INFORME FINAL AUDITORÍA INTERNA DE CALIDAD PROCESO DE RIESGOS NO FINANCIEROS

Fecha: Desde el 01 al 09 de julio de 2026

Auditor Líder: Yesenia Marcela Ospina Alvarado – Contratista OCI

Nair Estefani Murillo Zamora – Profesional especializado grado 03

Líder del Proceso: Wilson Edisson Niño Reyes – Jefe Oficina de Riesgos

Colaboradores que atendieron la auditoría: Mónica Pinto García, Lida Gutiérrez Martínez, Lely Herlin López Zárate, Leonardo Santos Chacón.

Tipo de auditoría: Auditoría programada

MACROPROCESO	Gestión y Administración del Riesgo
PROCESO	Riesgos No Financieros
OBJETIVO DE LA AUDITORÍA	Evaluar la conformidad del Sistema de Gestión de Calidad, de acuerdo con la Norma Técnica Colombiana ISO 9001:2015, con el fin, de validar la capacidad, la eficiencia y la eficacia del sistema, para dar cumplimiento a los objetivos definidos y las políticas establecidas por la Entidad
ALCANCE	Comprende la revisión desde la planeación del proceso de Riesgos No Financieros, en cumplimiento de su misionalidad, los criterios desarrollados, los requisitos normativos y la prestación del servicio, hasta el seguimiento, evaluación y mejora continua del proceso, considerando el intervalo de auditorías de la vigencia 2026.
METODOLOGÍA	La metodología se realiza bajo la revisión de documentos, resultados de auditorías anteriores, evaluación frente a los criterios de la auditoría, muestreo aleatorio apropiado, revisión de indicadores de gestión y Acciones correctivas y de mejora, entrevistas con los funcionarios auditados, análisis de datos y observaciones encontradas durante el proceso auditor.
CRITERIOS	Los criterios establecidos por la entidad: Procedimientos. Manuales incluidos SIAR Política Tratamiento de Datos Planes de mejoramiento Tratamiento No Conformidades Indicadores de gestión Riesgos asociados al proceso Demás criterios asociados En el fundamento de la Norma técnica ISO 9001:2015, se auditarán todos los numerales de la Norma, exceptuando los que actualmente no aplican a la Entidad por su naturaleza operativa como son **7.1.5.2 y 8.3.**

ASPECTOS RELEVANTES DEL PROCESO AUDITOR

- El proceso de auditoría dio inicio el miércoles 01 de julio de 2026 con una reunión de apertura realizada de manera virtual a través de Microsoft Teams. Durante este encuentro inicial, correspondiente al ejercicio de auditoría interna del proceso de Riesgos No Financieros, donde se presentó al líder del proceso, a su equipo de trabajo, al equipo auditor, así como el plan de auditoría a desarrollar.
- Se realizaron entrevistas a los colaboradores del proceso para verificar el cumplimiento de los requisitos normativos y procedimentales los días 03, 06, 07, 08 y 09 de julio del 2026.
- Durante el desarrollo de la auditoría se solicitaron y analizaron evidencias que permitieron verificar la trazabilidad y el cumplimiento de las actividades del proceso.
- Durante la reunión de apertura, se indica los documentos que vamos a auditar, sin embargo, el Líder del Proceso manifiesta que el Manual SARO ya no se maneja, es el manual SIAR donde están contemplados todos los riesgos de la entidad. Al solicitar la evidencia de solicitud de eliminación se encuentra por el aplicativo InProcess.

DESARROLLO DEL PROCESO AUDITOR

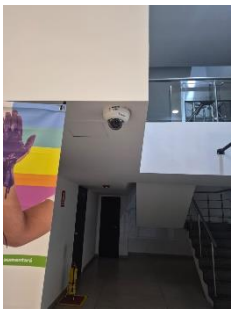
En cumplimiento del Programa Anual de Auditorías Internas de Calidad y de los lineamientos de la Norma ISO 9001:2015, se realizó la auditoría interna al proceso de Riesgos No Financieros, con el fin de evaluar la conformidad y eficacia de las actividades desarrolladas frente a los requisitos normativos, procedimentales e institucionales definidos por la Entidad.

