

OFICINA DE CONTROL INTERNO ICETEX - SEGUIMIENTO MAPA DE RIESGOS DE CORRUPCIÓN PRIMER CUATRIMESTRE DE 2022

Nombre Proceso	Riesgo	Causa	Controles	Resultado de la calificación del diseño del control	Resultado de la Calificación de la ejecución del control	Observación y recomendaciones - Seguimiento Oficina de Control Interno
Planeación Financiera	Posibilidad de recibir cualquier dádiva, soborno o beneficio a nombre propio, de IES o de terceros por la manipulación de información para el cálculo de los aportes al Fondo de Sostenibilidad.	Tráfico de influencias.	El analista de la Oficina Asesora de Planeación cada que se aplica la evaluación remite el documento con los resultados de dicha evaluación para revisión y aprobación del Jefe, a través de correo electrónico. De no efectuarse la aprobación se realizan las correcciones propuestas por el jefe de área. Evidencias: Cruces de correos electrónicos.	Fuerte	Fuerte	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, teniendo en cuenta que el Líder del Proceso manifestó que durante la última revisión del cálculo de aportes al Fondo de Sostenibilidad del Crédito Educativo realizada en 2020 se efectuó el control respectivo para evitar el riesgo de corrupción identificado en este proceso. Recomendación: Seguimiento periódico del control con el fin de actualizar según los cambios operacionales y normativos.
Gestión de Riesgos financieros	Posibilidad de recibir cualquier dádiva, soborno o beneficio a nombre propio o de terceros para manipular las calificaciones en los sistemas de Administración de Riesgos no Financieros.	Por actuación indebida de los profesionales a cargo.	El coordinador de Riesgos no Financieros realiza validación de las planillas de sesión y de los resultados de la calificación del ejercicio de monitoreo en la herramienta de administración de riesgos, de manera semestral, antes de presentar los resultados al Comité SARO de la entidad. Lo anterior con el fin de verificar que los resultados en el proceso de calificación sean acordes con el monitoreo realizado en las áreas del Icetex y prevenir errores en los informes. En caso de error se revisa con el encargado del monitoreo para rerealizar su corrección. Evidencia: Planillas de sesiones de trabajo, grabaciones por Teams de las sesiones de trabajo y aprobación de resultados, calificaciones de matriz de riesgos en la herramienta de gestión de Riesgos.	Débil	Moderado	La ejecución del control no es acorde con la periodicidad indicada en la descripción del mismo, según lo indicado por el líder de riesgos del área, "la actividad no se ha ejecutado, debido a que el monitoreo de riesgos de corrupción se realiza una vez al año y por cuestiones de cronograma de actividades, éste generalmente se lleva a cabo entre junio y julio de cada vigencia." Recomendación: Se recomienda efectuar verificación de la estructuración del control respecto a la relación con el riesgo y la causa.
Administración de personal	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros para modificar los valores de la nómina en beneficio propio o de un tercero.	Acceso al aplicativo de personal ajeno a la dependencia.	Acceso restringido a personal ajeno a la dependencia. Restricciones según perfil de profesional.	El criterio no aplica para riesgos, causas y controles del sector.	Fuerte	Como consecuencia del confinamiento por pandemia y las obras civiles de remodelación del edificio desde el regreso a labores presenciales no se cuenta con oficina cerrada para nómina, no obstante se tomarán a partir de mayo las medidas necesarias para cumplir con el control establecido. Recomendación: Se recomienda efectuar verificación de la estructuración del control respecto a la relación con el riesgo y la causa.
Administración de personal	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros para modificar los valores de la nómina en beneficio propio o de un tercero.	Debilidad en el aplicativo de nómina.	El profesional encargado de nómina, al inicio de cada año, actualiza los parámetros en el aplicativo, de acuerdo a la normatividad legal vigente, garantizando que los resultados de la liquidación de nómina que se entregan para revisión, sean correctos. Evidencia: Ajustes realizados en el aplicativo de nómina - Logs de auditoría del sistema.	El criterio no aplica para riesgos, causas y controles del sector.	Fuerte	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, teniendo en cuenta que se realiza actualización de parámetros periódicamente. Recomendación: Seguimiento periódico del control con el fin de actualizar según los cambios operacionales y normativos.

