ACUERDO No. 071

(04 DIC 2014)

Por el cual se modifica las metodologías para el Sistema de Gestión de Seguridad de la Información –SGSI-

LA JUNTA DIRECTIVA

En ejercicio de sus facultades legales y estatutarias en especial de las que le confiere la Ley 1002 de diciembre 30 de 2005, el numeral 1 del artículo 9 del Decreto 1050 del 6 de abril de 2006 y,

CONSIDERANDO

Que la Ley 1002 del 30 de diciembre de 2005, transformó al ICETEX en una entidad financiera de naturaleza especial, con personería jurídica, autonomía administrativa y patrimonio propio, vinculada al Ministerio de Educación Nacional, cuyas operaciones financieras son vigiladas, inspeccionadas y controladas por la Superintendencia Financiera.

Que el numeral 4 del Artículo 9 del Decreto 1050 de 2006 faculta a la Junta Directiva del ICETEX, expedir conforme a la ley y a los estatutos del ICETEX, los actos administrativos que se requieran para el cumplimiento de las funciones y de las operaciones autorizadas al ICETEX como entidad financiera de naturaleza especial.

Que la Junta Directiva del ICETEX, adoptó mediante el Acuerdo 010 del 04 de Marzo de 2011, el Manual de seguridad de información del ICETEX, cuyo objeto es establecer las políticas en seguridad de la información, con el fin de regular la seguridad de la información al interior de la entidad, al cual se le incorporó el capítulo de Ley de Protección de Datos mediante acuerdo 036 del 15 de octubre de 2013.

Que la Junta Directiva del ICETEX, mediante el Acuerdo 017 del 06 de mayo de 2014 estableció las metodologías para la gestión de riesgos de seguridad de la información y de inventario y clasificación de activos de información.

Que el Comité de Seguridad de la Información revisó y recomendó las modificaciones de las metodologías de Clasificación de Activos información y Análisis de Riesgos de Seguridad de la información según consta en el Acta No. 003 del 20 de Octubre de 2014.

Que mediante memorando ORD-2500-14-186, la Oficina de Riesgo de la entidad, propuso a la Junta Directiva, la actualización de las metodologías de Clasificación de Activos información y Análisis de Riesgos de Seguridad de la información.

Que en sesión del 22 de Octubre de 2014, la Junta Directiva aprobó la actualización de las metodologías de Clasificación de Activos información y Análisis de Riesgos de Seguridad de la información.

ACUERDO No. 071

(04 DIC 2014)

Por el cual se modifica las metodologías para el Sistema de Gestión de Seguridad de la Información –SGSI-

En virtud de lo anterior acuerda,

ACUERDA

ARTÍCULO 1º. Modificar el artículo 3 del Acuerdo 017 de 2014, el cual quedará así:

ARTICULO TERCERO. METODOLOGÍA PARA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN. Las etapas para desarrollar la metodología de gestión de riesgos de seguridad de la información son:

- **Identificación del riesgo.** En esta etapa se lleva a cabo la identificación de amenazas y vulnerabilidades, en donde las amenazas corresponden a fuentes de riesgos externos y no controlables por la entidad, las vulnerabilidades hacen referencia a las flaquezas o debilidades inherentes a los procesos del instituto. Con la amenaza y la vulnerabilidad se establece el riesgo.

- **Cálculo del Riesgo Inherente.** Para el cálculo del riesgo inherente se tiene en cuenta (2) aspectos: el primero es la frecuencia, la cual considera la probabilidad de ocurrencia de cada uno de los riesgos identificados; el segundo de ellos es el nivel de impacto que a su vez considera cuatro variables como son el nivel de impacto reputacional, de proceso, legal y económico.

- **Identificación y calificación de controles.** En esta etapa se identifican los controles existentes que mitigan los riesgos definidos inicialmente y posteriormente se procede a calificar cada uno de estos controles de acuerdo con los siguientes criterios:

- **Oficialidad.** En este criterio se evalúa si el control existente se encuentra documentado, aprobado, divulgado y genera evidencia.
- **Aplicación.** En este criterio se evalúa si el control es aplicado siempre, es aplicado a discreción o nunca se aplica.
- **Efectividad.** En este criterio se evalúa si el control es efectivo, requiere mejoras o no es afectivo.