La auditoría se desarrolló entre el 01 y el 09 de julio de 2026, iniciando con reunión de apertura virtual a través de Microsoft Teams, donde se presentó el alcance, metodología y plan de trabajo. Posteriormente, se realizaron entrevistas, revisión documental y validación de evidencias para verificar la aplicación de los procedimientos, controles y lineamientos establecidos para el proceso.

Con base en la documentación asociada al proceso, se tomó como referencia el inventario documental vigente conformado por 69 documentos, correspondientes a 1 caracterización, 1 política, 16 formatos, 11 guías, 15 instructivos, 1 Lineamientos sistemas de gestión, 7 manuales, 1 normatividad, 3 planes operativos y 14 procedimientos, los cuales sirvieron como marco de referencia para el desarrollo de la auditoría. Así mismo, se revisaron los procedimientos objeto de auditoría, así como indicadores de gestión, riesgos operativos, controles, planes de mejoramiento y tratamiento de no conformidades, verificando su aplicación y trazabilidad mediante registros institucionales, soportes documentales y casos gestionados en las herramientas definidas por la Entidad.

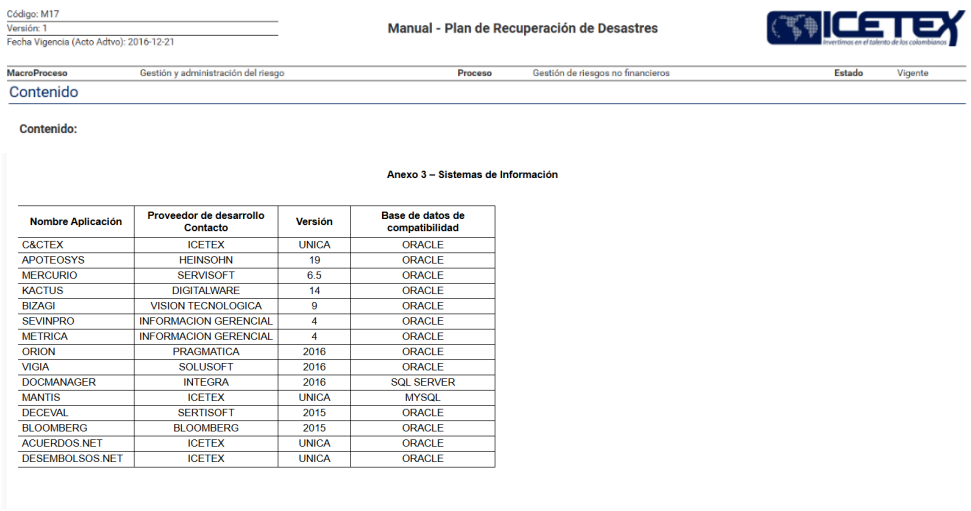
Como resultado del ejercicio auditor, se identificaron las siguientes No Conformidades, tal como se muestra a continuación:

N°	NO CONFORMIDADES
1	Se evidenció que en los puntos de atención al usuario y oficinas del ICETEX donde se encuentran instaladas cámaras de videovigilancia no se dispone de avisos de

