MANUAL DE POLÍTICAS DE SEGURIDAD DIGITAL

INSTITUTO COLOMBIANO DE CRÉDITO EDUCATIVO Y ESTUDIOS TÉCNICOS EN EL EXTERIOR

Junio 2026

TABLA DE CONTENIDO

INTRODUCCIÓN

El Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior – ICETEX reconoce que la información constituye uno de los activos más valiosos para el cumplimiento de su misión institucional y el desarrollo de sus funciones, ya que es un elemento esencial para la continuidad operativa, la confianza de los usuarios y el cumplimiento de las obligaciones legales y regulatorias.

En este contexto, el presente documento tiene como finalidad establecer las políticas que orientan la gestión de la seguridad y la privacidad de la información. Su propósito es definir lineamientos, roles, controles y prácticas que permitan prevenir incidentes, gestionar riesgos y fomentar una cultura organizacional centrada en la protección de la información, reduciendo la probabilidad de ocurrencia de eventos que comprometan la seguridad institucional.

1. OBJETIVO

Establecer las políticas para la gestión de la seguridad y la privacidad de la información, con el fin de asegurar la protección de la confidencialidad, integridad, disponibilidad, continuidad, autenticidad y no repudio de los activos de información institucionales, promoviendo prácticas que minimicen riesgos y aseguren su adecuado manejo.

2. ALCANCE

Este documento es aplicable a todas las áreas, procesos y dependencias del ICETEX, sin excepción. Su cumplimiento es obligatorio para los servidores públicos, contratistas, practicantes y terceros que mantengan vínculos laborales o contractuales, en el marco de sus funciones, responsabilidades y compromisos institucionales.

3. MARCO NORMATIVO

El presente documento se fundamenta en el conjunto de normas, lineamientos y estándares que regulan la gestión de la seguridad, privacidad y protección de los datos en Colombia. Este marco normativo orienta la adopción de controles, responsabilidades y prácticas necesarias para garantizar la confidencialidad, integridad, disponibilidad, privacidad, continuidad, autenticidad y no repudio de la información administrada por el Icetex.

- **CONPES 3701 de 2011**: Este documento menciona los lineamientos de la política para la ciberseguridad y ciberdefensa, buscando fortalecer las capacidades del Estado para enfrentar amenazas en el ciberespacio. Se enfoca en crear un ambiente seguro y proteger la infraestructura crítica del país.
- **Ley 1581 de 2012:** Establece el régimen de protección de datos personales en Colombia.
- **Ley 1712 de 2014:** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional
- **Decreto 1078 de 2015:** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”
- **CONPES 3854 de 2016**: La Política Nacional de Seguridad Digital tiene como objetivo que los ciudadanos y las empresas identifiquen y gestionen los riesgos en el entorno digital. Se busca fomentar una cultura de seguridad digital, educando a la población sobre cómo protegerse de delitos cibernéticos y promoviendo buenas prácticas, como el uso de contraseñas seguras y la precaución con correos electrónicos sospechosos
- **Circular de la SFC No. 007 de 2018:** Imparte instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad
- **Circular de la SFC No. 025 de 2020:** Define lineamientos de continuidad del negocio
- **ISO/IEC 27001:2022- Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información:** establece los requisitos para implementar y mantener un Sistema de Gestión de Seguridad de la Información

- **Resolución 2277 de 2025:** Por la cual se actualiza el Modelo de Seguridad y Privacidad de la Información

4. DEFINICIONES

- **Activo de información:** cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios del Instituto y, en consecuencia, debe ser protegido.
- **Acuerdo de Confidencialidad:** es un documento en los contratistas y personal provisto por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información del Instituto, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.
- **Acuerdo de Nivel de servicio (ANS):** son los acuerdos que se hacen con los usuarios de los servicios en los cuales se estipula el nivel de calidad para la aceptación del servicio.
- **Análisis de riesgos de seguridad digital:** proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.
- **Autenticación:** es el procedimiento de comprobación de la Entidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.
- **BYOD**: Del inglés Bring Your On Device (Trae Tu Propio Dispositivo). Son los lineamientos mediante los cuales el Icetex permite el acceso a su información y plataforma tecnológica a través de los dispositivos personales de los colaboradores o terceros para ejecutar sus funciones u obligaciones.
- **Clasificación y etiquetado de la Información:** es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación de la información (pública, clasificada, o reservada) para recibir el nivel de protección adecuado
- **Centros de cableado:** son habitaciones donde se deben instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.
- **Centro de cómputo:** es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.
- **Ciberamenaza o amenaza cibernética:** aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.
- **Ciberataque o ataque cibernético:** acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de esta o donde el ciberespacio es fuente o herramienta de comisión de un crimen.
- **Ciberespacio:** entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.
- **Ciber riesgo o riesgo cibernético:** posibles resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos.
- **Ciberseguridad:** Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la Entidad.
- **Cifrado:** es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, acceso no autorizado a los repositorios de información.
- **Componentes informáticos:** Son todos aquellos recursos tecnológicos que hacen referencia a: aplicativos, software de sistemas, sistemas operativos, bases de datos, redes, correo electrónico, software ofimático, software de seguridad, hardware y equipos de comunicaciones
- **Confidencialidad:** es la garantía de que la información no es divulgada a personas, Entidades o procesos no autorizados.

- **Control:** es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.
- **Criptografía**: es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.
- **Custodio del activo de información:** es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.
- **Derechos de Autor:** es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.
- **Disponibilidad**: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.
- **Dispositivos Personales:** Se entiende como dispositivo personal cualquier artefacto que tenga la capacidad de almacenar, transferir y/o procesar cualquier tipo de información. Entre estos dispositivos se incluye los equipos computo (portátiles o de escritorio), teléfonos inteligentes, tabletas, entre otros.
- **Equipo de cómputo**: dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.
- **Evento de seguridad**: ocurrencia de una situación que podría afectar la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio.
- **Hacking ético:** es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.
- **Incidente de seguridad:** ocurrencia de una situación que afecta la protección o el aseguramiento de los datos, sistemas y aplicaciones de la Entidad que son esenciales para el negocio.
- **Información en reposo:** datos guardados en dispositivos de almacenamiento persistente (por ejemplo, cintas, copias de seguridad externas, dispositivos móviles, discos duros, entre otros).
- **Información en tránsito:** información que fluye a través de la red pública, como Internet, y los datos que viajan en una red privada, como una red de área local (LAN) corporativa o empresarial.
- **Integridad**: es la protección de la exactitud y estado completo de los activos.
- **Inteligencia artificial:** Es un campo de la informática dedicado a resolver problemas cognitivos comúnmente asociados con la inteligencia humana o seres inteligentes, entendidos como aquellos que pueden adaptarse a situaciones cambiantes. Su base es el desarrollo de sistemas informáticos, la disponibilidad de datos y los algoritmos. Conpes 3975.
- **Inventario de activos de información**: es una lista ordenada y documentada de los activos de información pertenecientes al Instituto.
- **Licencia de software**: es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.
- **LOG (Registro):** es el registro de auditoría de las acciones y de los acontecimientos que ocurren en un sistema computacional cuando un usuario o proceso está activo y sucede un evento que está configurado para reportar. Rastro de lo que se está ejecutando sobre la plataforma tecnológica**.**
- **Medio removible:** es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.
- **Malware o Virus**: es cualquier tipo de software diseñado para causar daño, robar información o tomar control de un sistema sin permiso del usuario.
- **Perfiles de usuario**: son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.
- **Propiedad intelectual:** es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a

cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

- **Propietario de la información:** es la unidad organizacional o proceso donde se crean los activos de información.
- **Resiliencia:** es la capacidad de un mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que pudo estar sometido.
- **Recursos tecnológicos:** son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior del Instituto.
- **Registros de Auditoría:** son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos del Instituto. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.
- **Responsable por el activo de información:** es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.
- **Sensibilización:** es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.
- **SGSI:** Sistema de Gestión de Seguridad de la Informaciòn.
- **Sistema de información:** es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por el Instituto o de origen externo ya sea adquirido por la Entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta..
- **Software malicioso:** es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.
- **Teletrabajo:** Hace referencia a todas las formas de trabajo por fuera de la oficina, incluidos los entornos de trabajo no tradicionales, a los que se denomina "trabajo a distancia", "lugar de trabajo flexible", "trabajo remoto" y ambientes de "trabajo virtual".
- **Terceros:** todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad.
- **Versiones LST (Long Support Term):** son versiones de software que reciben soporte extendido por parte del proveedor. Se caracterizan por su estabilidad, seguridad y mantenimiento a largo plazo.
- **Vulnerabilidades:** son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por el Instituto (amenazas), las cuales se constituyen en fuentes de riesgo.

5. POLITICA GENERAL DE SEGURIDAD y PRIVACIDAD DE LA INFORMACIÓN

El Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior – ICETEX en desarrollo a su misión *“Promovemos el progreso social, acompañando los proyectos de vida de las y los colombianos mediante opciones incluyentes en la educación superior”* y con la finalidad de prestar servicios confiables a las partes interesadas se compromete a:

- Preservar y administrar la confidencialidad, integridad y disponibilidad de los activos de información
- Mitigar incidentes de seguridad y privacidad de la información y continuidad de la prestación de los servicios.
- Gestionar riesgos de seguridad y privacidad de la información y continuidad de la prestación de los servicios.
- Fortalecer la cultura de seguridad y privacidad de la información en los servidor público, contratistas, practicantes y terceros que tengan vínculos laborales o contractuales con el instituto.

Lo anterior, enmarcado en el cumplimiento de los requisitos legales, regulatorios y mejora continua, para apoyar los servicios que presta el Icetex.

6. POLÍTICAS ESPECIFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Las políticas de seguridad de la información acá enunciadas están enmarcadas en el cumplimiento de las buenas prácticas ISO 27001:2022 y serán evaluadas de acuerdo con la establecido en el Modelo de Seguridad y Privacidad de la Información de MINTIC.