OFICINA DE CONTROL INTERNO ICETEX - SEGUIMIENTO MAPA DE RIESGOS DE CORRUPCIÓN PRIMER CUATRIMESTRE DE 2022

Nombre Proceso	Riesgo	Causa	Controles	Resultado de la calificación del diseño del control	Resultado de la Calificación de la ejecución del control	Observación y recomendaciones - Seguimiento Oficina de Control Interno
Administración de personal	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros para modificar los valores de la nómina en beneficio propio o de un tercero.	Acceso al aplicativo de personal ajeno a la dependencia.	El profesional encargado de validar la nómina mensualmente, revisa la totalidad de la información a través de comparación de archivo excel y aplicativo, se entrega la nómina al Coordinador del Grupo de talento humano para su revisión final. Evidencia: Archivo Excel de revisión de nómina, correos electrónicos validando información y/o ajustes.	El criterio no aplica para riesgos, causas y controles del sector.	Fuerte	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, teniendo en cuenta que se realiza la validación mensual de la liquidación de nómina. Recomendación: Seguimiento periódico del control con el fin de actualizar según los cambios operacionales y normativos.
Otorgamiento de crédito	Posibilidad de materialización de eventos relacionados con corrupción, soborno y/o fraude por adjudicar recursos a personas que no cumplan los requisitos definidos en el Reglamento de Crédito para beneficio propio o de terceros.	Manipular los estados y la información del proceso de crédito (desde el registro de la solicitud hasta el desembolso) por parte de un funcionario con las facultades para hacerlo con el propósito de incluir beneficiarios que no se encuentran autorizados por el Comité de Aprobación de Crédito dentro del acta.	Revisión del documento (actas de comité de crédito) por parte del profesional y el coordinador del grupo de crédito, así mismo se ejecutan controles estadísticos que registren todos los créditos realmente aprobados en Comité.	Moderado	Moderado	Las Actas de Comité de Crédito mostradas en la prueba de recorrido del 6 de mayo de 2022, evidencian en los anexos la validación dual entre el colaborador y Coordinador del Grupo de Crédito; sin embargo, las actas no cuentan con todas las firmas de los miembros del comité. Recomendación: Se recomienda efectuar verificación de la estructuración del control respecto a la relación con el riesgo y la causa.
Otorgamiento de crédito	Posibilidad de materialización de eventos relacionados con corrupción, soborno y/o fraude por adjudicar recursos a personas que no cumplan los requisitos definidos en el Reglamento de Crédito para beneficio propio o de terceros.	Manipular los estados y la información del proceso de crédito (desde el registro de la solicitud hasta el desembolso) por parte de un funcionario con las facultades para hacerlo con el propósito de incluir beneficiarios que no se encuentran autorizados por el Comité de Aprobación de Crédito dentro del acta.	Restricciones en los perfiles de los funcionarios del Grupo de Crédito. El control se realiza semanalmente a través de solicitud por medio Aranda con los debidos soportes.	Débil	Fuerte	En la redacción del control no se indica el responsable de su ejecución ni el funcionario que realiza el control dual; de otra parte, la periodicidad de este control no es semanal, es actividad se ejecuta de forma esporádica de conformidad con las novedades de contratación al final e inicio de la vigencia, según los soportes suministrados. Recomendación: Se recomienda efectuar verificación de la estructuración del control respecto a la relación con el riesgo y la causa.
Otorgamiento de crédito	Posibilidad de materialización de eventos relacionados con corrupción, soborno y/o fraude por adjudicar recursos a personas que no cumplan los requisitos definidos en el Reglamento de Crédito para beneficio propio o de terceros.	Manipular los estados y la información del proceso de crédito (desde el registro de la solicitud hasta el desembolso) por parte de un funcionario con las facultades para hacerlo con el propósito de incluir beneficiarios que no se encuentran autorizados por el Comité de Aprobación de Crédito dentro del acta.	Verificación del número y valor de créditos aprobados en comité de crédito por acta frente a las cifras publicadas en página Web.	Débil	Fuerte	En la redacción del control no se indica el responsable de su ejecución ni el funcionario que realiza el control dual; en lo relacionado a como se realiza el control, no es claro, teniendo en cuenta a que los soportes hacen referencia a los valores de giro que el estudiante ve en el sistema, frente a los valores del CDP. Recomendación: Se recomienda efectuar verificación de la estructuración del control respecto a la relación con el riesgo y la causa.

