ACUERDO Nº.

"Por la cual se actualiza y compila el Manual de Políticas de Seguridad Digital del ICETEX".

LA JUNTA DIRECTIVA

En ejercicio de sus facultades legales y estatutarias en especial de las que le confiere la Ley 1002 de 2005, Decreto 1050 de 2006, Acuerdo 013 de 2022 y,

CONSIDERANDO:

Que, la Ley 1002 de 2005 modificó la naturaleza jurídica del Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior, Mariano Ospina Pérez, ICETEX, al transformarlo en una entidad financiera de naturaleza especial, con personería jurídica, autonomía administrativa y patrimonio propio, vinculada al Ministerio de Educación Nacional.

Que, el numeral 1 del artículo 9° del Decreto 1050 del 6 de abril de 2006 estableció que es función de la Junta Directiva, *"(...) formular la política general y los planes, programas y proyectos para el cumplimiento del objeto legal del ICETEX, de sus funciones y operaciones autorizadas y todas aquellas inherentes a su naturaleza jurídica, acorde con lo dispuesto por la Ley 1002 de diciembre 30 de 2005, y los lineamientos y políticas del Gobierno Nacional en materia de crédito educativo".*

Que, el numeral 21 del artículo 9° del Acuerdo 013 de 2022 señaló como función de la Junta Directiva la de: *"Aprobar las políticas, procedimientos, metodologías y manuales para la gestión y administración integral de los riesgos, y fijar el nivel de tolerancia de las medidas relativas al perfil de riesgo residual sobre las que se realizará el monitoreo".*

Que, en Junta Directiva del ICETEX adoptó, mediante el Acuerdo 03 de 2022, el Manual de Políticas de Seguridad Digital, cuyo objeto es establecer las políticas y lineamientos en seguridad digital del ICETEX, con el fin de regular su gestión al interior de la Entidad.

Que, con el fin de extender los lineamientos de control para la protección de la información producida, custodiada y transmitida en la ejecución de los contratos de prestación de servicios profesionales y asegurar un enfoque coherente y eficaz de gestión ante un ataque cibernético, requiere adicionar, en el Manual de Políticas de Seguridad Digital, la Política para Contratistas de Prestación de Servicios Profesionales en la Política de Personal y el Protocolo para la atención de incidentes de seguridad de la información asociados con ataques cibernéticos en la Política de Ciberseguridad.

Que, conforme con lo anterior, la Oficina de Riesgos realizó la propuesta de estas políticas y presentó a consideración del Comité de Seguridad de la Información, en sesión del 12 de diciembre de 2022, la actualización del Manual de Políticas de Seguridad Digital del ICETEX, donde fue recomendado.

Que, de conformidad con el documento técnico presentado por la Oficina de Riesgos, en sesión adelantada el 25 de enero de 2023, la Junta Directiva aprobó la actualización del Manual de Políticas de Seguridad Digital en los aspectos que se relacionan a continuación, con el fin de incorporar ajustes por evolución del Sistema de Gestión de Seguridad Digital:

- Numeral 9.4 - Política para Contratistas de Prestación de Servicios Profesionales: donde se establece la política general, roles y responsabilidades, lineamientos de: Vinculación

Carrera 3 # 18-32 Bogotá Colombia
Bogotá: 601 417 3535 | **Nacional:** 01 8000 91 68 21
www.icetex.gov.co
@icetex @icetex_colombia ICETEXCOLOMBIA ICETEX

del personal contratista, Gestión de Acceso, Clasificación de la Información, Almacenamiento de la Información, Borrado seguro y Seguimiento a Políticas de seguridad digital.

- Numeral 23.1 - Protocolo para la atención de incidentes de seguridad de la información asociados con ataques cibernéticos: conformado por las premisas, los roles y responsabilidades y el protocolo a desarrollar ante un ataque cibernético.

Que, en virtud de lo anterior se requiere la actualización del Manual de Políticas de Seguridad Digital al adicionar los numerales Numeral 9.4 - Política para Contratistas de Prestación de Servicios Profesionales y Numeral 23.1 - Protocolo para la atención de incidentes de seguridad de la información asociados con ataques cibernéticos.