6.1. Políticas de seguridad y privacidad de la información

a) Las políticas de seguridad y privacidad de la información están descritas en este documento y en los documentos que hacen parte del Sistema de Gestión de Seguridad de la Información- SGSI ubicados en el aplicativo dispuesto por el Icetex.
b) Las políticas son comunicadas a los servidores públicos, contratistas, practicantes y terceros a través de los canales de comunicación disponibles por el Icetex.
c) Las políticas son objeto de revisión anual y pueden ser actualizadas cuando se presenten cambios normativos, tecnológicos o requerimientos institucionales que así lo demanden. La aprobación de dichas actualizaciones corresponde a la Junta Directiva del Icetex.

6.2. Roles y responsabilidades

El ICETEX establece una estructura organizacional responsable de la seguridad y privacidad de la información, definiendo roles y responsabilidades asegurando la cobertura integral de los aspectos técnicos, operativos y estratégicos relacionados con la seguridad de la información:

Alta dirección:

a) Definir y establecer los roles y responsabilidades relacionados con la seguridad y privacidad de la información en los niveles directivo y operativo.
b) Revisar y aprobar las políticas de seguridad y privacidad de la información contenidas en este documento.
c) Revisar y aprobar el presupuesto de seguridad digital.
d) Promover una cultura de Seguridad Digital en todos los servidores públicos de la Entidad y al personal provisto por terceras partes.
e) Dirigir y apoyar a las personas para contribuir a la eficacia del Sistema de Gestión de Seguridad Digital.
f) La Alta Dirección y la secretaria general asigna los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad digital del Instituto.
g) Revisar el estado del Sistema de Gestión de Seguridad Digital.

Comité de riesgos:

a) Actualizar y presentar ante la Junta Directiva las Políticas de Seguridad Digital.
b) Verificar el cumplimiento de las políticas de seguridad digital del Instituto.
c) Evaluar el estado del Modelo de Seguridad y Privacidad de la Información del Instituto.

Oficina de riesgos:

a) Liderar la generación de lineamientos para gestionar la seguridad digital y asesorar en la implementación de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.
b) Formular, documentar y gestionar el Plan Estratégico de Seguridad de la Información y Plan de Tratamiento de Riesgos de Seguridad de la Información.
c) Validar y monitorear la gestión de riesgos de seguridad.
d) Realizar sensibilizaciones a los colaboradores del Icetex en temas relacionados en seguridad y privacidad de la información
e) Gestionar los incidentes de seguridad digital y en caso de ser necesario avisar a autoridades competentes, de acuerdo con las normas legales establecidas.

Oficina control interno:

a) Planear y coordinar la contratación para la ejecución de las auditorías internas al Sistema de Gestión de Seguridad Digital, a fin de determinar si las políticas, procesos, procedimientos y controles

establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables.

b) Realizar seguimiento a los Planes de Mejoramiento, producto de las Auditorías realizadas a los procesos y/o procedimiento del Sistema de Gestión de Seguridad Digital.
c) Socializar y Remitir el Informe de Auditoría Interna al Sistema de Gestión de Seguridad Digital, a la Oficina de Riesgos.

Dirección Tecnologia- VOT:

a) Realizar la validación, corrección, restauración o ajuste de la información en los sistemas de información institucionales cuando esta haya sido alterada, comprometida o afectada como consecuencia de la materialización de riesgos o incidentes de seguridad digital, garantizando la integridad, disponibilidad y trazabilidad de la información en todos los sistemas de información de la entidad.
b) Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos al Sistema de Gestión de Seguridad Digital.
c) Desarrollar los procedimientos e instructivos necesarios para la correcta operación y administración del Sistema de Gestión de Seguridad Digital.

6.3. Segregación de funciones

a) La información estará bajo la responsabilidad del Líder de Proceso para evitar la modificación intencional o no autorizada o mal uso de los activos de información del Icetex.
b) Una vez formalizado el proceso de vinculación, el supervisor de contrato o jefe inmediato solicitará la creación de la cuenta de usuario de acuerdo con lo establecido en el procedimiento A7 -1-05 Gestión de accesos y retiro de servicios.
c) El supervisor de contrato o jefe inmediato, deberán informar a la Mesa de Ayuda las novedades del colaborador (ejemplo: terminación contrato, sesión de contrato, cambio de área, retiro de la entidad, entre otras). de acuerdo con lo establecido en el A7 -1-05 Gestión de accesos y retiro de servicios.

6.4. Contacto con autoridades y grupos de interés

El equipo de seguridad y privacidad de la Información del Icetex establecerá contacto con los siguientes grupos:

a) Autoridades nacionales competentes en materia de seguridad de la información y protección de datos, con el fin de garantizar el cumplimiento normativo, la gestión adecuada de incidentes y la articulación interinstitucional.
b) Grupos de interés, tales como la Policía Nacional, CSIRT, INTERPOL, Fiscalía, DIJIN, cuerpos de Bomberos, Defensa Civil, y entidades especializadas en atención de desastres, en aquellos casos en los que se presente un incidente de seguridad de la información que requiera asesoría técnica externa, apoyo operativo o coordinación para la mitigación de riesgos.

6.5. Inteligencia de amenazas

La Dirección de Tecnología - VOT identificará y analizará la información sobre las amenazas existentes o emergentes de seguridad y privacidad de la información a las que se encuentra expuesto el Instituto y tomará las acciones respectivas para mitigarlas. En caso de que dichas amenazas se materialicen, adoptará las acciones de corrección necesarias para restablecer, ajustar o recuperar la información en los sistemas institucionales, garantizando su integridad, disponibilidad y trazabilidad.

6.6. Seguridad de la información en la gestión de proyectos

La seguridad y privacidad de la información se incluye de manera explícita en los estudios previos de contratos, acuerdos y proyectos tecnológicos, como también se evalúan los riesgos inherentes y se recomiendan algunos controles para mitigarlos.

6.7. Inventario de activos de información

a) La gestión de activos de información se realiza de acuerdo con lo establecido en la Guía para la clasificación de activos de información - G176 y en el Procedimiento identificar y clasificar activos de información- E2-1-13.
b) Los líderes de los procesos son los propietarios de los activos de información y deberán mantener un inventario de sus activos de información actualizado.
c) Los lideres de los procesos establecen y monitorean los controles definidos durante todo el ciclo de vida del activo de información, teniendo en cuenta la criticidad asignada. Asi mismo, informar al equipo de

Seguridad y Privacidad de la Información de la Oficina de Riesgos cualquier situación que ponga en riesgo la confidencialidad, integridad, disponibilidad y/o privacidad del activo de información.

d) Los lideres de los procesos definen, revisan y monitorean periódicamente los usuarios, permisos, restricciones, clasificaciones y perfiles de acceso a los activos de información, teniendo en cuenta las políticas de control de acceso aplicables.

6.8. Uso aceptable de los activos de información

La información, los sistemas, aplicaciones, servicios y equipos tecnológicos incluyendo computadores de escritorio, portátiles, impresoras, redes, acceso a internet, dispositivos móviles, correo electrónico institucional, herramientas de acceso remoto, teléfonos y demás recursos digitales son activos de información que el Icetex proporciona a sus servidores públicos, colaboradores y terceros autorizados para cumplir con actividades específicas del instituto. Por lo tanto, deben ser utilizados de manera responsable y segura.

6.8.1 Uso del Internet

El Internet es un recurso que el Icetex provee a sus servidores públicos y colaboradores para apoyar el desarrollo de sus funciones y obligaciones, por tal motivo, a continuación, se definen las medidas para hacer un buen uso y aprovechamiento de este recurso:

a) La Vicepresidencia de Operaciones y Tecnología - VOT implementará políticas de navegación basadas en categorías y niveles de usuario, con el objetivo de proteger el instituto de afectaciones por malware, fuga de información o navegación de contenido inapropiado.
b) La Vicepresidencia de Operaciones y Tecnología - VOT, realiza monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los servidores públicos colaboradores y/o terceros. Así mismo, se podría inspeccionar, registrar e informar las actividades realizadas durante la navegación.
c) La Vicepresidencia de Operaciones y Tecnologia - VOT al ser quien administra y gestiona los canales de internet, podrá verificar y monitorear la navegación en general de todos los servidores públicos y contratistas, con el fin de velar por el adecuado uso de este recurso y el cumplimiento de las políticas de seguridad de los activos.
d) Esta restringido el acceso a páginas relacionadas con pornografía, drogas, terrorismo, segregación racial, hacking y/o cualquier otra página que vaya en contra de la ética, la moral, las leyes vigentes o las políticas aquí establecidas.
e) El Icetex cuenta con servicios de almacenamiento en la nube para intercambio de información, por lo tanto, el acceso a portales de intercambio y almacenamiento de archivos gratuitos o abiertos en la nube como Google, DropBOX, BOX, Mega, WeTransfer, entre otros, están restringidos.
f) Se permitirán servicios de streaming de audio a través de sitios web que no pongan en riesgos las redes e infraestructura del Icetex.
g) Se permitirán servicios de streaming de video a través de sitios web que no pongan en riesgos las redes e infraestructura del Icetex, sin embargo, los portales permitidos tendrán limitaciones en consumo de red, para optimizar el uso de los recursos disponibles.
h) Está prohibido el acceso a webproxies y/o cualquier página por la cual se intente violar las políticas definidas por el Icetex.
i) No está permitida la descarga y el uso de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables, herramientas de hacking, entre otros.
j) No está permitido el acceso a servicios de mensajería, redes sociales o correo diferentes a los establecidos por el Icetex como la suite Gmail, Outlook, Yahoo!, Messenger, Facebook, WhatsApp Web, YouTube y páginas de chat.
k) Los procesos que, en cumplimiento de sus funciones, requieran el uso de redes sociales u otras páginas, el líder del proceso realizara la solicitud a la VOT, quien garantizara el cumplimiento de los protocolos de seguridad de la información.
l) No está permitido el acceso, ni el uso de servicios interactivos, páginas de mensajería instantánea o que tengan como objetivo crear comunidades para intercambiar información o bien para fines diferentes a las actividades propias del Icetex.
m) Es responsabilidad de los usuarios dar el uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, legislación vigente y las políticas de seguridad y privacidad de la información del instituto.

n) Los servidores públicos, colaboradores, terceros y/o proveedores, al igual que los servidores públicos o contratistas de éstos, no pueden asumir en nombre del Icetex, posiciones personales en encuestas de opinión, foros u otros medios similares.
o) El uso de internet no considerado dentro de las restricciones antes mencionadas es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad, ni la protección de la información del Icetex.