	personales conocer la existencia del tratamiento, su finalidad, los derechos que les asisten y los canales para ejercerlos. Adicionalmente, durante la revisión de la Política de Tratamiento de Datos Personales (Código 40, Versión 05, vigente desde el 02/03/2026), se evidenció que el documento no incorpora de manera expresa la finalidad del tratamiento de los datos personales recolectados mediante los sistemas de videovigilancia implementados por la Entidad, ni se encontraron políticas o protocolos específicos que regulen la recolección, uso, circulación, conservación y disposición final de las imágenes y grabaciones obtenidas a través de dichos sistemas. Lo anterior evidencia incumplimiento de los artículos 4, 12 y el literal o) del artículo 17 de la Ley 1581 de 2012, así como de los artículos 2.2.2.25.2.3 y 2.2.2.25.3.2 del Decreto 1074 de 2015, relacionados con el principio de finalidad, el deber de informar a los titulares y la implementación de políticas para el tratamiento de datos personales. Asimismo, se incumple el **numeral 8.2.2 de la Norma ISO 9001:2015**, al no asegurar el cumplimiento de los requisitos legales y reglamentarios aplicables al tratamiento de datos personales durante la prestación del servicio. Esta situación genera riesgo de incumplimiento normativo, vulneración de los derechos de los titulares de la información y la eventual imposición de medidas administrativas por parte de la Superintendencia de Industria y Comercio.
Evidencia No Conformidad 1:	   **3.2. TRATAMIENTO DATOS PERSONALES DE NIÑOS, NIÑAS Y ADOLESCENTES** El tratamiento de los datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, de conformidad con lo establecido en el artículo 7º de la Ley 1581 de 2012 y cuando dicho tratamiento cumpla con los siguientes parámetros y requisitos: 1. Que responda y respete el interés superior de los niños, niñas y adolescentes. 2. Que se asegure el respeto de sus derechos fundamentales. El ICETEX fomenta la educación de los colombianos en Colombia y en el mundo, con calidad y equidad; dando cumplimiento a los principios y obligaciones establecidos en la Ley 1581 de 2012 y el Decreto 1074 de 2015; en el desarrollo de su objeto social, el ICETEX recopila los datos de niños, niñas y adolescentes que acceden a los servicios para responder al interés superior de los mismos, solicitando previamente la autorización de tratamiento de datos personales al Representante Legal o Tutor y velando por el manejo adecuado de éstos.
2	Durante la revisión de la información documentada se evidenció que el documento **"Manual - Plan de Recuperación de Desastres"**, código **M17**, **versión 1**, con **fecha de vigencia 21 de diciembre de 2016**, se encuentra desactualizado respecto al entorno tecnológico actual de la entidad. En el contenido del manual se hace referencia a plataformas y aplicativos que ya no forman parte de la operación institucional, tales como **Mercurio, Bizagi, DocManager, ORION y MANTIS**, sin que se evidencie la actualización del documento para incorporar los sistemas de información actualmente utilizados por la organización. Como consecuencia, el documento no garantiza que los procedimientos, estrategias y actividades definidas para la recuperación ante desastres contemplen la totalidad de los activos tecnológicos vigentes, ni asegura la existencia de un plan de contingencia actualizado para la recuperación y continuidad de los servicios soportados por las plataformas actualmente en producción. Lo anterior evidencia incumplimiento en el control y actualización de la información documentada, al no asegurar que el documento sea revisado y actualizado cuando sea

	necesario para mantener su conveniencia, adecuación y eficacia, conforme a lo establecido en el numeral 7.5.2 de la Norma ISO 9001:2015.

Evidencia No Conformidad 2:



Código: M17
Versión: 1
Fecha Vigencia (Acto Adtvo): 2016-12-21

Manual - Plan de Recuperación de Desastres

MacroProceso: Gestión y administración del riesgo | Proceso: Gestión de riesgos no financieros | Estado: Vigente

Contenido

Contenido:

Anexo 3 – Sistemas de Información

Nombre Aplicación	Proveedor de desarrollo Contacto	Versión	Base de datos de compatibilidad
C&CTEX	ICETEX	UNICA	ORACLE
APOTEOSYS	HEINSOHN	19	ORACLE
MERCURIO	SERVISOFT	6.5	ORACLE
KACTUS	DIGITALWARE	14	ORACLE
BIZAGI	VISION TECNOLOGICA	9	ORACLE
SEVINPRO	INFORMACION GERENCIAL	4	ORACLE
METRICA	INFORMACION GERENCIAL	4	ORACLE
ORION	PRAGMATICA	2016	ORACLE
VIGIA	SOLUSOFT	2016	ORACLE
DOCMANAGER	INTEGRA	2016	SQL SERVER
MANTIS	ICETEX	UNICA	MYSQL
DECEVAL	SERTISOFT	2015	ORACLE
BLOOMBERG	BLOOMBERG	2015	ORACLE
ACUERDOS.NET	ICETEX	UNICA	ORACLE
DESEMBOLSOS.NET	ICETEX	UNICA	ORACLE