OFICINA DE CONTROL INTERNO ICETEX - SEGUIMIENTO MAPA DE RIESGOS DE CORRUPCIÓN PRIMER CUATRIMESTRE DE 2022

Nombre Proceso	Riesgo	Causa	Controles	Resultado de la calificación del diseño del control	Resultado de la Calificación de la ejecución del control	Observación y recomendaciones - Seguimiento Oficina de Control Interno
Administración de la cartera	Posibilidad de materialización de eventos de corrupción, soborno y/o fraude al condonar obligaciones a personas que no cumplen con los requisitos, a cambio de favorecer un interés particular o el de un tercero.	Inclusión de personas que no cumplen requisitos en la resolución de condonación.	El profesional designado para el control de procedimientos de condonación de VFA valida la resolución de condonación frente a los documentos soportes de solicitud de condonación. Si se observa alguna inconsistencia se devuelve la respectiva resolución al profesional encargado de emitir la resolución para su análisis y ajuste. El control se ejecuta cada vez que se solicita el procedimiento de condonación de beneficiarios. Evidencia: Resolución de condonación aprobada y soportes de solicitud de condonación.	Fuerte	Fuerte	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos. Recomendación: Seguimiento periodico del control con el fin de actualizar según los cambios operacionales y normativos.
Liquidación de fondos en administración	Posibilidad de materialización de eventos de corrupción, soborno y/o fraude al liquidar un fondo sin el cumplimiento de los requisitos establecidos en el reglamento operativo y la normatividad vigente, con el fin de favorecer un interés personal o el de terceros.	Modificar o alterar valores en el estado de cuenta del fondo.	El profesional de liquidación solicita a las áreas de Contabilidad y Cartera el estado de cuenta para verificación de saldo 0 en el fondo a liquidar. Si se detecta algún valor pendiente se solicita el ajuste al área respectiva. Este control se aplica al momento de liquidar un fondo. Evidencia: Estado de cuenta de fondo y conciliación de valores en 0 de ser necesarios.	Fuerte	Fuerte	Se observa que el control se ejecuta correctamente según la necesidad del servicio, es de señalar que el control es esporádico. Recomendación: Seguimiento periodico del control con el fin de actualizar según los cambios operacionales y normativos.
Otorgamiento de crédito a través de la administración de recursos de terceros	Posibilidad de materialización de eventos de corrupción, soborno y/o fraude al adjudicar recursos a personas que no cumplan con los requisitos exigidos, con el fin de beneficiar a un particular o recibir dádivas a cambio.	Manipulación de la información y/o documentación presentada para aplicar a la convocatoria y/o alteración de los resultados a favor de terceros.	El Coordinador de la VFA verifica la información remitida por el gestor del fondo contra los documentos soporte para validar el estado de los beneficiarios y realizar el cargue respectivo en el sistema. Si se observa alguna diferencia en la información, el coordinador remite la observación al gestor del fondo a través de correo electrónico para su respectivo análisis y ajuste. Lo anterior se realiza teniendo en cuenta el cronograma de la convocatoria. Evidencia: Información y documentos soporte remitidos por el ejecutivo del fondo para la adjudicación de créditos.	Fuerte	Fuerte	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, conforme con la descripción del mismo, en el cual el Coordinador valida la información entregada por el gestor del fondo y solicita el cargue de información. Recomendación: Seguimiento periodico del control con el fin de actualizar según los cambios operacionales y normativos.
Administración de la cartera	Posibilidad de condonar obligaciones a beneficiarios que no cumplen con los requisitos, con el propósito de recibir soborno, beneficio a nombre propio o favorecer a un tercero.	Aplicación de condonación a obligaciones en el sistema de cartera, que no cuenten con la aprobación del comité de cartera.	El analista funcional del Grupo de Administración de Cartera semanalmente verifica y compara la información consignada en el acta del comité de cartera vs la Resolución de condonación, con el fin de asegurar que las obligaciones a condonar fueron aprobadas por el Comité de Cartera. Evidencia: Acta del comité de cartera y la Resolución.	Débil	Fuerte	No se determina el tratamiento de las desviaciones en la redacción del control; de otra parte el control se ejecuta correctamente y dentro de los tiempos establecidos, conforme con la descripción del mismo. Recomendación: Se recomienda efectuar verificación de la estructuración del control respecto a la relación con el riesgo y la causa.
Administración de la cartera	Posibilidad de condonar obligaciones a beneficiarios que no cumplen con los requisitos, con el propósito de recibir soborno, beneficio a nombre propio o favorecer a un tercero.	Aplicación de condonación a obligaciones en el sistema de cartera, que no cuenten con la aprobación del comité de cartera.	El analista funcional del Grupo de Administración de Cartera una vez obtenido la aprobación del comité y Resolución firmada, verifica los valores a condonar antes y después de la aplicación de la novedad, tomando los saldos de manera individual o masiva del sistema de información de cartera (se descarga los saldos antes de aplicar la condonación, resultado de la novedad aplicada y base detallada de los créditos condonados), con el fin de verificar que el registro en la cartera sea el correcto. Evidencia: Archivo en Excel (masivo) y pantallazos (análisis individual).	Débil	Fuerte	No se determina el tratamiento de las desviaciones en la redacción del control; de otra parte el control se ejecuta correctamente y dentro de los tiempos establecidos, conforme con la descripción del mismo. Recomendación: Se recomienda efectuar verificación de la estructuración del control respecto a la relación con el riesgo y la causa.