Que, en sesión ordinaria la Junta Directiva de fecha 25 de enero de 2023, aprobó la actualización del Manual de Políticas de Seguridad Digital del ICETEX, que hace parte integral de este Acuerdo, de conformidad con la información presentada por Oficina de Riesgos, adicionalmente el documento técnico se encuentra anexo al presente Acuerdo y hace parte integral de él con 12 folios.

Que, en mérito de lo expuesto,

ACUERDA:

Artículo 1. Adoptar la actualización del Manual de Políticas de Seguridad Digital del ICETEX, en el cual se adiciona las siguientes políticas así:

- ***Numeral 9.4 - Política para Contratistas de Prestación de Servicios Profesionales.***

"9.4 POLÍTICA DE SEGURIDAD DIGITAL PARA CONTRATISTAS DE PRESTACION DE SERVICIOS PROFESIONALES.

El ICETEX establece mecanismos de control para la protección de la información producida, custodiada y transmitida en la ejecución de los contratos de prestación de servicios profesionales, quienes tienen la obligación de propender por la integridad, disponibilidad y confidencialidad de ésta.

Generalidades:

- *El Contratista debe asegurar la protección de la información del ICETEX a la que tiene acceso durante el desarrollo del contrato por medio del cumplimiento de las Políticas de Seguridad Digital.*
- *Toda la información objeto del contrato de prestación de servicios, información de usuarios y contraseñas para acceso a las aplicaciones e información de gestión, es de carácter confidencial, por lo que el Contratista debe garantizar los controles necesarios para mantener su confidencialidad, integridad y disponibilidad en todo momento.*
- *El Contratista no divulgará información sin la debida autorización del ICETEX, a menos que exista una obligación legal y no utilizará tal información para lucro y/o beneficio personal y/o de terceros, o que de alguna manera que fuere contraria a la ley en detrimento de los objetivos legítimos y éticos del ICETEX.*

Carrera 3 # 18-32 Bogotá Colombia
Bogotá: 601 417 3535 | **Nacional:** 01 8000 91 68 21
www.icetex.gov.co
@icetex @icetex_colombia ICETEXCOLOMBIA ICETEX

- *Los contratistas que tienen información del ICETEX en sus equipos de cómputo personales para el desarrollo del objeto del Contrato son responsables de la seguridad de la información en su poder y de cumplir con las directrices aquí estipuladas, de manera que se evite la fuga, hurto o secuestro de información.*

Normas para Vinculación del personal contratista

Normas dirigidas al SUPERVISORES DE CONTRATO

- *Deberán garantizar que dentro de las cláusulas del contrato se encuentre la aceptación de las políticas de seguridad digital.*
- *Serán responsables por asegurar la confiabilidad y veracidad de la información consignada en los documentos y así mismo dan fe de que dicha información ha sido verificada.*
- *Deberán garantizar que se suscriban los Acuerdos de Confidencialidad, se formalicen y se cumplan.*
- *Deberán garantizar la firma de la autorización de tratamiento de datos personales por parte del contratista.*
- *Deberán garantizar la divulgación de las políticas de seguridad digital del Manual de Políticas de Seguridad Digital.*

Normas para Uso de equipos de cómputo no corporativos.

Normas dirigidas: CONTRATISTAS

- *El equipo de cómputo de su propiedad debe estar debidamente licenciado de acuerdo con las leyes de propiedad intelectual vigentes y aplicables, para lo cual entregará al Supervisor del contrato con copia a la Mesa de Servicio de la Dirección de Tecnología, el listado del software que va a utilizar y evidencia de las licencias correspondientes (tanto para el sistema operativo como para las aplicaciones).*
- *El computador personal debe contar con un software antivirus licenciado y actualizado.*
- *Deberán evitar el uso de aplicaciones que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de la información, por ejemplo: aplicaciones de Hacking, Proxies, DNS Changer, NMAP, Wireshark, etc, se recomienda solo descargar aplicaciones de sitios oficiales.*
- *Las conexiones a sistemas y servicios del ICETEX deberán efectuarse por canales seguros, para lo cual deben tener instalado el cliente de VPN o Escritorio Virtual en el computador personal, con el fin de conectarse vía remota a los servicios tecnológicos del ICETEX.*
- *El Contratista que sospeche la infección por virus u otro software malicioso en su computado personal, debe notificar a la mayor brevedad posible al personal de soporte de la Dirección de Tecnología y/o a la Oficina de Riesgos al correo seguridaddigital@ICETEX.gov.co.*
- *Deberá garantizar que el computador utilizado para el cumplimiento del objeto del contrato esté actualizado permanentemente en los parches de seguridad divulgados públicamente por los distintos fabricantes de software.*
- *El Contratista deberá asegurarse que los datos del ICETEX se mantengan lógicamente separados de los datos de sus demás clientes.*