6.8.2. Uso correo electrónico

La Dirección de Tecnología – VOT asigna una cuenta de correo electrónico (con dominio **@icetex.gov.co**) como herramienta de trabajo para cada uno de los servidores públicos y/o contratistas que lo requieran para el desempeño de sus funciones, obligaciones y en algunos casos a terceros con previa autorización; su uso se encuentra sujeto a las siguientes políticas:

a) El único servicio de correo autorizado para el manejo o transmisión de la información institucional es el proporcionado por la VOT del Icetex.
b) La cuenta de correo electrónico debe ser usada únicamente para el desempeño de las funciones u obligaciones asignadas por el Icetex.
c) Los mensajes y la información contenida en los buzones de correo son de propiedad del Icetex. Cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones u obligaciones.
d) Todo mensaje tipo SPAM o malicioso deberá reportarse a la VOT a través de la herramienta establecida por el instituto. Está expresamente prohibido el reenvío de mensajes sospechosos a otros buzones, ya que se entenderá como propagación intencional de virus.
e) Todo mensaje de índole personal debe ser reenviado a un correo externo del servidor público y/o colaborador y eliminado del buzón institucional.
f) El tamaño de los buzones de correo, de los mensajes enviados y recibidos, está determinado por la VOT, con el propósito de preservar la capacidad de almacenamiento, garantizar la disponibilidad del servicio y prevenir riesgos asociados al uso excesivo de recursos tecnológicos.
g) No está permitido el envío de información clasificada como “Información Reservada” o “Información Clasificada” del Icetex sin previa autorización de la alta dirección o líder de proceso.
h) Todo correo electrónico que se envié deberá contener el mensaje de confidencialidad definido por el Icetex.
i) No está permitido usar las cuentas institucionales para registrarse en servicios de terceros en internet como páginas publicitarias, comercio electrónico, redes sociales entre otros.
j) No está permitido el envío de correos masivos a más de 30 destinatarios tanto internos como externos, salvo los correos emitidos por los procesos misionales.
k) Está prohibido enviar o recibir cadenas de correo, mensajes con contenidos religioso, juegos, políticos, racistas, sexistas, pornográficos, publicitarios no corporativos o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.
l) No está permitido el envío de archivos que contengan extensiones como wav, .exe, .com, .dll, .bat. o cualquier otro archivo ejecutable; en caso de ser necesario deberá ser autorizado por la Vicepresidencia de Operaciones y Tecnologia VOT.
m) Está prohibido distribuir, copiar o reenviar información del Icetex a través de correos personales o sitios web diferentes a los autorizados.

6.8.3. Dispositivos Personales - Trae Tu Propio Equipo- BYOD

El Icetex permite el acceso a su información y plataforma tecnológica a través de los dispositivos personales de los colaboradores, servidores públicos o terceros para ejecutar sus funciones u obligaciones. Por lo anterior, se debe cumplir con las siguientes políticas:

a) Los servidores públicos, colaboradores o terceros, que utilicen sus dispositivos personales al interior del Icetex para ejecutar sus funciones u obligaciones se conectaran a la red definida por el Instituto.
b) Al conectar el dispositivo personal a la red del Icetex, el servidor público, colaborador o tercero propietario del dispositivo acepta los controles establecidos en este documento.
c) Todo dispositivo personal que ingrese a las instalaciones del Icetex deberá ser registrado en la bitácora, ubicada en el área de recepción.

d) Toda la información relacionada con la ejecución de las funciones u obligaciones contractuales del servidor público, colaborador o tercero contenida en los dispositivos personales debe estar almacenada en el repositorio institucional de cada dependencia de la entidad de acuerdo con los lineamientos de gestión del conocimiento que defina el Grupo de Talento y Desarrollo Humano de la Secretaría General para preservar la memoria institucional
e) Es responsabilidad directa del colaborador, contratista o tercero garantizar la protección, confidencialidad y adecuado manejo de la información del Icetex que se encuentre bajo su custodia en dispositivos personales. Esta obligación incluye la implementación de medidas de seguridad física y digital que prevengan el acceso no autorizado, la pérdida, alteración o divulgación indebida de dicha información.
f) El servidor público, colaborador o tercero propietario del dispositivo personal, deberá tener en cuenta las buenas prácticas de seguridad de la información incluyendo: contar con una contraseña para el inicio de sesión en el equipo y cerrar la sesión cada vez que finalice su labor o que se deba ausentar de su área o puesto de trabajo.
g) Cuando el servidor público, colaborador o tercero utilice el dispositivo personal en lugares públicos, debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas, así mismo, evitar la conexión a redes públicas (aeropuertos, centros comerciales, hoteles, entre otros), las cuales no cuentan con ningún tipo de monitoreo o seguridad y representan un riesgo para la seguridad de la información del Instituto.
h) Una vez se autorice la conexión de un dispositivo a la red de dominio Icetex (VPN, office 365, entre otros), la entidad tendrá acceso para visualizar y monitorear la conexión hacia la red del Instituto.
i) La VOT no dará soporte técnico a los dispositivos personales, en caso de ser necesario a través de la mesa de servicio dará soporte a las aplicaciones institucionales que el colaborador tenga asignado el acceso.
j) La VOT definirá e implementará los mecanismos de seguridad necesarios para monitorear los dispositivos personales con el fin de garantizar la seguridad y buen uso de la informaciòn que se accede desde estos dispositivos.

6.9. Devolución de activos de información

El Grupo de Recursos Físicos y Gestión Documental establecerán e implementarán los lineamientos para la devolución de los activos de información (físicos y digitales), teniendo en cuenta:

a) Cuando un servidor público, colaborador o tercero termina o cambia la relación contractual o laboral con el Icetex, debe entregar al jefe de área, supervisor o área designada los recursos tecnológicos y los activos de información que le fueron entregados en el momento de su vinculación o durante la relación contractual o laboral.
b) El colaborador debe realizar la devolución a Gestión Documental de los expedientes y/o informaciòn suministrada para la ejecución de las actividades laborales o contractuales.

6.10. Clasificado y etiquetado de la información

a) Los niveles de clasificación y etiquetado de la información establecidos en el Icetex son “Información Pública”, “Información Pública Clasificada” e “Información Pública Reservada”, lo cual aplica para la información física como para la información digital.
b) La información se clasifica y etiqueta de acuerdo con lo establecido en la guía para la clasificación de activos de información - G176, el procedimiento para identificar y clasificar activos de información- E2-1-13 y la guía para el manejo de los activos de información y etiquetado - G180.
a) Todos los servidores públicos y colaboradores del Icetex son responsables de clasificar y etiquetar la información que producen en cumplimiento de las funciones y obligaciones asignadas.
b) Los documentos digitales deben tener un espacio para la clasificación (Pública, Clasificada, Reservada) de la información según corresponda.
c) El área de Gestión Documental será responsable de definir y establecer los lineamientos técnicos para el etiquetado de la información física del Icetex. Estos lineamientos deberán garantizar que todos los documentos cuenten con el etiquetado correspondiente, conforme al tipo de información que contienen, su nivel de confidencialidad, y su clasificación institucional.
d) No está permitido publicar en carteleras físicas, digitales o cualquier otro espacio del Icetex, información que contengan:
    - Datos personales privados, semiprivados o sensibles,

- Documentos sin etiquetado.
- Documentos con etiquetado “Clasificada” o “Reservada”

e) No debe permanecer en las impresoras documentos impresos que contengan información etiquetada como “Clasificada” o “Reservada”. Estas deberán ser retirados de manera inmediata por el servidor público, colaborador o tercero responsable de la impresión, con el fin de evitar accesos no autorizados, pérdidas o divulgaciones indebidas. En lo posible esta información no debería imprimirse.
f) Antes de depositar cualquier documento en el contenedor de basura, se deberá verificar si contiene información etiquetada como “Clasificada” o “Reservada”. En caso afirmativo, el documento deberá ser eliminado en su totalidad mediante métodos seguros de destrucción (trituradora, incineración).
g) Toda información que contenga datos personales deberá estar sujeta a las disposiciones legales contenidas en la Ley 1581 de 2012 y las demás que la complementen, modifiquen o sustituyan y la Política de Tratamiento de Datos Personales del Icetex (publicada en el portal web del instituto).

5.10.1. Ley de Transparencia

a) La oficina de riesgos genera los “Instrumentos de Gestión de la Información Pública” y tramita su publicación.
b) Los lideres de cada proceso actualizan periódicamente la información pública que están bajo su responsabilidad a través de los procedimientos establecidos.
c) La Oficina Comercial y Mercadeo recibe las solicitudes de acceso a la información que solicita la ciudadanía y otros terceros. Las áreas a quienes corresponda y la Oficina de Riesgos atienden estos requerimientos y dan respuesta a los mismos.

6.11. Transferencia de información

a) La Dirección de Tecnologia – VOT, aplicará los lineamientos establecidos en el procedimiento Intercambio de información digital con terceros - E2-1-16, así como los demás procedimientos, instructivos y políticas vigentes que regulen el tratamiento, transmisión y protección de la información institucional en entornos digitales.
b) Todo intercambio de información del Icetex con terceros, debe ser respaldado por un contrato, acuerdo, convenio, memorando de entendimiento o cualquier otro instrumento legal que se defina para la transmisión o transferencia de datos que incluya cláusulas de confidencialidad, tiempos, responsabilidades finalidad, alcance, tratamiento y no divulgación de la información proporcionada.
c) La información recibida o enviada a otra entidad, debe ser salvaguardada bajo las condiciones que esta exige de acuerdo con su naturaleza.
d) La información “Pública Clasificada” y “Publica Reservada” que se intercambie, debe estar cifrada. Este control lo proporcionará la VOT.
e) Los propietarios y custodios de los activos de información deben proteger la confidencialidad, integridad y privacidad de la información durante la transferencia de la información, estableciendo canales seguros que eviten la divulgación o modificación no autorizada de la información.
f) Los acuerdos de intercambio de información bajo el concepto de interoperabilidad, como mínimo deben tener en cuenta:
    - Métodos de autenticación.
    - Contar con protocolos de transferencia seguros.
    - Acordar los respectivos anexos técnicos donde se defina claramente la información a intercambiar, medios, periodicidad, diccionarios de datos, entre otros aspectos.
    - Tiempos y duración del intercambio de la información.
    - Personal autorizado de las partes involucradas
    - Alcance de la información a intercambiar.
    - Cumplir con los lineamientos establecidos en el marco de interoperabilidad de gobierno digital y en el modelo de Servicios Ciudadanos Digitales o los que los complementen o actualicen.
    - Definir los Acuerdos de Nivel de Servicio (ANS) que contemplen características de seguridad necesarias.
    - Asegurar que existan cláusulas de Tratamiento de Datos Personales.
g) Mensajería Electrónica:
   La Dirección de Tecnologia – VOT proporcionará un servicio idóneo y seguro para la ejecución de las actividades del Icetex que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones por este medio. Por lo cual debe tener en cuenta:
    - Implementar en la plataforma de correo electrónico procedimientos y controles necesarios que permitan detectar y proteger la integridad de la información que viaja a través de esta plataforma.