Nombre Proceso	Riesgo	Causa	Controles	Resultado de la calificación del diseño del control	Resultado de la Calificación de la ejecución del control	Observación y recomendaciones - Seguimiento Oficina de Control Interno
Terminación o cumplimiento de obligaciones de crédito	Posibilidad de entregar el pagare y certificado de paz y salvo, sin que la obligación este cancelada para recibir soborno, beneficio propio o de un tercero.	Autorización de la entrega de un pagare y expedición de paz y salvo de obligaciones que no tengan saldo en cero.	El analista funcional del Grupo de Administración de Cartera mensualmente verifica y depura el megareporte identificando las obligaciones que presentan saldo cero \$0,00 o saldo a favor; así mismo verifica que la cartera cumpla con las condiciones , por lo que emite paz y salvo de las líneas de propios y para las líneas de Fondos y de Alianzas, la Vicepresidencia de Fondos en Administración y la Vicepresidencia de Crédito y Cobranzas emiten la viabilidad de expedición de paz y salvo, con el fin de que el Grupo de Cartera genere el certificado. Evidencia: Correo con la viabilidad de cada área y base consolidada de expedición de paz y salvos.	Débil	Fuerte	No se determina el tratamiento de las desviaciones en la redacción del control; de otra parte, el control se ejecuta correctamente y dentro de los tiempos establecidos, se evidencia trazabilidad de las solicitudes de viabilidad de paz y salvo. Recomendación: Se recomienda efectuar verificación de la estructuración del control respecto a la relación con el riesgo y la causa.
Terminación o cumplimiento de obligaciones de crédito	Posibilidad de entregar el pagare y certificado de paz y salvo, sin que la obligación este cancelada para recibir soborno, beneficio propio o de un tercero.	Autorización de la entrega de un pagare y expedición de paz y salvo de obligaciones que no tengan saldo en cero.	El analista funcional del Grupo de Administración de Cartera por solicitud genera autorización para la devolución de las garantías, verificando que la obligación tenga saldo cero \$0,00 y la cartera este liquidada correctamente en el sistema. Para las líneas de propios el Grupo de Cartera genera la autorización y para los Fondos y alianzas la Vicepresidencia de Fondos en Administración y la Vicepresidencia de Crédito y Cobranzas emiten la viabilidad de devolución de las garantías, con el fin de que el Grupo de Cartera genere la autorización mediante memorando. Evidencia: Sistema de atención al usuario "Cosmos" y base consolidada. Eventualmente la VFA solicita la entrega de las garantías por medio de memorando, en el cual emite la viabilidad de Paz y Salvo y devolución de garantías y el analista funcional del Grupo de Administración de Cartera verifica que la obligación tenga saldo cero \$0,00 y la cartera este liquidada correctamente en el sistema. Evidencia: Memorando de solicitud por la VFA y memorando de autorización por el Grupo de Cartera.	Débil	Fuerte	No se determina el tratamiento de las desviaciones en la redacción del control; de otra parte, el control se ejecuta correctamente y dentro de los tiempos establecidos, se evidencia trazabilidad de las solicitudes de viabilidad de paz y salvo. Recomendación: Se recomienda efectuar verificación de la estructuración del control respecto a la relación con el riesgo y la causa.

Nombre Proceso	Riesgo	Causa	Controles	Resultado de la calificación del diseño del control	Resultado de la Calificación de la ejecución del control	Observación y recomendaciones - Seguimiento Oficina de Control Interno
Gestión de legalización y renovación para aprobación del desembolso	Posibilidad de recibir cualquier dádiva, soborno o beneficio a nombre propio o de terceros por realizar giros por mayor o menor valor.	Manipulación del valor a girar.	El analista de liquidación realiza una validación de topes a girar de acuerdo a las líneas y modalidades de crédito, para Recursos Propios en el momento de la generación de la liquidación se realiza verificación previa de los valores de acuerdo a los salarios mínimos y porcentajes liquidados frente a lo autorizado; al momento de identificar un valor inusual se reporta mediante correo electrónico a la Oficina Comercial – Grupo Canal IES con el fin de gestionar el ajuste. Para Fondos en Administración los analistas de preparación ejecutan diariamente teniendo en cuenta las autorizaciones de giro para Fondos Cerrados emitidas por la misional en el formato F341, se realiza verificación en el sistema que se encuentre acorde a los parámetros definidos para el crédito, posterior se genera la planilla F135, el cual bajo macro se verifican los datos contenidos en ella frente a lo registrado en el sistema, cabe aclarar que los cargues masivos se generan a través de la macro "cargue valores masivos" si se llega a presentar una inconsistencia en relación a valores se realiza el ajuste en la herramienta C&CTEX de acuerdo a la información remitida por parte de la misional; en el caso de Fondos Abiertos se realiza verificación bajo macro, la cual muestra el ultimo valor total de giro, se valida cada uno de los rubros de acuerdo al reglamento operativo y topes de financiación del fondo, si se evidencia un valor inusual se ajusta en la herramienta C&CTEX de acuerdo a la información del fondo. Evidencia: Registro en el sistema Desembolsos.NET, Correos que se remiten a las misionales solicitando los ajustes, formatos F341 y F135, resolución de giro.	Fuerte	Fuerte	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, en el cual realiza una validación de topes a girar de acuerdo con las líneas y modalidades de crédito, tanto para recursos propios y Fondos en Administración. Recomendación: Seguimiento periodico del control con el fin de actualizar según los cambios operacionales y normativos.
Gestión de legalización y renovación para aprobación del desembolso	Posibilidad de recibir cualquier dádiva, soborno o beneficio a nombre propio o de terceros por realizar giros por mayor o menor valor.	Manipulación del valor a girar.	El analista de liquidación del desembolso verifica diariamente los valores registrados en el aplicativo de desembolsos frente a la solicitud de liquidación recibida mediante Formato F135 por correo electrónico. Si se llegan a detectar inconsistencias en los valores de giro se devuelve la información para analisis y ajuste por parte del analista de preparación del desembolso. Este procedimiento se realiza para los giros relacionados con Fondos en Administración. Evidencia: Resolución de giro y correos electrónicos informando inconsistencias detectadas en la liquidación.	Fuerte	Fuerte	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, en el cual realiza una validación de topes a girar de acuerdo con las líneas y modalidades de crédito, tanto para recursos propios y Fondos en Administración. Recomendación: Seguimiento periodico del control con el fin de actualizar según los cambios operacionales y normativos.