Carrera 3 # 18-32 Bogotá Colombia
Bogotá: 601 417 3535 | **Nacional:** 01 8000 91 68 21
www.icetex.gov.co
@icetex @icetex_colombia ICETEXCOLOMBIA ICETEX

- *Deberá permitir que se realice la activación de tecnologías para el uso de un segundo o múltiple factor de autenticación (MFA) para la protección de accesos a*
- *Deberá llevar su equipo personal a la Dirección de Tecnología cuando ésta lo requiera, con el fin de permitir la revisión de las configuraciones de seguridad y la aplicación de controles de seguridad de la información.*
- *En complemento, se recomienda al Contratista:*
  - *Que el equipo de cómputo cuente con bloqueo automático por inactividad de sesión.*
  - *Hacer el cifrado de información en los discos duros de su equipo de cómputo.*

Normas dirigidas a: DIRECCIÓN DE TECNOLOGÍA

- *Para los equipos de cómputo de los contratistas que se conecten a la red corporativa, la Dirección de Tecnología deberá validar algunos aspectos de seguridad, entre éstos: antivirus activo y actualizado y sistema operativo actualizado.*
- *La Dirección de Tecnología establece las condiciones de conexión a la red de datos de la Entidad que deben cumplir las estaciones de trabajo o dispositivos móviles personales y verificar su cumplimiento de manera periódica.*
- *Con el fin de asegurar el cumplimiento de las normas colombianas en materia de seguridad y privacidad, y controlar posibles riesgos cibernéticos, el ICETEX a través de la Dirección de Tecnología se reserva el derecho de revisar, cuando lo considere necesario, el software instalado y utilizado en equipos de cómputo personal del contratista.*

Normas para Gestión de Acceso

Normas dirigidas a: CONTRATISTA

- *En caso de que el Contratista requiera acceder a los sistemas de información del ICETEX deberá cumplir con las políticas, procedimientos y controles vigentes de la Entidad para la gestión de los accesos y utilizar buenas prácticas para el uso de contraseñas. De ninguna manera los accesos concedidos al contratista vinculado generan una relación laboral directa como funcionario del ICETEX.*
- *Los contratistas serán responsables de las acciones realizadas con las cuentas de usuario asignadas, sus contraseñas y los privilegios otorgados.*
- *Los contratistas no deberán compartir sus cuentas de usuario y contraseñas con otros contratistas o funcionarios.*
- *Los contratistas deberán acogerse a lineamientos para la configuración de contraseñas implementados por el Instituto.*
- *Los contratistas deberán utilizar las cuentas de usuario únicamente para el desarrollo de las labores asignadas.*

Normas dirigidas a: SUPERVISORES DE CONTRATO

- *Los Supervisores de contratos suscritos con el ICETEX deberán otorgar los permisos para el acceso a los recursos tecnológicos o los sistemas de información de la Entidad a los Contratistas según los roles a desempeñar, de igual manera gestionarán la inactivación en el momento de la finalización de los contratos.*

Normas para Clasificación de la Información

Carrera 3 # 18-32 Bogotá Colombia
Bogotá: 601 417 3535 | **Nacional:** 01 8000 91 68 21
www.icetex.gov.co
@icetex @icetex_colombia ICETEXCOLOMBIA ICETEX