- Los mensajes electrónicos deben contar con mecanismos de protección contra código malicioso, tales como antivirus actualizados, filtros anti-phishing, y sistemas de detección de amenazas.

h) El área de Gestión Documental establecerá las directrices técnicas y operativas para la retención, disposición final y transferencia de la información física del Icetex, de acuerdo con la normativa legal vigente y lo dispuesto por el Archivo General de la Nación.

6.12. Control de Acceso Lógico

a) La gestión de accesos a los sistemas de información, aplicaciones institucionales, bases de datos entre otros, se realiza de acuerdo con lo establecido en los procedimientos gestión de accesos y retiro de servicios A7-1-05 y Asignación/ retiro de accesos a sistemas de información -IES e IES ORI A7-1-14.
b) El supervisor del contrato o jefe inmediato debe solicitar a la VOT la creación, modificación, suspensión e inactivación de los accesos a los sistemas de información, servicios tecnológicos e infraestructura, de acuerdo con las funciones u obligaciones de los colaboradores según lo establecido en el procedimiento gestión de accesos y retiro de servicios A7-1-05.
c) El acceso a la información, sistemas de información y/o aplicaciones de la entidad por parte de los servidores públicos, contratistas y terceros debe darse bajo el principio del mínimo privilegio; es decir que cada usuario solo debe tener acceso a lo que necesita conocer de acuerdo con sus actividades y rol dentro del Instituto.
d) La creación y modificación de usuarios en la infraestructura tecnológica son responsabilidad del colaborador que designe la Dirección de Tecnología – VOT y debe seguir los procedimientos correspondientes.
e) La Dirección de Tecnología – VOT realizara revisiones periódicas de acuerdo con los criterios definidos para los diferentes sistemas de información y servicios tecnológicos del Instituto, asi como los usuarios con privilegios de administración, con el fin de garantizar que se desactiven los usuarios que no tengan vinculación laboral o contractual vigente y, además, verificar que los usuarios habilitados cuenten con los permisos y privilegios de acuerdo con sus funciones u obligaciones contractuales.
f) El acceso a los sistemas de información del instituto debe realizarse a través de un usuario preferiblemente el asignado por el directorio activo, el cual permita identificar la persona, asociarla con sus actividades y hacerlos responsables de sus acciones.
g) El propietario de los sistemas de información o servicios debe autorizar o denegar el acceso y privilegios requeridos.
h) Las acciones ejecutadas por los usuarios en los sistemas de información quedarán registradas en los sistemas para conservar esta trazabilidad, lo anterior para efectos de auditoría.
i) La Dirección de Tecnología – VOT realizará monitoreo al uso, gestión y autenticación de las cuentas de usuario asignadas. La Oficina de Riesgos como responsable de la seguridad de la información también podrá gestionar la trazabilidad del buen uso que realizan los servidores públicos en las cuentas de usuario asignadas.
j) La Dirección de Tecnología – VOT definirá e implementará los controles necesarios para garantizar un inicio de sesión seguro, incluyendo mecanismos de autenticación robustos, validación de credenciales, protección contra accesos no autorizados, doble factor de autenticación y cumplimiento de las políticas internas de seguridad de la información.
k) La VOT establecerá los mecanismos formales para documentar y mantener actualizado el registro de usuarios con privilegios y/o superusuarios que acceden a los servicios tecnológicos, sistemas de información e infraestructura institucional. Este registro debe incluir la identificación del usuario, nivel de acceso, justificación del privilegio, fecha de otorgamiento y responsable de la autorización. Asimismo, deberá ser revisado periódicamente para garantizar su vigencia y/o detectar accesos innecesarios.
l) La Dirección de Tecnología – VOT definirá, documentará y aplicará la metodología para la codificación segura tanto para los desarrollos inhouse como para los desarrollos subcontratados con el fin de mitigar posibles vulnerabilidades.
m) La Dirección de Tecnología – VOT definirá los lineamientos para el acceso al código fuente aplicable tanto para desarrollos internos (inhouse) como a desarrollos subcontratados.

6.13. Gestión de identidades y autenticación – Contraseñas

a) La VOT establecerá los mecanismos para asegurar que solo identidades autorizadas y verificadas tengan acceso a los recursos del Icetex y que dicho acceso sea único, controlado y trazable durante todo su ciclo de vida.
b) La gestión de contraseñas se realiza conforme a los establecido en las guías autogestión de contraseñas G161 y contraseñas seguras G71.
c) Todas las contraseñas son de uso personal e intransferible, no se deben compartir con ninguna persona dentro o fuera del Instituto por ningún medio, los colaborades son responsables de la custodia, no divulgación y uso de estas.

d) Ningún usuario podrá acceder a un sistema de información o servicio tecnológico utilizando la cuenta y contraseña de otro usuario.
e) Los colaboradores son responsables de las acciones ejecutadas con sus usuarios en los sistemas de información del Instituto.
f) No está permitido almacenar en los navegadores de internet u otros sistemas las credenciales de acceso para ser recordada automáticamente por estos.
g) No esta permito registrar contraseñas en medios inseguros, tales como post-it físicos, agendas personales, notas rápidas del sistema operativo o cualquier otro formato accesible a personas no autorizadas.
h) Al definir las contraseñas, se debe evitar el uso de palabras comunes, nombres fácilmente deducibles por terceros, así como cualquier dato personal o familiar, tales como fechas de cumpleaños, números de teléfono, documentos de identidad, nombres de familiares, mascotas u otra información asociada al usuario. Las contraseñas deben ser robustas, contener una combinación de caracteres alfanuméricos y símbolos, con el fin de minimizar el riesgo de accesos no autorizados.
i) En caso de ser divulgada la contraseña por error, esta debe ser cambiada de inmediato y reportar el incidente por los canales establecidos en el procedimiento para reportar y gestionar incidentes de seguridad de la información E2-1-14.
j) No se debe utilizar usuarios genéricos como (root, superuser etc.…) sin excepción.
k) En las aplicaciones o servicios que sea posible, implementar la autenticación por doble o triple factor de autenticación.
l) Toda contraseña por defecto o suministrada por algún fabricante o sistema deberá ser reemplazada.
m) Las contraseñas de los administradores de aplicaciones deberán ser almacenadas en un lugar seguro o en un sistema de gestión de contraseñas institucional (keypass). El acceso a dichas credenciales, en caso de ser requerido, deberá realizarse de manera conjunta o con aprobación explícita del jefe inmediato, garantizando trazabilidad y control. Una vez revelada la contraseña, esta deberá ser cambiada de inmediato y nuevamente resguardada en un lugar seguro.

6.14. Gestión con proveedores

Asegurar una adecuada gestión con los proveedores de infraestructura de TI y con los que manejan información sensible del Icetex, con el propósito dar cumplimiento a las políticas, procedimientos y lineamientos de seguridad y privacidad de la información, teniendo en cuenta lo siguiente

Gestión Contractual:

a) Establecerá el medio idóneo para verificar con los proveedores los requisitos legales y regulatorios relacionados con la protección de datos personales, los derechos de propiedad intelectual y derechos de autor.
b) Incluirá en los contratos con proveedores la cláusula de “Compromiso de Confidencialidad”, con el fin de asegurar la información del Instituto.
c) Los contratos suscritos de servicios tecnológicos deberán incorporar de manera explícita, la obligación de cumplir con las políticas de seguridad digital del Icetex.

Dirección de Tecnología – VOT:

d) Cumplirá con los lineamientos establecidos por Gestión Contractual para realizar la contratación con proveedores.
e) Establecerá los mecanismos y asignación de permisos cuando un proveedor requiera tener acceso a la información a través de la infraestructura tecnológica del Icetex.
f) Realizará seguimiento al acceso a la información por parte de los proveedores a los recursos de almacenamiento o procesamiento, de acuerdo con las políticas y procedimientos de seguridad y privacidad de la información del Icetex.
g) Verificará de manera mensual el cumplimiento de los Acuerdos de Nivel de Servicio establecidos con los proveedores de tecnología (cuando aplique).
h) Supervisará las conexiones de los equipos de cómputo y dispositivos móviles utilizados por los proveedores, con el fin de garantizar su adecuado acceso y uso dentro de la red de datos y los recursos tecnológicos del Icetex, conforme a los protocolos de seguridad, privacidad de la información y normativas vigentes.
i) Gestionar los cambios de infraestructura, aplicativos y servicios tecnológicos que son soportados por proveedores, de acuerdo con lo establecido en el procedimiento control de cambios y despliegue A7-1-12.
j) Gestionar los incidentes de infraestructura, aplicativos y servicios tecnológicos que son soportados por proveedores de acuerdo con lo establecido en el procedimiento para reportar y gestionar incidentes

de seguridad de la información E2-1-14.

k) Establecer y monitorear las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los proveedores de servicios.
l) Identificar las vulnerabilidades asociadas al producto o servicio suministrado por el proveedor y gestionarlas de acuerdo con el procedimiento pruebas de vulnerabilidad A7-1-11.
m) La VOT realizará como mínimo dos veces al año, la evaluación de seguridad de la información a los proveedores que gestionan información sensible o que operan sistemas críticos, con el fin de verificar el cumplimiento de los controles establecidos y la adecuada protección de los activos institucionales.