- **Calculo del Riesgo Residual**. En esta etapa se realiza el cálculo del riesgo residual considerando la calificación de los controles existentes y si corresponden con acciones preventivas o correctivas, en concordancia con la Metodología de Riesgo Operativo y tal como se observa en la siguiente tabla:

Por el cual se modifica las metodologías para el Sistema de Gestión de Seguridad de la Información –SGSI-

RANGOS DE CALIFICACIONES DE CONTROLES	CUADRANTES A DISMINUIR EN LA PROBABILIDAD	CUADRANTES A DISMINUIR EN EL IMPACTO
	CONTROLES DETECTIVOS, PREVENTIVOS	CONTROLES CORRECTIVOS
ENTRE 0 Y 20%	0	0
ENTRE 21 Y 40%	0	0
ENTRE 41 Y 60%	1	1
ENTRE 61 Y 80%	1	1
ENTRE 81 Y 100%	2	2

- **Mapa Térmico.** En este numeral se hace referencia al mapa térmico que será usado durante la aplicación de la metodología, en este se consideran los criterios de impacto y frecuencia, a su vez definen el nivel de riesgo residual que la entidad está dispuesta a asumir y tratar. El máximo nivel de riesgo que la entidad debe aceptar es el calificado como "TOLERABLE". Para los niveles de riesgos graves o críticos, se deberán establecer planes de acción con el fin de reducir la frecuencia o impacto de los riesgos a través de nuevos controles o mejoras sobre los controles existentes. Los riesgos clasificados como aceptables y tolerables deben ser evaluados periódicamente, con el objetivo de monitorear los controles que mitigan e identificar posibles cambios en el nivel de riesgo.

ARTÍCULO 2º. Modificar el artículo 4 del Acuerdo 017 de 2014, el cual quedará así:

ARTICULO CUARTO. METODOLOGÍA PARA EL INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN. Las etapas para desarrollar la metodología de inventario y clasificación de activos de información son:

- **Identificación de Activos.** En esta etapa se identificarán los activos de información correspondientes a cada proceso y por cada activo de información identificado debe detallarse la información relacionada con la finalidad del activo, el tipo de activo, su ubicación, identificación del propietario, responsable y custodio del activo.

- **Valoración.** En esta etapa se realizará la valoración de los activos frente a los tres pilares de la seguridad de la información como son: Confidencialidad, Integridad y Disponibilidad; para cada uno

Por el cual se modifica las metodologías para el Sistema de Gestión de Seguridad de la Información –SGSI-

de estos criterios se realizará una serie de preguntas cerradas que tienen como objetivo proporcionar la valoración final que será usada para la clasificación de los activos de la información. El cálculo para la valoración final se representa en la siguiente formula:

Valoración Final=Valoración de Disponibilidad (20%) + Valoración de Integridad (20%) + Valoración de Confidencialidad (60%).

- **Clasificación.** Esta etapa tendrá como punto de partida la información generada en la fase de valoración, con el objetivo de proceder a clasificar los activos de información considerando la siguiente tabla:

CLASIFICACIÓN	RANGO DE VALORACIÓN
Restringida	75 - 100%
Reservada	55 – 74,9%
Uso interno	39– 54,9%
Pública	0 - 38,9%

ARTICULO TERCERO. VIGENCIA Y DEROGATORIAS: El presente Acuerdo rige a partir de la fecha de su publicación, modifica el Acuerdo 017 del 06 de Mayo de 2014 y deroga las disposiciones que le sean contrarías.

Publíquese, Comuníquese y Cúmplase

Dado en Bogotá D. C. a los 04 DIC 2014

Presidente **NATALIA ARIZA RAMIREZ**

Secretario **CAMPO ELIAS VACA PERILLA**

	Nombre Funcionario	Cargo	Firma	fecha
Proyectó	Monica Roberto Gonzalez	Abogada Secretaria General		23/10/2014
Revisó// Aprobó	César Augusto Morales Rizo	Jefe de la Oficina de Riesgos		23/10/2014
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes, por lo tanto bajo nuestra responsabilidad lo presentamos para la firma de la Secretaria General				