Normas dirigidas a: CONTRATISTA

- *El Contratista deberá conocer la clasificación de la información a la que tendrá acceso para el desarrollo de sus actividades y deberá garantizar que la misma cuente con un nivel apropiado de protección, de acuerdo con los lineamientos de clasificación del ICETEX.*
- *El Contratista acatará los lineamientos de etiquetado de la información contenida en los recursos tecnológicos, así como de la información física del Instituto de acuerdo con la Guía de manejo de activos de información.*
- *Cualquier novedad asociada a los activos entregados por ICETEX (daño, pérdida, robo, etc.) deberá ser comunicada al Supervisor del contrato de ICETEX de manera inmediata y oportuna, y el Supervisor del mismo deberá, su vez, informar dicha novedad al correo seguridaddigital@ICETEX.gov.co.*
- *El Contratista en desarrollo del objeto del contrato deberá implementar las buenas prácticas que garanticen la confidencialidad, integridad y disponibilidad de la información y el buen uso de los activos suministrados.*

Normas para Almacenamiento de la Información

Normas dirigidas a: CONTRATISTA

- *El Contratista deberá almacenar la información del ICETEX únicamente en los sitios autorizados de acuerdo con la política de almacenamiento de la información; está prohibido almacenar información en su dispositivo personal.*

Normas para Gestión de Riesgos

Normas dirigidas a: CONTRATISTA

- *El Contratista deberá conocer los riesgos de seguridad digital del proceso que atenderá en desarrollo de su objeto contractual y aplicará los controles tal como han sido definidos.*
- *El Contratista deberá apoyar al Líder de Riesgos y al Líder de Proceso en la gestión del riesgo de seguridad digital.*
- *En caso de que el Contratista llegase a tener conocimiento de algún incidente de seguridad o privacidad de la información, debe notificar al Supervisor del Contrato del ICETEX del incidente ocurrido dentro de las treinta y seis (36) horas siguientes a la detección de éste, como también al correo seguridaddigital@ICETEX.gov.co, con el fin de que se revise y atienda de acuerdo con el procedimiento para reportar y gestionar incidentes de seguridad de la información.*

Normas para Borrado seguro

Normas dirigidas a: CONTRATISTA

- *En el momento en que termine la relación contractual con el ICETEX, toda la información que el Contratista tenga en su poder, en relación con el contrato debe ser remitida al Supervisor del mismo, incluyendo documentos físicos, electrónicos y magnéticos en original o copias. De igual manera, se deberá borrar o destruir toda*

Carrera 3 # 18-32 Bogotá Colombia
Bogotá: 601 417 3535 | **Nacional:** 01 8000 91 68 21
www.icetex.gov.co
@icetex @icetex_colombia ICETEXCOLOMBIA ICETEX

información en el equipo del Contratista o medios de almacenamiento externo incluyendo servicios de almacenamiento en la nube, de acuerdo con el procedimiento de borrado seguro de la Entidad.

- *En caso de información imposible de borrar, la misma mantendrá su carácter de confidencial aun después de finalizada la relación contractual.*

Normas para Seguimiento a Políticas de seguridad digital

Normas dirigidas a: SUPERVISORES DE CONTRATO

- *Los Supervisores de contratos verificarán el adecuado uso de los recursos tecnológicos y de la información suministrada al Contratista para el desarrollo de las obligaciones del Contrato.*
- *Los Supervisores de contratos deberán hacer seguimiento al cumplimiento de las normas legales, políticas, procedimientos y requisitos específicos de seguridad digital por parte del Contratista.*

Normas dirigidas a: CONTRATISTAS

- *Los Contratistas deberán cumplir con todas las cláusulas contractuales y el marco legal colombiano aplicable a la seguridad digital.*
- *El incumplimiento de las políticas de seguridad digital se gestionará a través de procedimientos administrativos que pueden conducir a procesos penales según aplique de acuerdo con la gravedad de la falta. El ICETEX cuenta con canales de comunicación donde el personal puede reportar posibles incumplimientos que afecten la seguridad digital."*

- ***Numeral 23.1 - Protocolo para la atención de incidentes de seguridad de la información asociados con ataques cibernéticos:***

Premisas:

Es responsabilidad de la Entidad contar con los elementos tecnológicos necesarios y el personal requerido para la atención de un ataque cibernético (infiltración por medio de suplantación de identidad - phishing, borrado de la información, cifrado de la información, entre otros.), definiendo estrategias de aseguramiento, continuidad de la operación y la recuperación de la información de aplicativos e infraestructura que soporte la operación del ICETEX.