Proveedores deberán:

n) Informar de manera inmediata y efectiva al supervisor del contrato los incidentes de seguridad y privacidad de la información que pongan en riesgo la confidencialidad, integridad, disponibilidad o privacidad de los activos de información del Icetex.
o) Divulgar al personal asignado para la ejecución de las actividades, las políticas y procedimientos de seguridad y privacidad de la información del Icetex.
p) Informar oportunamente al Icetex cualquier cambio que afecte el suministro de los servicios como: controles implementados, mejoras, nuevas aplicaciones, modificación o actualizaciones de las políticas o procedimientos, nuevas tecnologías, ubicación física, contratación externa o interna, entre otros.
q) En caso de que la ejecución del servicio contratado implique el uso de programas o software, estos deberán contar con las licencias correspondientes, garantizando su legalidad, vigencia y conformidad con la normativa aplicable en materia de propiedad intelectual, seguridad de la información y estándares institucionales.
r) Realizar la devolución de los activos físicos y/o lógicos, generados o modificados, durante la ejecución contractual.
s) Dar cumplimiento a los requisitos legales y reglamentarios para la protección de datos personales, derechos de propiedad intelectual, derechos de autor y los que apliquen a razón del cumplimiento contractual.
t) Utilizar la información que reciban o conozcan del Icetex, exclusivamente para la ejecución contractual.
u) Definir, documentar y mantener actualizado un plan de recuperación y contingencia tecnológica que contemple medidas técnicas, operativas y administrativas ante eventos que puedan afectar el cumplimiento contractual.
v) Propagar en la cadena de suministro las buenas prácticas, políticas y documentación relacionada con la seguridad de la información del Icetex.

6.15. Seguridad de la información para el uso del servicio en la nube:

El Icetex propende por mantener la seguridad de sus activos de información al autorizar el uso de servicios en la nube con el fin de garantizar la disponibilidad, privacidad, confidencialidad, integridad y cumplimiento de los requisitos legales en materia de protección de la información, teniendo en cuenta:

a) Estas políticas aplican a los servicios de nube contratados y utilizados por los procesos del Icetex.
b) La adopción de servicios en la nube que operen bajo licenciamiento gratuito o de código abierto deberá contar con la aprobación previa del Comité de Control de Cambios, instancia que evaluará dicha solicitud en concordancia con los lineamientos establecidos en la estrategia de Gobierno Digital.
c) Los contratos suscritos de servicios en la nube deberán cumplir con las políticas que se mencionan en el numeral 5.14 Gestión con Proveedores de este documento.
d) Al utilizar plataformas internacionales para el almacenamiento y/o procesamiento de información personal en la nube, el Icetex contará con la autorización del titular del tratamiento datos personales. En ningún caso se permitirá el almacenamiento de datos personales en la nube sin dicha autorización, especialmente cuando implique la transmisión internacional de información.
e) La Oficina de riesgos en conjunto con la VOT realizara la identificación, valoración y evaluación de los riesgos asociados al uso de servicios en la nube.

Responsabilidades de la Dirección de Tecnología – VOT:

f) Establecer los criterios para seleccionar los servicios en la nube y el alcance del uso del servicio en la nube.
g) Definir los Roles y responsabilidades relacionadas con el uso y la gestión del servicio en la nube.

h) Aplicar los lineamientos para la gestión de incidentes de seguridad de la información en el servicio en la nube.
i) Realizar monitoreo, revisión y evaluación del uso de los servicios en la nube para identificar y gestionar riesgos de seguridad de la información.
j) Proveer servicios de copia de respaldo para la información del Icetex que está autorizada para almacenamiento en la nube.
k) Proveer y administrar copias de respaldo de la información almacenada en las carpetas compartidas institucionales, de acuerdo con las políticas y lineamientos de seguridad digital y gestión de la información del Instituto, garantizando su disponibilidad, integridad y recuperación ante incidentes, fallas o pérdida de información.
l) Implementar controles de seguridad digital para preservar los accesos a los servicios en la nube autorizados por el Instituto.
m) Definir e implementar plan de contingencia para preservar la información almacenada en servicios de computación en la nube.
n) Mantener el inventario de los servicios autorizados que se encuentren alojados en la nube.
o) Realizar monitoreo de seguridad digital utilizando las tecnologías de correlación aprovisionadas por el Instituto.
p) Asegurar el servicio en la nube y herramientas emergentes contenidas como servicios de inteligencia artificial se diseñen, implementen y operen conforme a las políticas de seguridad digital y gestión de riesgo institucional, procurando por la implementación de controles de protección de datos como el cifrado de datos en tránsito como en reposo y herramientas de monitoreo para detectar vulnerabilidades y amenazas en tiempo real.

Responsabilidad de los Colaboradores:

q) Solicitar a la Dirección de Tecnología el uso de servicios en la nube.
r) La información que se almacene en la nube de carácter “Pública Clasificada”, “Pública Reservada” y que contenga datos personales debe permanecer cifrada de acuerdo con las políticas de cifrado institucional.
s) Utilizar el servicio en la nube autorizado, únicamente para el cumplimiento de las labores asignadas institucionalmente.
t) Evitar ingresar al servicio en la nube desde equipos de cómputo de uso inseguros como café internet o centros de alquiler de equipos públicos, aeropuertos, hoteles, entre otros.
u) No está permitido almacenar en la nube información sujeta a derechos de autor (videos, imágenes, audio, libros, entre otros).

6.16. Gestión de incidentes

a) La VOT gestionara los incidentes de tecnología de acuerdo con lo establecido en el Procedimiento gestión de incidentes – A7-1-13.
b) La Oficina de Riesgos apoyara la gestión de incidentes de seguridad de la información de acuerdo con el Procedimiento para reportar y gestionar incidentes de seguridad de la información- E2-1-14.
c) Es responsabilidad de todos los colaboradores reportar oportunamente y por los canales establecidos, cualquier evento o debilidad de seguridad de la información detectada o que se tenga sospecha que afecte o ponga en riesgo los activos de información.
d) La Oficina de Riesgos en conjunto con las áreas involucradas realizarán el análisis, contención, recuperación y normalización de la operación en caso de que un incidente afecte la continuidad del negocio del Instituto.

6.17. Seguridad de la información durante una interrupción

La Dirección de Tecnología – VOT incluirá en el Plan de Recuperación de Desastres los requerimientos y controles de seguridad de la información que deben cumplirse durante situaciones de contingencia o interrupción de los servicios institucionales. Así mismo, será responsable de implementar y mantener:

a) Los controles de seguridad de la información, sistemas y herramientas de apoyo dentro de los planes de continuidad del negocio y de las TIC.
b) Los Procesos para preservar la efectividad de los controles de seguridad de la información existentes durante la interrupción.

Las medidas de compensación para los controles de seguridad de la información que no puedan ejecutarse durante la interrupción, con el fin de garantizar un nivel aceptable de seguridad durante la interrupción

6.18. Preparación de las TIC para la continuidad del negocio

La Dirección de Tecnología – VOT aplicara la guía Plan de recuperación de desastres de TI-G234, y los procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados incorporando los controles de seguridad digital, como también:

a) Realizar cada año el Análisis de Impacto de Negocio – BIA identificando la criticidad de los servicios tecnológicos, sistemas de información e infraestructura critica del instituto.
b) Establecer un Plan de Recuperación ante Desastres Tecnológicos que consolide, articule y priorice las actividades necesarias para garantizar la continuidad operativa de los servicios críticos soportados por las Tecnologías de la Información y las Comunicaciones (TIC), identificadas en el Análisis de Impacto al Negocio (BIA).
c) Asignar recurso humano, tecnológico y económico para desarrollar e implementar la continuidad tecnológica del Icetex.
d) Definir las estrategias de continuidad de Tecnologías de la Información y las Comunicaciones (TIC),
e) Realizar las pruebas de continuidad tecnológica y/o Plan de Recuperación de Desastres -DRP y documentar el resultado.
f) Responder de manera oportuna antes de que se produzca una interrupción en los servicios TIC como después de la detección de cualquier incidente que pueda generar afectación o interrupción en la prestación de los servicios del Icetex.
g) Los productos y/o servicios que sean subcontratados por terceros deben disponer de planes de continuidad para no afectar el cumplimiento de la misionalidad del Instituto, principalmente los proveedores críticos de la operación.
h) La VOT realizara seguimiento por lo menos una vez al año a la ejecución de las pruebas de continuidad tecnológica y/o DRP de los proveedor críticos.
i) Socializar y comunicar oportunamente al ICETEX, a través de los canales institucionales definidos, la activación del Plan de Continuidad del Negocio o del Plan de Recuperación ante Desastres Tecnológicos (DRP) cuando se presenten fallas o incidentes que afecten los sistemas de información o los servicios tecnológicos del Instituto.

6.19. Requisitos legales y Derechos de Propiedad Intelectual

La Dirección de Tecnología – VOT definirá controles con el objetivo de proteger adecuadamente la propiedad intelectual del Icetex, tanto propia como la de terceros, teniendo en cuenta:

a) Asegurar que todo el software que se ejecuta en el Instituto cumpla con los requisitos de derechos de autor y licenciamiento de uso.
b) Mantener un inventario de software y sistemas de información que se encuentran permitidos en las estaciones de trabajo, servidores o equipos móviles del Instituto para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado corresponda únicamente al permitido. Este inventario debe contener la evidencia de la propiedad de las licencias.
c) La gestión y seguimiento de software licenciado, libre y no autorizado en los equipos de cómputo del Icetex se realizará conforme a lo establecido en la G172 Guía Instalación/desinstalación de software.
d) Definir controles que garanticen la continuidad en el uso del software bajo el riesgo de desaparición del proveedor.
e) Establecer la reserva de los derechos de propiedad intelectual, donde se evidencia la reserva de todos los derechos existentes sobre el sitio web institucional.
f) Para las aplicaciones Web del Icetex que son ejecutadas de forma remota por los usuarios, no siendo necesaria la descarga o instalación de software en su equipo, se debe aclarar en la licencia de uso una protección tanto a la aplicación, como a los contenidos que son ejecutados a través de esta.
g) Definir e implementar mecanismos que impidan la instalación de software no autorizado por parte de los usuarios finales.
h) Vigilar el software instalado por usuarios privilegiados como administradores de los equipos de cómputo y servidores.