Nombre Proceso	Riesgo	Causa	Controles	Resultado de la calificación del diseño del control	Resultado de la Calificación de la ejecución del control	Observación y recomendaciones - Seguimiento Oficina de Control Interno
Gestión de legalización y renovación para aprobación del desembolso	Posibilidad de recibir cualquier dádiva, soborno o beneficio a nombre propio o de terceros por realizar giros por mayor o menor valor.	Cambios intencionales de las parametrizaciones en los sistemas y herramientas de giro.	El analista encargado del procedimiento de creación o modificación de reglas de giro en el aplicativo de desembolsos recibe el formato F248 de solicitud que contiene las condiciones para giro de las diferentes sublíneas y/o fondos. Una vez finalizado el registro en el sistema se procede a notificar al área misional para su verificación. Este procedimiento se realiza a solicitud del área misional. Evidencia: Correo electrónico de solicitud de creación o modificación y formato de solicitud F248.	Fuerte	Fuerte	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, en el cual el responsable verifica los valores registrados en el aplicativo de desembolsos frente a la solicitud de liquidación recibida mediante Formato F135. Recomendación: Seguimiento periodico del control con el fin de actualizar según los cambios operacionales y normativos.
Gestión de legalización y renovación para aprobación del desembolso	Posibilidad de realizar giros que no cumplen los requisitos de desembolso por recibir dádiva, soborno, beneficio a nombre propio o de terceros.	Manipular el aplicativo con el fin de alterar los estados de legalización o renovación	El coordinador realiza la asignación de perfiles cada que se requiera de acuerdo con las funciones establecidas y/o actividades contratadas mediante le Gestor de Servicios(Aranda) definido por la Entidad. Evidencia: Solicitud de perfiles por medio de Aranda.	Fuerte	Fuerte	Durante el periodo evaluado no se ha presentado modificación de perfiles de conformidad con la rotación del personal. Recomendación: Seguimiento periódico del control con el fin de actualizar según los cambios operacionales y normativos.
Gestión del servicio	Posibilidad de modificar, hurtar, extraer o darse pérdida definitiva de la información pública, reservada o clasificada contenida en los diferentes sistemas de la Entidad para obtener alguna dádiva, soborno o beneficio a nombre propio o de terceros.	Operación inadecuada de equipos e infraestructura de comunicación (hardware) para que hackers o delincuentes (terceros conocidos) accedan a los recursos informáticos de la Entidad con la intención de extraer información confidencial o eliminarla.	Se identifican las debilidades de la Infraestructura Tecnológica mediante la ejecución del procedimiento de pruebas de vulnerabilidades, para evitar infracciones de seguridad informática. Se aplica cada trimestre y los administradores mitigan las vulnerabilidades que se lleguen a identificar en el escaneo realizado por los encargados de seguridad informática, supervisados por la coordinación de Infraestructura en la Dirección de Tecnología . En caso de no realizarse las pruebas de vulnerabilidades mediante el escaneo de estas de acuerdo con el cronograma definido se notifica al jefe de area y se reprograma nuevamente. Evidencia: Actas comités de vulnerabilidades, archivos de resultados de escaneos de vulnerabilidades	Moderado	Moderado	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, por cuanto se han realizado las pruebas correspondientes para la identificación de las vulnerabilidades y se han establecido los planes de mitigación para realizar el seguimiento adecuado, el seguimiento se realiza en los comites de vulnerabilidades trimestrales, sin embargo, en la redacción del control no se incluyen los reportes con los controles implementados a la gestión de vulnerabilidades. Recomendación: Se recomienda efectuar verificación de la estructuración del control respecto a la relación con el riesgo y la causa.