Se establecen las siguientes premisas para prevenir contener y mitigar cualquier impacto en la materialización de un ataque cibernético:

- *Ante una situación de secuestro de información, el lineamiento del ICETEX es no ceder ante chantajes, extorsiones o cualquier otro tipo de requerimiento dado por un ciberdelincuente o grupo de ciberdelincuentes.*
- *El ICETEX deberá contar con una infraestructura tecnológica de respaldo en una ubicación en donde se encuentre suficientemente protegida y aislada de acceso a través de la red de internet.*

Carrera 3 # 18-32 Bogotá Colombia
Bogotá: 601 417 3535 | **Nacional:** 01 8000 91 68 21
www.icetex.gov.co
@icetex @icetex_colombia ICETEXCOLOMBIA ICETEX

- *La Entidad deberá contar con el permanente funcionamiento de infraestructura redundante en cuanto a telecomunicaciones, utilizando el apoyo de proveedores, de ser requerido.*
- *El ICETEX deberá contar con copias de respaldo de la información aisladas de la red y con sus respectivas pruebas de restauración.*
- *La Entidad deberá implementar y mantener operativo un esquema de recopilación automática y sincrónica de su información principal.*
- *El ICETEX deberá contar con el inventario de sistemas de información críticos, la infraestructura tecnológica que lo soporta, el personal que se requiere para la recuperación de los sistemas y la priorización de estos.*
- *La Entidad deberá identificar los proveedores críticos para su operación, así como haber definido los canales de comunicación oficial con estos proveedores y los acuerdos de nivel de servicio.*
- *Mantenerse informado por medio de un SOC (herramienta tecnológica que permite detectar y analizar incidentes de seguridad) que realice constantemente la supervisión y administración de la seguridad de los sistemas de información a través de herramientas de recogida, correlación de eventos e intervención remota cuando se requiera.*
- *La Entidad deberá realizar la gestión oportuna de tratamiento de brechas identificadas en los análisis de vulnerabilidades realizados.*
- *La Entidad deberá realizar campañas de sensibilización y socialización de las actividades que se deben realizar antes, durante y después de presentarse un incidente de seguridad de la información.*
- *La Entidad deberá realizar simulacros en temas de continuidad del negocio frente a ataques cibernéticos.*
- *El ICETEX deberá contar con el conocimiento para el aislamiento de los elementos probatorios tecnológicos para la realización de un análisis forense.*
- *La Entidad deberá mantener contacto permanente con las entidades del sector y del gobierno, a través de la participación en grupos de interés, que le permitan estar informada sobre los incidentes presentados, las noticias relevantes y la información relacionada con posibles vulnerabilidades o amenazas de día cero.*
- *El ICETEX deberá contar con el directorio actualizado con los nombres, correos electrónicos, número de teléfono y entidad o empresa a la que pertenece, de quienes deben ser informados en caso de presentarse un incidente de seguridad de la información.*

Normas dirigidas a: COMITÉ SARO – SARLAFT - RESPUESTA A INCIDENTES DE SEGURIDAD DE INFORMACIÓN RELACIONADOS CON ATAQUES CIBERNÉTICOS

- *Evaluar y aprobar las comunicaciones formales en el manejo del incidente que pueden afectar la operación de tecnología y/o de la Entidad.*
- *Definir y asignar recursos que sean necesarios para gestionar el incidente presentado.*
- *Convocar al personal de la Dirección de Tecnología y aquel que se requiera para atender la emergencia presentada por el incidente.*
- *Tomar la decisión de activar un plan de recuperación de desastres de ser necesario.*
- *Declarar la contingencia y retorno a la normalidad de la operación cuando se obtengan las condiciones esperadas.*

Carrera 3 # 18-32 Bogotá Colombia
Bogotá: 601 417 3535 | **Nacional:** 01 8000 91 68 21
www.icetex.gov.co
@icetex @icetex_colombia ICETEXCOLOMBIA ICETEX

- *Gestionar el presupuesto para la sostenibilidad de las acciones que se deban realizar durante y después de la contingencia del incidente.*
- *Mantener la documentación de las sesiones de trabajo por medio de informes, actas de reunión, lecciones aprendidas, durante y después del incidente.*
- *Definir la persona encargada de hablar con los medios de comunicación.*
- *Definir el responsable de generar las piezas comunicativas y los medios que se usarán para comunicar al ciudadano, al cliente interno y grupos de interés.*

Normas dirigidas a: LÍDER DE RECUPERACIÓN DE PROCESOS EN EL INCIDENTE (OFICIAL DE SEGURIDAD DE LA INFORMACIÓN Y/O LÍDER DE RIESGOS).