6.20. Protección de registros

La VOT y Gestión documental dará lineamientos para cumplir con la protección de registros contra pérdida, destrucción y falsificación aplicando los requisitos legislativos, reglamentarios y los demás que apliquen, asi como:

a) Establecer directrices sobre retención, almacenamiento, manipulación y eliminación de registros e información física y digital.
b) Establecer e implementar controles para proteger los registros en su confidencialidad, integridad y disponibilidad.
c) Establecer procedimientos de almacenamiento a largo plazo y manipulación de los registros físicos y digitales.

6.21. Privacidad y Protección de la Información Personal

a) El Icetex cuenta con la política de tratamiento de datos personales la cual se encuentra publicada en la página web de la entidad.
b) La Dirección de Tecnología – VOT establecerá los controles necesarios para proteger la información personal de beneficiarios, colaboradores, servidores públicos, proveedores y demás terceros. Asimismo, será responsable de implementar y ejecutar los controles relacionados con el almacenamiento de bases de datos o cualquier otro repositorio de información, con el propósito de evitar su divulgación, alteración o eliminación sin la autorización correspondiente.
c) La Dirección de Tecnología – VOT facilitará a todos los procesos de la entidad los controles adecuados para la custodia de las bases de datos que contienen autorizaciones de tratamiento de datos personales, garantizando su protección conforme a la normativa vigente.

6.22. Revisión Independiente de la Seguridad de la Información

a) Las Oficina de Control Interno del Icetex realizará auditorías internas para comprobar el cumplimiento de controles, políticas, procesos y procedimientos establecidos para el sistema de seguridad y privacidad de la información de acuerdo con lo establecido en el Procedimiento plan y programa anual de auditorías - EV1-02-04.
b) Los líderes de los procesos deberán asegurar que la documentación (procedimientos, guías, manuales, entre otros), de seguridad y privacidad de la información que son de responsabilidad del proceso se aplique y cumpla de manera oportuna y correctamente.
c) Es responsabilidad de todos los colaboradores cumplir las políticas de seguridad y privacidad de la información mencionadas en este manual como la documentación dispuesta en la herramienta documental (procedimientos, guías, manuales, entre otros).

6.23. Procedimientos Operativos Documentados

a) Los documentos que definen los lineamientos para gestionar la seguridad y privacidad de la información se encuentran disponibles en la herramienta habilitada por la entidad.
b) La VOT y el equipo de seguridad de información de la Oficina de Riesgos, velará por documentar y mantener actualizado los procedimientos operativos para asegurar la disponibilidad, integridad y confidencialidad de la información.

6.24. Selección Personas

a) El Grupo de Talento y Desarrollo Humano definirá y aplicará mecanismos de verificación de antecedentes y perfil del personal para los procesos de selección o vinculación de los servidores públicos, dando el cumplimiento a la normativa para el empleo público y los lineamientos institucionales.
b) El proceso de Gestión Contractual definirá y aplicará mecanismos para la revisión de los antecedentes y perfil del personal previo a la contratación por prestación de servicios, de acuerdo con lo que dicta la ley y la reglamentación vigente.
c) El Grupo de Talento y Desarrollo Humano y el Grupo de Gestión Contractual deberán establecer los mecanismos o controles necesarios para proteger la confidencialidad y reserva de la información contenida en las historias laborales y expedientes contractuales respectivamente, de acuerdo con los lineamientos definidos por el Grupo de Gestión Documental.

6.25. Términos y Condiciones del Empleo

a) El proceso de Gestión Contractual definirá los términos y condiciones del contrato, en el cual se establezca las obligaciones que el contratista debe cumplir en materia de seguridad y privacidad de la información.

b) El Grupo de Talento y Desarrollo Humano definirá dentro del proceso de selección o vinculación de servidores públicos, el estudio de seguridad, la verificación de las referencias laborales y la validación de la veracidad de los títulos académicos formales, conforme a los lineamientos institucionales.

6.26. Conciencia de Seguridad de la Información, Educación y Formación:

a) El Grupo de Talento y Desarrollo Humano, incluirá temas de seguridad y privacidad de la información en la inducción y reinducción de los servidores públicos.
b) El Grupo de Talento y Desarrollo Humano planificará charlas de sensibilización y formación de seguridad y privacidad de la información a través del Plan Institucional de Capacitación, previamente solicitados por la VOT y la Oficina de Riesgos, en el marco del diagnóstico de necesidades de capacitación.
c) La Oficina de Riesgos a través del equipo de seguridad de la información, sensibilizará a los colaboradores en temas relacionados con la seguridad y privacidad de la información.
d) La Oficina de Riesgos a través del equipo de seguridad de la información realizará ejercicios de simulaciones periódicas de correos falsos (phishing) para entrenar a los colaboradores en la identificación de riesgos, así como evaluaciones que permitan medir qué tan conscientes somos o que tan comprometida está la organización frente a la seguridad de la información.

6.27. Proceso Disciplinario

En caso de incumplimiento de las políticas de seguridad y privacidad de la información, se aplicará lo establecido en el procedimiento procesos disciplinarios - A5-1-01 y los lineamientos destinados por el Icetex para tal fin.

6.28. Responsabilidades después de la Terminación o Cambio de Empleo

El Grupo de Talento y Desarrollo Humano, y Gestión Contractual definirán y aplicarán lineamientos para las responsabilidades y deberes de seguridad y privacidad de la información que permanecen válidos después de la terminación o cambio de empleo, teniendo en cuenta:

a) El supervisor del contrato y/o jefe inmediato, informará de manera oportuna a la VOT las novedades que se presenten de los colaboradores (terminación anticipada de contrato, cesión de contrato, jubilación, retiro, cambio de funciones, entre otras) con el fin de inhabilitar, suspender o modificar los accesos físicos y lógicos asignados de acuerdo con lo establecido en el procedimiento gestión de accesos y retiro de servicios - A7 -1-05.
b) El Grupo de Talento y Desarrollo Humano y el Grupo de Gestión Contractual definirán la documentación y entregables requeridos para la desvinculación de los servidores públicos y contratistas de prestación de servicios respectivamente.

6.29. Acuerdos de Confidencialidad o no Divulgación

a) El Grupo de Talento y Desarrollo Humano y Gestión Contractual incluirán dentro del acto administrativo de nombramiento o del contrato, este último para el caso de contratistas de prestación de servicios, cláusulas relacionadas con el compromiso de confidencialidad de la Información y la autorización del tratamiento de datos personales.

b) Cada colaborador deberá firmar el formato Autorización de tratamiento de datos personales contratistas-F318, Autorización de tratamiento de datos personales funcionarios-F422 y el Compromiso de confidencialidad y no divulgación de la información F-557. Dichos documentos deberán reposar en la historia laboral o expediente contractual según sea el caso.

6.30. Trabajo Remoto

a) El Grupo de Talento y Desarrollo Humano gestionará el teletrabajo de acuerdo con lo establecido en el procedimiento de Teletrabajo - A3-3-25 y definirá los demás lineamientos necesarios para realizar el teletrabajo, trabajo remoto o trabajo en casa, con el fin de proteger la información que se accede, procesa o almacena.
b) La VOT proveerá los recursos tecnológicos y definirá los lineamientos de seguridad de la información los cuales están consignados en el F584 Acuerdo de Voluntariedad
c) La VOT monitoreará el uso de los recursos e infraestructura dispuesta para el teletrabajo, con el fin de prevenir y detectar vulnerabilidades, ataques cibernéticos y otras amenazas.
d) Es responsabilidad de los colaboradores almacenar la información institucional en los repositorios autorizados por el Icetex.

e) En caso de que el servidor público utilice su equipo personal para realizar trabajo en casa, es necesario cumplir con las siguientes condiciones:
    - Mantener actualizado el sistema operativo.
    - Garantizar el buen funcionamiento del equipo.
    - Contar con antivirus instalado, activo, actualizado y licenciamiento de software instalado en dicho equipo de cómputo.

   Así mismo, dar cumplimiento a las políticas "*Dispositivos Personales – Trae Tu Propio Equipo- BYOD*" y las demás políticas mencionadas en el presente manual.
f) Es responsabilidad del colaborador cumplir con las medidas de seguridad adoptadas por el Icetex para garantizar la confidencialidad, el secreto y la integridad de los datos personales a los que tenga acceso en el ejercicio de sus funciones, absteniéndose de divulgarlos, transferirlos o cederlos a terceros bajo cualquier modalidad, salvo autorización expresa y por escrito del titular o en cumplimiento de una obligación legal.
g) El colaborador deberá reportar a su jefe inmediato o supervisor cualquier riesgo y/o incidentes de ciberseguridad, seguridad y privacidad de la información que se lleguen a presentar en su contexto de teletrabajo o trabajo en casa.

6.31. Informe de Eventos de seguridad de la Información

Los colaboradores del Icetex reportarán los eventos e incidentes de seguridad de la información a través de los canales establecidos en el procedimiento para reportar y gestionar incidentes de seguridad de la información - E2-1-14.

6.32. Monitoreo Seguridad Fisica

El Grupo de Recursos Físicos velará por que los servidores públicos, contratistas y visitantes del Icetex, cumplan las siguientes indicaciones:

a) Todo servidor público, contratista o pasante deberá estar carnetizado y portarlo mientras se encuentre en las instalaciones del Icetex.
b) Todo servidor público, contratista o pasante sin carné, debe registrarse en la recepción de las sedes del Icetex, presentando su documento de identidad para el ingreso al Instituto, así mismo, deberá proporcionar la información solicitada por el personal de vigilancia, en concordancia a lo establecido en la Política de Protección de Datos del Icetex.
c) El ingreso de los visitantes (proveedores o terceras partes) debe estar autorizado por un colaborador del Icetex, este debe acompañarlo durante su estadía en el Instituto, así mismo, el visitante debe portar un elemento visible que lo identifique como visitante.
d) El ingreso y salida de todas las instalaciones del Icetex está condicionado a la revisión obligatoria y sin excepción de bolsos y demás paquetes, así como la revisión mediante detector de metales o demás medios tecnológicos por parte del personal de vigilancia, destinados para este fin.
e) Los servidores públicos, contratistas, terceros y visitantes sin excepción, deben registrar los elementos tecnológicos (computadores, discos duros, ente otros) en las bitácoras de vigilancia a la entrada y salida del Icetex.
f) Todo servidor público y contratista una vez terminado el vínculo con el Instituto, debe entregar el carnet al Grupo de Talento y Desarrollo Humano, con el fin de controlar el acceso y permanencia en las instalaciones de la Entidad. Los servidores públicos lo harán al momento de reportar el "Formato Informe de Entrega de Cargo" (F414), y los contratistas al momento de finalizar el vínculo contractual con la entrega del "Formato Paz y Salvo Contratistas Prestación de Servicios Profesionales o Apoyo a la Gestión - Persona Natural" (F509).
g) El Icetex debe contar con un sistema de videovigilancia que incluya cámaras de seguridad estratégicamente ubicadas en sus instalaciones. Dicho sistema debe ser monitoreado de manera continua por el personal de vigilancia autorizado, con el fin de garantizar la seguridad física de las personas, los bienes y la infraestructura institucional.
h) El proceso de Gestión Administrativa gestionara la adecuación y mantenimiento de la infraestructura física del Icetex.
i) Todo servidor público, contratista, pasante, personal de proveedores y visitante es responsable del cuidado, custodia y protección de sus bienes personales durante su permanencia en las instalaciones del Icetex. La entidad no se hace responsable por la pérdida, daño o sustracción de objetos personales.