Nombre Proceso	Riesgo	Causa	Controles	Resultado de la calificación del diseño del control	Resultado de la Calificación de la ejecución del control	Observación y recomendaciones - Seguimiento Oficina de Control Interno
Gestión del servicio	Posibilidad de modificar, hurtar, extraer o darse pérdida definitiva de la información pública, reservada o clasificada contenida en los diferentes sistemas de la Entidad para obtener alguna dádiva, soborno o beneficio a nombre propio o de terceros.	Operación inadecuada de equipos e infraestructura de comunicación (hardware) para que hackers o delincuentes (terceros conocidos) accedan a los recursos informáticos de la Entidad con la intención de extraer información confidencial o eliminarla.	Personal designado realiza la ejecución del procedimiento de Backups para mantener asegurada y disponible la información en caso de darse la afectación de la misma. En caso de no ejecutar el procedimiento se notifica al responsable para que sea realizado. Evidencia: Informe mensual por proveedor del servicio.	Débil	Moderado	<p>Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, toda vez que se ejecutan las tareas de Backup y se genera reporte de su correcta ejecución, sin embargo:</p> <p>La responsabilidad de la ejecución del control se encuentra asignada a un contratista.</p> <ul style="list-style-type: none"> •El control no tiene definida la periodicidad para su ejecución, según la metodología establecida por el DAFP. •Se evidenció el reporte de Backus del proveedor, sin embargo no se evidenció el reporte del relanzamiento de Backus con resultado fallido, de conformidad a lo estipulado en el procedimiento del proveedor. <p>Recomendación: Recomendación: Se recomienda efectuar verificación de la estructuración del control respecto a la relación con el riesgo y la causa.</p>
Gestión del servicio	Posibilidad de modificar, hurtar, extraer o darse pérdida definitiva de la información pública, reservada o clasificada contenida en los diferentes sistemas de la Entidad para obtener alguna dádiva, soborno o beneficio a nombre propio o de terceros.	Operación inadecuada de equipos e infraestructura de comunicación (hardware) para que hackers o delincuentes (terceros conocidos) accedan a los recursos informáticos de la Entidad con la intención de extraer información confidencial o eliminarla.	Se tiene configurado el registro diariamente de ataques cibernéticos que se presentan en algunos servicios y servidores de la entidad con el fin de tener conocimiento, detectar y realizar la corrección de los eventos de seguridad presentados por el Asesor de Seguridad o personal designado. En caso de no realizarse la identificación de los eventos se procede a revisar manualmente la disponibilidad y estado de cada de los servicios. Evidencia: Informes de la herramienta Firewall. Envío de alertas FortiSiem a los administradores.	Débil	Débil	<p>Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos por cuanto desde la plataforma FortiAnalyzer se consolidan los eventos de seguridad registrados diarios y durante el mes, adicional se envía informe mensual de seguridad.</p> <p>Para el estado de los servidores se entregó usuario de lectura en la herramienta FortiSiem para acceso a los dashboard verificación y autoconsulta para el Administrador Especialista de Microsoft Azure, Microsoft Office 365.</p> <p>Se evidenciaron los documentos que soportan la ejecución del control, sin embargo, en la redacción del control no se relaciona el reporte de la corrección de los eventos de seguridad identificados.</p> <p>Recomendación: Se recomienda efectuar verificación de la estructuración del control respecto a la relación con el riesgo y la causa.</p>

OFICINA DE CONTROL INTERNO ICETEX - SEGUIMIENTO MAPA DE RIESGOS DE CORRUPCIÓN PRIMER CUATRIMESTRE DE 2022

Nombre Proceso	Riesgo	Causa	Controles	Resultado de la calificación del diseño del control	Resultado de la Calificación de la ejecución del control	Observación y recomendaciones - Seguimiento Oficina de Control Interno
Gestión del servicio	Posibilidad de modificar, hurtar, extraer o darse pérdida definitiva de la información pública, reservada o clasificada contenida en los diferentes sistemas de la Entidad para obtener alguna dádiva, soborno o beneficio a nombre propio o de terceros.	Falta de seguimiento a los accesos a nivel de infraestructura y/o a sistemas de información de la Entidad.	Se cuenta con el procedimiento "A7-1-05 Gestión de accesos y retiro de servicios" para gestionar los privilegios de administrador a las plataformas de la infraestructura tecnológica y los sistemas de información cuando sea requerido por el usuario con autorización del jefe inmediato. La gestión de accesos solicitados es asignados a cada especialista encargado, con el objetivo de mantener disponibles (operativos), asegurados y actualizados los ingresos de los diferentes usuarios a los servicios que se prestan en las plataformas y/o sistema de información de la Entidad. En caso de no poder realizar el requerimiento por el sistema se realiza notificación a los administradores para que realicen la acción requerida. Evidencia: Casos generados a través de herramienta de gestión.	Moderado	Moderado	<p>Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos y se han realizado la administración de accesos de usuarios (creación, modificación o retiro), de acuerdo con el procedimiento de gestión de accesos (A7-1-05). Se brinda permisos para compartir información de repositorio información (OneDrive) a entidad externas, de acuerdo con el procedimiento de gestión de accesos (A7-1-05). Se tiene activa la restricción para uso de puertos USB y CD/DVD en los equipos de la entidad.</p> <p>Recomendación: Se recomienda efectuar verificación de la estructuración del control respecto a la relación con el riesgo y la causa.</p>
Gestión del servicio	Posibilidad de modificar, hurtar, extraer o darse pérdida definitiva de la información pública, reservada o clasificada contenida en los diferentes sistemas de la Entidad para obtener alguna dádiva, soborno o beneficio a nombre propio o de terceros.	Falta de seguimiento a los accesos a nivel de infraestructura y/o a sistemas de información de la Entidad.	Se cuenta con el documento "políticas y procedimientos de uso DataCenter" código 24 publicado en In-Process cuando se hace necesario el ingreso de personal a estos, donde se describen los lineamientos a seguir para el acceso físico a los Centros de Datos, lo cual es supervisado por la Coordinación de Infraestructura en la Dirección de Tecnología. En caso de no seguir los lineamientos se procederá a notificar por correo electrónico al gerente asignado del proveedor. Evidencia: Correos con autorizaciones al proveedor de servicios de Data Center .	Débil	Débil	<p>Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, en razón a que las solicitudes de ingreso a los centros de datos de Internexa, se hacen de acuerdo al procedimiento. Los accesos atienden actividades de emergencia en el funcionamiento de los equipos de ICETEX, para dar solución y continuidad al correcto funcionamiento, sin embargo:</p> <p>Según la guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, el solo hecho de establecer un procedimiento o contar con una política por sí sola, no va a prevenir o detectar la materialización del riesgo o una de sus causas.</p> <p>•Para el control analizado, no se indica cual es el propósito del mismo (verificar, validar, revisar), para mitigar la causa de la materialización del riesgo.</p> <p>Recomendación: Se recomienda efectuar verificación de la estructuración del control respecto a la relación con el riesgo y la causa.</p>