3	Durante la auditoría se evidenció que no existe evidencia suficiente que demuestre que la Oficina de Riesgos realizó la guía, coordinación y seguimiento para la ejecución de pruebas anuales a la totalidad de los planes de contingencia definidos por la Entidad, conforme a lo establecido en el numeral 6.5 del Manual de Administración del Plan de Continuidad del Negocio. Si bien se identificaron ejercicios y pruebas para algunos planes de contingencia, no se evidenció una programación, coordinación, consolidación o control que permita asegurar que todos los planes de contingencia vigentes fueron sometidos a pruebas anuales, ni registros que demuestren el cumplimiento integral de esta actividad por parte de las áreas responsables bajo la coordinación de la Oficina de Riesgos. Lo anterior evidencia incumplimiento de los lineamientos definidos en el M-14 Manual de Administración del Plan de Continuidad del Negocio. Así mismo, incumple el numeral 8.1 de la Norma ISO 9001:2015, el cual establece que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos y llevar a cabo las acciones determinadas, asegurando la ejecución y control de las actividades planificadas. Lo anterior genera el riesgo de que las estrategias y procedimientos de contingencia no sean validados oportunamente, afectando la capacidad de respuesta y recuperación de la Entidad ante eventos de interrupción.

Evidencia No Conformidad 3:



6.5.1. COBERTURA DE LOS PLANES

4	Durante la auditoría se evidenció que el monitoreo de los riesgos de continuidad del negocio no se realiza con la periodicidad definida en el numeral 6.5 del Manual de Administración del Plan de Continuidad del Negocio. Aunque el procedimiento establece que dicho monitoreo debe efectuarse de manera semestral, los registros revisados evidencian que la actividad se ejecuta con una frecuencia anual. No se encontraron evidencias que demuestren la realización de monitoreos semestrales durante el período auditado, ni la existencia de mecanismos de control que aseguren el cumplimiento de la periodicidad establecida en el manual. Lo anterior evidencia el incumplimiento de los lineamientos internos definidos para la administración de la continuidad del negocio y del **numeral 9.1.1 de la Norma ISO 9001:2015**, el cual establece que la organización debe realizar el seguimiento, la medición, el análisis y la evaluación de los procesos conforme a los métodos y la frecuencia definidos, con el fin de obtener resultados válidos. Esta situación limita la capacidad de la Entidad para identificar oportunamente cambios en el contexto de riesgo, evaluar la eficacia de los controles implementados y adoptar acciones preventivas frente a posibles eventos que puedan afectar la continuidad de la operación.

Evidencia No Conformidad 4:



Código: M14
Versión: 4
Fecha Vigencia (Acto Adtvo): 2024-12-16

Manual de Administración del Plan de continuidad del Negocio

MacroProceso: Gestión y administración del riesgo — Proceso: Gestión de riesgos no financieros — Estado: Vigente

Contenido

Contenido:

Manual de Admi...

6.5. LINEAMIENTOS GENERALES DEL PLAN DE CONTINUIDAD DE NEGOCIO

Los planes de continuidad de negocio establecen la forma en que los equipos responderán a las interrupciones y reanudarán las actividades dentro del alcance de la continuidad de negocio.

El plan de continuidad de negocio está orientado a la protección de las personas, así como al restablecimiento oportuno de los procesos y servicios críticos e infraestructura, frente a eventos de interrupción o desastre, los cuales deben ser recuperados dentro de los márgenes de tiempo requeridos en el análisis de impacto del negocio.

todo el personal de la Entidad debe estar capacitado en los procedimientos definidos y conocer claramente los roles y responsabilidades que le competen en el marco de la continuidad de negocio, mediante labores periódicas de formación, divulgación y prueba de los Planes de Continuidad de Negocio.