- *Comunicar la situación a los directivos y grupos de interés de la Entidad.*
- *Acompañar en la toma de decisiones del manejo del incidente.*
- *Gestionar las necesidades o requerimientos que se presenten en relación con el incidente.*
- *Verificar el cumplimiento del protocolo establecido para el manejo de incidentes.*
- *Realizar un análisis constante del impacto que ha ocasionado o está ocasionando el incidente.*
- *Mantener comunicación constante con el Comité SARO-SARLAFT y el equipo de trabajo que está conteniendo el incidente.*
- *Comunicar al personal encargado de atender el incidente, la recuperación de la infraestructura y los sistemas de información las decisiones del Comité SARO-SARLAFT.*

Normas dirigidas a: DIRECCIÓN DE TECNOLOGÍA.

- *Asistir a las jornadas de sensibilización y capacitación vinculadas a los planes de contingencia frente a ataques cibernéticos.*
- *Reportar de manera inmediata a los líderes de recuperación los incidentes de interrupción que identifiquen.*
- *Atender las instrucciones y decisiones dadas por el Comité SARO-SARLAFT.*
- *Apoyar los ejercicios de análisis de impacto del ataque cibernético presentado, por ejemplo: infraestructura afectada, dificultades en la restauración de los servicios tecnológicos, apoyo en contener el impacto en la imagen institucional, apoyo en las justificaciones técnicas que se deban emitir a medios de comunicación o entes de control.*
- *Ejecutar las actividades necesarias para el restablecimiento de la operación.*

Protocolo ante un ataque cibernético

- *El Oficial de Seguridad de la Información o Líder de Riesgos deberá comunicar la situación presentada al comité SARO-SARLAFT.*
- *El Oficial de Seguridad de la Información, Líder de Riesgos o el Director de Tecnología deberá comunicarse con los proveedores de servicios críticos y el personal que apoya en el restablecimiento de la operación de la Entidad.*
- *El Oficial de Seguridad de la Información o Líder de Riesgos deberá informar a las autoridades competentes COLCERT (Equipo de Respuesta a Emergencias Informáticas de Colombia,), Superintendencia Financiera de Colombia - SFC y Ministerio de Educación Nacional- MEN, sobre la situación presentada en la Entidad.*

Carrera 3 # 18-32 Bogotá Colombia
Bogotá: 601 417 3535 | **Nacional:** 01 8000 91 68 21
www.icetex.gov.co
@icetex @icetex_colombia ICETEXCOLOMBIA ICETEX

- *Junto con el equipo de trabajo (proveedores y personal de la Entidad), el Director de Tecnología deberá realizar un diagnóstico de los daños o la afectación en la infraestructura, aplicaciones y servicios que presta la Entidad, que,*

a. *Contenga la identificación de la afectación, la cual incluye el análisis de lo que se vio impactado por el ataque cibernético, si las causas del incidente se encuentran aún activas y pueden comprometer elementos que no se vieron afectados en un primer momento.*
b. *Identifique, seleccione y recopile de forma segura, con la debida cadena de custodia los elementos técnicos y tecnológicos, así como la información (trazas de tráfico de red, logs de auditoría de usuarios privilegiados, logs de eventos etc.) que se requerirá para la ejecución del análisis forense y de conformidad con la Guía para el manejo de posible delito informático.*
c. *Propenda por el aseguramiento de la red y comunicaciones, permitiendo habilitar de forma segura los elementos que articula el restablecimiento de los servicios, tanto interno como externos.*
d. *Permita el alistamiento de servidores: este procedimiento conlleva el formateo de todos los elementos que componen la infraestructura del Datacenter y el restablecimiento de cada uno de los servidores, con sus características propias, que permitan el correcto funcionamiento de cada uno de los sistemas de información que soportan los procesos misionales y de apoyo del ICETEX.*
e. *Permita el alistamiento y levantamiento de infraestructura tecnológica para aplicaciones misionales, dando prioridad a los sistemas que soportan los procesos afectados de la Entidad.*
f. *Busque la restauración de bases de datos y aplicaciones misionales, pruebas y puesta en producción, dando prioridad a los sistemas que soportan los procesos afectados de la Entidad.*
g. *De cómo resultado la salida a producción escalonada de acuerdo con la habilitación progresiva de servicios hasta lograr el 100% de los servicios tecnológicos del ICETEX.*