Nombre Proceso	Riesgo	Causa	Controles	Resultado de la calificación del diseño del control	Resultado de la Calificación de la ejecución del control	Observación y recomendaciones - Seguimiento Oficina de Control Interno
Gestión del servicio	Posibilidad de afectar la disponibilidad los servicios de TI y la operación del ICETEX para recibir cualquier dádiva, soborno o beneficio particular o de terceros.	Sabotaje de los sistemas de la entidad por parte de personal interno y/o externo	Se cuenta con un sistema de protección de seguridad perimetral sobre la infraestructura tecnológica del ICETEX habilitado y/o ejecutado permanentemente y que corresponde a la integración de elementos y sistemas, para la protección de dispositivos y detección de tentativas de intrusión. Quienes son supervisados por el coordinador de infraestructura en la Dirección de Tecnología. En caso de no contar con el sistema se tiene dispositivo de respaldo que entraría a realizar la protección. Evidencia: Informes de alertas y filtrado web de la herramienta.	Fuerte	Fuerte	<p>Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, dado que se cuenta con dispositivo firewall y FortiWeb el cual detecta y deniega las eventos y/o intrusión no permitidos en la red de icetex, adicional se cuenta con plataforma FortiAnalyzer la cual realiza la labor de consolidación para la ejecución de los reportes de las dispositivos de seguridad:</p> <p>Con los módulos de IPS y Antimalware se logró bloquear más de 1481 eventos de diferentes tipos de ataques, que pudieran comprometer la infraestructura de Icetex.</p> <p>Top 20 de las aplicaciones más usadas, la aplicación con mayor consumo Microsoft Portal y con más conexiones es DNS.TXT.Records.Tunneling.</p> <p>Recomendación: Seguimiento periodico del control con el fin de actualizar según los cambios operacionales y normativos.</p>
Gestión del servicio	Posibilidad de afectar la disponibilidad los servicios de TI y la operación del ICETEX para recibir cualquier dádiva, soborno o beneficio particular o de terceros.	Sabotaje de los sistemas de la entidad por parte de personal interno y/o externo	Se cuenta con un Web Application Firewall (WAF) que a diario supervisa, filtra o bloquea el tráfico HTTP hacia y desde las aplicaciones web. El Web Application Firewall se usa para impedir el ataque al sitio web de la Entidad, de igual forma permite implementar políticas de seguridad avanzada para aplicaciones web definidas por la entidad. Este contrato es supervisado por la coordinación de Infraestructura de la Dirección de Tecnología. En caso no contar con el WAF se tiene respaldo de un segundo dispositivo para la protección de las aplicaciones. Evidencia: Informe mensual con información de consumo.	Fuerte	Fuerte	<p>Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, dado que se cuenta con dispositivo WAF Fortinet 2000E para protección de las aplicaciones manejadas internamente y WAF Imperva el cual brinda protección hacia los portales publicados en internet.</p> <p>Se relaciona reporte de la plataforma FortinAnalyzer con la data del Top de los usuarios categorías más bloqueadas para el trafico de la red interna de Icetex.</p> <p>Se relacionado reporte graficas del WAF Imperva con los porcentajes del trafico permitido, bloqueado y vulnerabilidades detectadas para los portales y paginas de Icetex.</p> <p>Recomendación: Seguimiento periodico del control con el fin de actualizar según los cambios operacionales y normativos.</p>