El Icetex debe contar con una estructura de respuesta apoyada por planes y procedimientos de continuidad de negocio para:

- Controlar la respuesta a la interrupción;
- Comunicarse efectivamente con las partes interesadas;
- Utilizando soluciones de continuidad de negocio para reanudar las actividades.

El Plan de Continuidad de Negocio se debe revisar una vez cada año. Sin embargo, los factores que pueden influir revisiones extraordinarias pueden ser:

- Nuevos requerimientos legales aplicables
- Nuevos productos
- Nuevo hardware, plataformas, aplicativos u otros cambios de tecnología (Sistemas Operativos, Bases de Datos, Canales de comunicación de datos, Canales de comunicación de voz, Servicios de Directorio Activo, entre otros).
- Modificaciones a servicios de un proveedor de servicios críticos. Quiebra y/o cambio de un proveedor crítico
- Cambio de instalaciones
- Cambios significativos o transferencia de roles en el personal administrativo y/u operativo. Cambios en el personal o reubicación de este. Transferencia de funciones entre sitios existentes. Consolidación o tercerización de funciones
- Resultados de las pruebas del Plan de Continuidad de Negocio.
- Cambios en los procesos Sistema de Gestión de Calidad y Procesos.

Los jefes de área deben designar un Líder de Riesgos, quien es responsable de apoyar las actividades de la administración de continuidad de negocio para el área que representa.

Las etapas de la administración de continuidad deben ser ejecutadas por cada una de las áreas de la Entidad, con la guía y coordinación de la Oficina de Riesgos.

- El análisis de impacto del negocio debe actualizarse como mínimo una vez al año o cada vez que un Líder de Proceso lo requiera, teniendo en cuenta los cambios del instituto y sus necesidades.
- El monitoreo a los riesgos de continuidad se efectuará de manera semestral.
- Pruebas anuales deben realizarse a todos los planes de contingencia definidos.
- Las estrategias se revisarán cada vez que el Líder del Proceso lo considere o como resultado del análisis de riesgos se determine el ajuste o implementación de estrategias de contingencia.

La Entidad ha definido como el nivel máximo de aceptación del riesgo residual, la clasificación de tolerable.

Se establecerán planes de contingencia sobre los recursos que soportan los procedimientos identificados como críticos a través de la aplicación del análisis de impacto de negocio y la revisión de riesgos de

Así mismo, se identificaron las siguientes oportunidades de mejora:

N°	OPORTUNIDADES DE MEJORA
1	Se identifica la conveniencia de que el proceso evalúe y gestione las acciones necesarias para formalizar la designación de un Oficial de Tratamiento de Datos