- *El Oficial de Seguridad de la Información o Líder de Riesgos instaura y documenta las sesiones de trabajo periódicas diarias al inicio del incidente que se ampliaran en el tiempo de acuerdo con el avance de la recuperación de los servicios afectados*
- *Con el apoyo de la Oficina Asesora Jurídica, se presentará la denuncia respectiva ante las autoridades competentes, informando sobre la afectación.*
- *El Oficial de Seguridad de la Información registra el incidente ante la Superintendencia de Industria y Comercio, por afecta de datos personales de las partes interesadas.*
- *El Oficial de Seguridad de la Información inicia la investigación forense respectiva.*
- *El Oficial de Seguridad de la Información o Líder de Riesgos mantiene informados a los medios de comunicación y al personal interno de ICETEX.*
- *El Oficial de Seguridad de la Información documenta las lecciones aprendidas en el informe del incidente de seguridad de la información".*

Artículo 2. Comunicaciones. El presente Acuerdo deberá ser comunicado, a través de la Secretaría General del ICETEX, a Vicepresidencia de Fondos en Administración, Vicepresidencia de Operaciones y Tecnología, Vicepresidencia Financiera, Vicepresidencia de Crédito y Cobranza, Oficina de Riesgos, Oficina Asesora de Planeación, Oficina Comercial y Mercadeo, Oficina Asesora Jurídica, Oficina de Control Interno, Oficina de

Carrera 3 # 18-32 Bogotá Colombia
Bogotá: 601 417 3535 | **Nacional:** 01 8000 91 68 21
www.icetex.gov.co
@icetex @icetex_colombia ICETEXCOLOMBIA ICETEX

ACUERDO Nº.

"Por la cual se actualiza y compila el Manual de Políticas de Seguridad Digital del ICETEX".

Relaciones Internacionales y Oficina Asesora de Comunicaciones y al Grupo de Contratación.

Artículo 3. Vigencias y derogatorias. El presente Acuerdo rige a partir de la fecha de su publicación en Diario Oficial, compila y deroga las disposiciones que le sean contrarias, en especial el Acuerdo 03 de fecha 28 de enero de 2022.

Publíquese, comuníquese y cúmplase.

Dada en Bogotá D.C. a los

Presidente de la Junta Directiva,

ALEJANDRO GAVIRIA URIBE

Secretaria Técnica de la Junta Directiva,

MARÍA CAROLINA CARRILLO SALTARÉN

	Nombre funcionario	Cargo	Firma
Proyectó por parte del ICETEX	Claudia Stella Cortes Albornoz	Analista de Riesgos	
Aprobó por parte del ICETEX.	Liceth Paola Lizcano Castillo	Jefe Oficina de Riesgos	
Revisó por parte del Ministerio de Educación Nacional	Nancy Judith Botia Hernández	Abogada del Grupo de Delegados del Ministro	
Aprobó por parte del Ministerio de Educación Nacional	Ana Carolina Quijano Valencia	Asesora Viceministerio de Educación Superior	Ana Carolina Quijano
Aprobó por parte del Ministerio de Educación Nacional	Ricardo Moreno Patiño	Asesor del Ministro de Educación Nacional	
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 del Presidente de la Junta Directiva y la Secretaria Técnica de Junta.			

Carrera 3 # 18-32 Bogotá Colombia
Bogotá: 601 417 3535 | **Nacional:** 01 8000 91 68 21
www.icetex.gov.co
@icetex @icetex_colombia ICETEXCOLOMBIA ICETEX