OFICINA DE CONTROL INTERNO ICETEX - SEGUIMIENTO MAPA DE RIESGOS DE CORRUPCIÓN PRIMER CUATRIMESTRE DE 2022

Nombre Proceso	Riesgo	Causa	Controles	Resultado de la calificación del diseño del control	Resultado de la Calificación de la ejecución del control	Observación y recomendaciones - Seguimiento Oficina de Control Interno
Gestión del servicio	Posibilidad de afectar la disponibilidad los servicios de TI y la operación del ICETEX para recibir cualquier dádiva, soborno o beneficio particular o de terceros.	Sabotaje de los sistemas de la entidad por parte de personal interno y/o externo	Se cuenta con el procedimiento "A7-1-05 Gestión de accesos y retiro de servicios" para gestionar los Usuarios y su depuración cada que se presente solicitud por la herramienta de gestión de creación o retiro de usuarios , realizada por cada administrador el cual verifica la oportuna y segura asignación, modificación o retiro de accesos de los usuarios a los sistemas de información, aplicaciones y/o plataformas. En caso de no poder realizar la solicitud a través de la herramienta se tiene contingencia por parte de la mesa de ayuda para la atención. Evidencia: Casos generados a través de herramienta de gestión.	Moderado	Moderado	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos y se han realizado la administración de accesos de usuarios (creación, modificación o retiro), de acuerdo con el procedimiento de gestión de accesos (A7-1-05). Se brinda permisos para compartir información de repositorio información (OneDrive) a entidad externas, de acuerdo con el procedimiento de gestión de accesos (A7-1-05). Se tiene activa la restricción para uso de puertos USB y CD/DVD en los equipos de la entidad. Recomendación: Se recomienda efectuar verificación de la estructuración del control respecto a la relación con el riesgo y la causa.
Gestión del servicio	Posibilidad de afectar la disponibilidad los servicios de TI y la operación del ICETEX para recibir cualquier dádiva, soborno o beneficio particular o de terceros.	Sabotaje de los sistemas de la entidad por parte de personal interno y/o externo	Existen canales de backups de la red de datos proporcionados por el proveedor de servicios de infraestructura y telecomunicaciones para algunas sedes a nivel nacional y para la Sede principal de Aguas, cada que se requiera, con el fin de respaldar la conectividad y disponibilidad de los servicios en caso de caída del servicio principal de la red de datos. Evidencia: Informe mensual (con respecto a la disponibilidad de los servicios a nivel nacional) presentado por proveedor del servicio.	Fuerte	Fuerte	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, se cuenta con una herramienta de monitoreo, que nos ayuda a identificar fallas en el servicio, intermitencias, caídas. Se tiene un balanceador Exinda que nos muestra la saturación de los canales, aplicativos que generan consumo, y que IP la esta realizando. en caso de emergencia se cuenta con equipos conmutadores en las sedes que cuentan con canal principal y backup. Recomendación: Seguimiento periodico del control con el fin de actualizar según los cambios operacionales y normativos.
Gestión del servicio	Posibilidad de afectar la disponibilidad los servicios de TI y la operación del ICETEX para recibir cualquier dádiva, soborno o beneficio particular o de terceros.	Instalación de software malicioso.	Configuración por parte del administrador (Microsoft) cada que se actualicen y/o soliciten ajustes a las políticas de dominio para la restricción de privilegios de instalación de software no autorizado por parte de los usuarios en los equipos de propiedad del Icetex. La mesa de servicio monitorea el software autorizado, en caso de presentarse una instalación no autorizada se procede a desinstalar. Evidencia: Reglas de seguridad en la herramienta.	Fuerte	Fuerte	Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos, en razón a que se realiza supervisión permanente del software instalado y se procede a realizar desinstalación de software cuando se evidencie software no autorizado y se aplica la política para restringir la instalación de software por el usuario. Recomendación: Seguimiento periodico del control con el fin de actualizar según los cambios operacionales y normativos.

Nombre Proceso	Riesgo	Causa	Controles	Resultado de la calificación del diseño del control	Resultado de la Calificación de la ejecución del control	Observación y recomendaciones - Seguimiento Oficina de Control Interno
Gestión del servicio	Posibilidad de afectar la disponibilidad los servicios de TI y la operación del ICETEX para recibir cualquier dádiva, soborno o beneficio particular o de terceros.	Instalación de software malicioso.	Se cuenta con software antivirus permanentemente que impide la ejecución de software malicioso. El software antivirus se encarga de la protección de los equipos de cómputo para detectar, contener y eliminar amenazas informáticas. En caso de no tener antivirus ejecutando en los equipos se tienen escaneo a todos los dispositivos y servidores, al detectar archivo malicioso o dañino se deja en cuarentena. Este contrato es supervisado de la coordinación de Infraestructura de la Dirección de Tecnología. Evidencia: Información en la consola de administración del antivirus.	Fuerte	Fuerte	<p>Se observa que el control se ejecuta correctamente y dentro de los tiempos establecidos mediante la Plataforma Fortclient EMS se garantiza centralización registro de detección y bloqueo de virus y malware, los cuales son reportados mensualmente.</p> <p>Con los módulos de IPS y Antimalware se logró bloquear más de 1481 eventos de diferentes tipos de ataques, que pudieran comprometer la infraestructura de Icetex.</p> <p>Recomendación: Seguimiento periodico del control con el fin de actualizar según los cambios operacionales y normativos.</p>