6.33. Prohibición contra Amenazas Públicas y Ambientales

La Dirección de Tecnología-VOT realizará seguimiento a las condiciones ambientales como la temperatura y humedad, identificando oportunamente las situaciones que puedan afectar negativamente las instalaciones del datacenter con el fin de tomar las acciones pertinentes.

6.34. Trabajo en Áreas Seguras

a) Toda persona que requiera ingresar a los centros de cableado y datacenter deberá, de manera previa, registrarse en la bitácora de ingreso correspondiente.
b) Todo trabajo o mantenimiento de redes eléctricas, cableado de datos y voz, pruebas a los sistemas de UPS, aires acondicionados, plantas eléctricas y sistemas contra incendios, entre otros, deben ser realizados por personal especializado, si lo realiza un externo debe estar identificado y acompañado por un colaborador de la VOT.
c) En los centros de cableado y datacenter no se deben almacenar elementos ajenos a los requeridos de acuerdo con la actividad que se realiza en esta área.
d) La VOT será responsable de establecer, implementar y monitorear los controles preventivos y correctivos necesarios para mitigar riesgos en los centros de cableado y datacenter. Estos controles incluirán, entre otros, sistemas de detección y extinción de incendios, mecanismos de control de inundaciones, alarmas de seguridad, y demás dispositivos o procedimientos que contribuyan a la protección de la infraestructura tecnológica crítica.
e) Los centros de cableado, datacenter y cualquier área destinada al procesamiento de información sensible deberán permanecer bajo llave en todo momento.
f) No está permitido tomar fotos o realizar grabaciones de las áreas seguras sin la previa autorización del responsable de dicha área.
g) No está permitido consumir alimentos ni bebidas, ingresar elementos inflamables en área seguras.
h) Toda persona ajena a la entidad que ingrese al área segura debe estar acompañada por un servidor público del Icetex durante el tiempo que dure su visita.

6.35. Escritorio y Pantalla Limpia

A continuación, se definen medidas preventivas para reducir los riesgos de acceso no autorizado a la información:

a) Cada vez que los colaboradores se retiren del lugar de trabajo deben bloquear los equipos de cómputo. La sesión de usuario se bloqueará automáticamente a los 5 minutos de inactividad.
b) No está permitido el consumo de alimentos y bebidas en los puestos de trabajo, ya que podrán verse afectado los activos de información (computadores, documentos, token, entre otros).
c) Es recomendable, que los equipos de cómputo sean apagados al final de la jornada.
d) Los puestos de trabajo deben permanecer limpios y ordenados y no debe existir información de tipo sensible (Clasificada o Reservada) sobre los puestos de trabajo, a menos que la misma se esté utilizando. Una vez el usuario se ausente de su puesto de trabajo o no vaya a utilizar más la información, deberá almacenarla de manera segura para evitar robo o pérdida de esta.
e) Los computadores (portátiles) que son propiedad del Icetex deben asegurarse con una guaya o deben almacenarse dentro de los cajones del escritorio.

6.36. Ubicación y Protección de Equipos

El Grupo de Recursos Físicos y VOT establecerán controles para la protección y ubicación de los equipos que son propiedad del Instituto:

a) Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas, peligros del entorno y los posibles accesos no autorizados, adoptando controles contra robo, incendio, humo, agua, polvo, vibración e interferencia en el suministro eléctrico o de comunicaciones, entre otros.
b) Todo equipo que sea propiedad del Icetex y que deba ser retirado de las instalaciones deberá contar con la debida autorización previa, conforme a los procedimientos establecidos por el instituto.
c) Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro (Electricidad, telecomunicaciones, ventilación, aire acondicionado, etc.), cumpliendo con las especificaciones de los fabricantes de equipos y los requisitos para su adecuado funcionamiento.
d) Los equipos de cómputo deben estar conectados a la corriente regulada del Instituto.
e) Se debe contar con sistemas de borrado seguro, cifrado de discos y un protocolo de destrucción de medios de almacenamiento de información “Pública clasificada” y “Pública reservada” en equipos destinados para reutilización o equipos para dar de baja.

6.37. Seguridad de los Activos Fuera de las Instalaciones del Icetex

El Grupo de Recursos Físicos y la VOT definirá y establecerá los controles necesarios para la asignación, uso, seguimiento y devolución de los activos institucionales entregados a los colaboradores que desempeñan sus funciones bajo la modalidad de teletrabajo, garantizando su adecuada custodia, trazabilidad y cumplimiento de las políticas de seguridad de la información.

6.38. Medios de Almacenamiento

a) Los colaboradores que hagan uso del token para el desempeño de sus funciones u obligaciones velarán por la custodia y buen manejo de estos.
b) Los colaboradores deben asegurar que los medios removibles dónde se almacena información institucional, son tratados de manera segura, evitando su daño o deterioro, manteniéndolos alejados del polvo, humedad o cualquier contacto con químicos corrosivos.
c) El colaborador a cargo del dispositivo (medio removible) institucional debe realizar periódicamente copias de respaldo de la información. Antes de eliminar información o destruir medios de almacenamiento de información se debe realizar la respectiva copia de respaldo.
d) En caso de ser estrictamente necesario almacenar información catalogada como “Pública Clasificada” o “Pública Reservada” en medios removibles, el dispositivo o la información deben estar cifrados.
e) Los medios de almacenamiento se deben proteger contra accesos no autorizados, uso indebido o corrupción, usando un transporte o servicios de mensajería confiables, utilizando cuando se requiera, embalaje para proteger el contenido contra cualquier daño físico o ambiental que se pudiera presentar durante el tránsito.

6.39. Servicios Públicos de Apoyo

El Grupo de Recursos Físicos y la VOT se asegurarán de suministrar plantas eléctricas, UPS, aire acondicionado y canal redundante de datos. asi mismo garantizar su mantenimiento preventivo y correctivo.

6.40. Seguridad del Cableado

El Grupo de Recursos Físicos y la VOT se asegurarán de suministrar el cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información el cual debe estar protegido durante todo su recorrido contra interceptación, interferencia o daño.

6.41. Mantenimiento de Equipos

La VOT dispondrá de un plan de mantenimiento para fortalecer la infraestructura tecnológica del Instituto y asegurar su ejecución.

6.42. Disposición o Reutilización Segura de Equipos

a) La VOT y el Grupo de Recursos Físicos, asegurará que los medios de almacenamiento (dispositivos tecnológicos y/o equipos de cómputo, portátiles, servidores) cuando cambien de propósito, sean devueltos por garantía, o terminen la vida útil, la información institucional que haya sido almacenada y procesada en estos sea borrada, eliminada y destruida de forma segura.
b) La disposición y reutilización de equipos se realizará de acuerdo con lo establecido en el Procedimiento Manejo de residuos ordinarios, tóneres, reciclables y tecnológicos - A1-4-10.

6.43. Dispositivos de Punto Final de Usuarios

Es responsabilidad de la VOT garantizar la implementación de los controles tecnológicos necesarios para asegurar la integridad, confidencialidad y disponibilidad de la información de los dispositivos de punto final.

6.44. Derechos de Acceso Privilegiado

La VOT gestionará los accesos de usuarios privilegiados, considerando:

a) Identificar a los usuarios que necesitan derechos de acceso con privilegios para cada sistema (eje: sistemas operativos, sistemas de gestión de bases de datos, entre otros).
b) Gestionar los derechos de acceso privilegiado de acuerdo con lo establecido en el Procedimiento gestión de accesos y retiro de servicios- A7 -1-05.
c) Definir y establecer los requisitos para la expiración de los derechos de acceso privilegiado.
d) Los usuarios con derechos de acceso privilegiado tendrán habilitado el log de acceso y transacciones en el servicio tecnológico al que tenga acceso.

6.45. Restricción de Acceso a la Información

a) La VOT gestionará las solicitudes de acuerdo con lo establecido en el Procedimiento gestión de accesos y retiro de servicios- A7 -1-05.
b) La VOT asignará a una cuenta de usuario (nombrada) permisos o privilegios de acuerdo con lo solicitado por el jefe inmediato o supervisor de contrato.
c) La VOT realizará revisiones periódicas de acuerdo con los criterios definidos para los diferentes sistemas de información y servicios tecnológicos del Instituto con el fin de garantizar que se desactiven los usuarios que no tengan vinculación laboral o contractual vigente.
d) El acceso a la Información, sistemas de información y/o aplicaciones de la entidad por parte de los servidor público, contratistas y terceros debe darse bajo el principio del mínimo privilegio; es decir que cada usuario solo debe tener acceso a lo que necesita conocer de acuerdo con sus actividades y rol que desempeña dentro del Instituto.

6.46. Acceso a Código Fuente

La VOT establecerá los lineamientos para controlar el acceso a los códigos fuentes de los programas, con el fin de evitar la introducción de funciones no autorizadas, cambios intencionados o malintencionados y mantener la confidencialidad de la propiedad intelectual.

6.47. Autenticación Segura

La VOT definirá e implementará los controles necesarios para que los usuarios o entidades se autentiquen de forma segura cuando se conceda el acceso a sistemas, aplicaciones, servicios e inicio de sesión, entre otras. Para ello dispondrá de controles como usuario y contraseña, doble factor de autenticación, entre otros.