	seguimiento. Lo anterior contribuiría a fortalecer la gestión, protección y cumplimiento de las disposiciones aplicables en materia de tratamiento de datos personales, así como a favorecer la coordinación de las actividades relacionadas con la privacidad y protección de la información dentro de la entidad.
2	Fortalecer la gestión del conocimiento al interior del proceso de Gestión del Riesgo, mediante la formalización de un cronograma de capacitaciones y/o socializaciones dirigido a los integrantes del proceso, que facilite la transferencia y apropiación de conocimientos relacionados con sus actividades y responsabilidades. Igualmente, se recomienda garantizar el registro y conservación de las evidencias de estas actividades en la planilla institucional establecida para tal fin, con el propósito de asegurar la trazabilidad de las acciones realizadas y contribuir al mejoramiento continuo del proceso.
3	Se identifica la conveniencia de que el proceso evalúe la pertinencia y capacidad de medición del indicador **"Gestión de Activos de Información"**, teniendo en cuenta que su fórmula corresponde al número de procesos con activos de información identificados y clasificados sobre el número total de procesos de la Entidad. Durante la auditoría se evidenció que la totalidad de los procesos cuentan con activos de información identificados y clasificados, situación que genera resultados constantes del 100% y limita la capacidad del indicador para medir la eficacia de la gestión realizada, identificar oportunidades de mejora, evidenciar variaciones en el desempeño o apoyar la toma de decisiones. Se recomienda revisar la formulación del indicador o complementar su medición con variables asociadas a la actualización, calidad, completitud, consistencia o seguimiento de los inventarios de activos de información, con el fin de fortalecer el análisis de resultados y generar información que aporte valor a la gestión del proceso.
4	Fortalecer los controles y mecanismos de seguimiento para asegurar que los proveedores y contratistas que realizan tratamiento de datos personales en nombre de la Entidad obtengan y conserven las autorizaciones correspondientes antes de la recolección de información de terceros, incluidos los datos de niños, niñas y adolescentes, garantizando el cumplimiento de la normativa vigente y de la Política de Tratamiento de Datos Personales.
5	Se identificó la oportunidad de fortalecer las condiciones de accesibilidad e inclusión en los avisos de videovigilancia y tratamiento de datos personales mediante la incorporación de elementos como pictogramas, información en braille o señalización en alto relieve, con el fin de facilitar el acceso a la información por parte de las personas con discapacidad y contribuir al cumplimiento de los criterios de accesibilidad establecidos en la Política de Servicio al Ciudadano.

RECOMENDACIÓN

- Documentar en el formato **F05 – Acta General de Reuniones** los resultados de las reuniones realizadas durante el monitoreo de riesgos, incluyendo decisiones, compromisos, responsables y plazos. Lo anterior permitirá contar con evidencia objetiva de los temas tratados y las acciones concertadas, fortaleciendo la trazabilidad y el seguimiento de la gestión realizada.

FORTALEZAS

- Se resalta la excelente disposición y colaboración del equipo auditado durante todas las etapas de la auditoría, evidenciando apertura al proceso de evaluación, disponibilidad para atender los requerimientos efectuados y compromiso con el mejoramiento continuo, lo que permitió el desarrollo eficiente y efectivo de la auditoría

- Se resalta la organización de los archivos y la documentación del proceso, la cual permitió una atención eficiente de los requerimientos de auditoría y una rápida ubicación de los registros solicitados. Esta fortaleza refleja buenas prácticas en materia de gestión documental, contribuyendo a la conservación de la información, la transparencia y la mejora continua del proceso.

CONCLUSIONES

El proceso de Riesgos No Financieros demostró compromiso, disposición y colaboración durante el desarrollo de la auditoría, así como fortalezas relacionadas con la organización de la información documentada, la atención de los requerimientos efectuados por el equipo auditor y la disponibilidad de la información necesaria para la ejecución del ejercicio de evaluación.

Como resultado de la auditoría, se identificaron cuatro (4) no conformidades asociadas al cumplimiento de requisitos legales aplicables en materia de protección de datos personales, la actualización de información documentada relacionada con la continuidad del negocio, la realización y seguimiento de pruebas de los planes de contingencia, y el monitoreo de riesgos de continuidad del negocio conforme a la periodicidad establecida por la Entidad.

De igual forma, se identificaron oportunidades de mejora orientadas al fortalecimiento de la gestión de datos personales, la gestión del conocimiento, la pertinencia de los indicadores de gestión, el control sobre terceros que realizan tratamiento de datos personales y la accesibilidad de la información suministrada a los ciudadanos. De igual forma, se identificaron oportunidades de mejora orientadas al fortalecimiento de la gestión de datos personales, la gestión del conocimiento, la pertinencia de los indicadores de gestión, el control sobre terceros que realizan tratamiento de datos personales y la accesibilidad de la información suministrada a los ciudadanos.

Fin del informe

Marcela Ospina Alvarado
Auditor Líder
Contratista

Nair Estefani Murillo Zamora
Auditor Interno
Profesional Especializado 03.