6.48. Gestión de la Capacidad de TI

a) La VOT realizará seguimiento al uso de los recursos tecnológicos, con el fin de ajustar y proyectar los requisitos de capacidad futura de los servicios e infraestructura de tecnología del Icetex.
b) El líder de infraestructura tecnológica informará al Director de Tecnología de la VOT los recursos de infraestructura tecnológica (obsolescencia, capacidad de usuario, almacenamiento, bases de datos y licenciamiento), que han llegado a su límite (umbral), con el fin de incluirlos en el Plan Anual de Adquisiciones, el cual se ejecutará en la próxima vigencia.

6.49. Protección Contra Malware

La VOT implementará controles para asegurar que la información y otros activos de información estén protegidos contra malware, teniendo en cuenta:

a) Proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad digital contenida y administrada en la plataforma tecnológica del Icetex y los servicios que se ejecutan en la misma.
b) Asegurar que el software de antimalware y antispam cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.
c) Garantizar que la información almacenada en la plataforma tecnológica sea verificada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.
d) Asegurar que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.
e) Garantizar que el software de antimalware y antispam, posea las últimas actualizaciones y parches de seguridad para evitar que sean explotadas algunas vulnerabilidades.

Colaboradores:

f) No cambiar o eliminar la configuración del software de antimalware y antispam definida por la VOT.
g) Asegurar que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.
h) Ante sospechas o detección de alguna infección por software malicioso deben notificar a la mesa de ayuda, para que la VOT tome las medidas de control correspondientes.
i) Evitar abrir correos de fuentes desconocidas, y publicidad engañosa.

j) En caso de requerirse, llevar el equipo de cómputo y/o portátiles asignados por el Icetex a la VOT para realizar actualizaciones de seguridad, ajustes de configuración o despliegues de nuevas soluciones de protección antimalware.

6.50. Gestión de Vulnerabilidades Técnicas

a) La VOT realizará la gestión de vulnerabilidades técnicas de acuerdo con lo establecido con el procedimiento Pruebas de vulnerabilidad A7-1-11.
b) De acuerdo con el procedimiento Pruebas de vulnerabilidad A7-1-11 la Dirección de Tecnología realizará análisis de vulnerabilidades técnicas con de fin de identificar algunas nuevas y las reportará a los administradores de la plataforma tecnológica y a los desarrolladores de los sistemas de información, con el propósito de que se implementen las acciones correctivas y preventivas necesarias para su mitigación.
c) La VOT realizará ejercicios de Ethical Hacking sobre las plataformas tecnológicas deli ICETEX como mínimo anualmente

6.51. Gestión de la Configuración

La Dirección de Tecnología a través del controlador de dominio del directorio activo gestionará las configuraciones a los equipos que son propiedad del Icetex y lo establecido en el procedimiento activos y configuración de TI A7-1-09.

6.52. Eliminación de Información

a) El proceso de Gestión Documental establecerá los mecanismos técnicos, administrativos y procedimentales necesarios para garantizar la eliminación segura de la información, una vez que esta haya cumplido con los tiempos de retención y deje de ser requerida para fines legales, operativos o contractuales.
b) El proceso de Gestión Documental conservará el registro de los resultados de la eliminación segura de la información.
c) La Dirección de Tecnología depurará información que ya no se necesite en sistemas de información o dispositivos (eje: cuentas de usuario o huellas de colaboradores que ya no labora en la entidad, etc.).

6.53. Enmascaramiento de datos

La Dirección de Tecnología y Gestión Documental establecerán e implementarán los lineamientos para limitar la exposición de información sensible del Icetex, teniendo en cuenta:

a) Establecer técnicas que permitan ocultar información sensible.
b) Identificar y establecer a que información se le debe aplicar estas técnicas.
c) Establecer controles para restringir el acceso a la información sensible.
d) Cumplir con la normatividad legal vigente que aplique al Instituto.

6.54. Prevención de Fuga de Datos

La Dirección de Tecnología establecerá medidas de prevención contra la fuga de datos, teniendo en cuenta:

a) Identificar, clasificar y proteger la información contra fugas (eje: información personal, misional, código fuente, entre otras)
b) Para los equipos propios del Icetex, establecer mecanismos que permitan controlar y supervisar la fuga de los datos (eje: información que se envía por correo, uso de USB, transferencia de archivos, dispositivos móviles, dispositivos de almacenamiento, portátiles, DLP, entre otros).
c) Para los equipos que no son propiedad del Icetex, establecer mecanismos que permitan controlar y supervisar la fuga de los datos (eje: información que se envía por correo, transferencia de archivos, DLP, entre otros).

6.55. Copias de Seguridad de la Informaciòn - Backup

La Dirección de Tecnología proporciona medios de almacenamiento (local o nube) seguros, para facilitar el acceso, uso y respaldo de la información, con el fin de mitigar riesgos de pérdida y acceso no autorizado a la misma, bajo las siguientes premisas:

a) La gestión de backup se realiza de acuerdo con lo establecido en el Procedimiento Gestión de Backup A7-1-10.
a) La Dirección de Tecnología realiza backup a la información que se aloja en el repositorio oficial de “File Server”, los usuarios deben solicitar el ingreso a este repositorio a través de la mesa de servicio, previa autorización del jefe inmediato.

b) La Dirección de Tecnología no realiza backup a la información que los usuarios almacenen en los discos duros de los equipos que son propiedad del Icetex.
c) Es responsabilidad de los colaboradores (servidor público y contratistas) almacenar la información en el “File Server” o en repositorios en la nube autorizados por la entidad.
d) Está prohibido alojar en el “File Server”, información personal como videos, archivos MP3, fotos y demás información que no haga parte de la ejecución de las funciones u obligaciones contractuales.
e) Ningún usuario debe realizar copias de información “Reservada o Clasificada” en medios extraíbles personales, dado que la información es propiedad del Icetex.
f) La Dirección de Tecnología generará una copia de respaldo del correo electrónico institucional de los servidor público y contratistas retirados, y la conserva por un período máximo de seis (6) meses contados a partir de la fecha de retiro.
g) La Dirección de Tecnología monitoreará el uso de las herramientas de almacenamiento institucional (OneDrive y SharePoint), identificando cuentas o espacios que no registren actividad de ingreso durante un período superior a treinta (30) días, con el fin de asegurar el adecuado uso de los recursos asignados, detectar posibles abandonos o desuso y mitigar riesgos asociados a la seguridad de la información.

6.56. Redundancia de las Instalaciones

La Dirección de Tecnología dispondrá de instalaciones de procesamiento de información requeridas en el plan de recuperación de desastres tecnológicos, contemplando lo siguiente:

a) Analizar y establecer los requerimientos de redundancia para los sistemas de información que se usan en los procesos críticos y la plataforma tecnológica.
b) Realizar pruebas sobre las soluciones de redundancia, para asegurar el cumplimiento de los requerimientos de disponibilidad.
c) Seleccionar soluciones de redundancia tecnológica sobre los sistemas de información de acuerdo con las necesidades del negocio.

6.57. Registro y Monitoreo de Actividades

La Dirección de Tecnología realizará monitoreo al uso de la plataforma tecnológica y los sistemas de información del Instituto, teniendo en cuenta:

a) Habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos a auditar y lo que establece la Guia de Log de Auditoria G212.
b) Velar por la integridad y disponibilidad de los registros de auditoría generados en la plataforma tecnológica y los sistemas de información del ICETEX. Estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.
c) Definir un usuario con privilegios únicamente para administración y control de los logs, adicional dicho usuario debe realizar el correspondiente seguimiento y revisiones periódicas.
d) Establecer los registros de auditoría en los recursos tecnológicos y los sistemas de información considerando los estándares de desarrollo seguro para registros de auditoría.

Desarrollos Internos y Externos:

e) Implementar en los desarrollos de software, los controles necesarios para generar y garantizar la integridad de los registros (logs) de auditoría de las actividades realizadas por los usuarios finales y administradores en los sistemas de información desarrollados.
f) Implementar en los desarrollos de software mecanismos para registrar en los logs de auditoría eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros.

Administradores de Sistemas de Información e Infraestructura Tecnológica

g) Los administradores de aplicaciones deben habilitar y generar logs de auditoría en las aplicaciones en la periodicidad establecida.
h) Los administradores de sistemas operativos deben habilitar y generar en la periodicidad establecida los logs de auditoría del sistema operativo.
i) Los administradores de bases de datos deben habilitar y generar logs en la periodicidad establecida sobre las bases de datos y tablas para los campos que manejen información catalogada como

"Clasificada" y "Reservada".

j) Los administradores de seguridad perimetral deben generar y revisar en la periodicidad establecida los reportes generados por la plataforma e identificar intentos de accesos no autorizados con su correspondiente cantidad de eventos, origen y tipo de evento (firewall, ips, waf, rdp, vpn, acceso a plataformas de gestión, otros componentes tecnológicos para la seguridad y telecomunicaciones).
k) Los administradores de consola de antivirus deben revisar los reportes generados por la plataforma e identificar anomalías en cada uno de los servidores y estaciones de trabajo generando un consolidado de amenazas identificadas.
l) El Coordinador de Infraestructura es responsable de recopilar y analizar los reportes generados por los administradores de bases de datos, aplicaciones, sistema operativo, consola de antivirus y correo electrónico, con el fin de presentar al Subcomité de Logs las propuestas de acción y los ajustes necesarios para atender las alarmas o incongruencias identificadas, de acuerdo a lo establecido en el procedimiento Revisión de Logs A7-1-08.
m) Los administradores de sistemas de información e infraestructura tecnológica deben configurar el envío de logs de auditoría generados al correlacionador de eventos para su revisión.

6.58. Actividades de Seguimiento

La Dirección de Tecnología implementará controles para detectar comportamientos anómalos y posibles incidentes de seguridad de la información, teniendo en cuenta:

a) Establecer mecanismos que realicen monitoreo al acceso a servidores, equipos de red, aplicaciones misionales, tráfico de red, sistemas y aplicaciones salientes y entrantes, acceso no autorizado, análisis no autorizado de aplicaciones, sistemas y redes de la entidad, intentos correctos e incorrectos de acceder a los recursos protegidos (servidores DNS, portales web recursos compartidos de archivos) entre otras.
b) Definir una línea base de comportamiento normal para vigilar sobre esa línea las actividades que realizan los usuarios con el fin de detectar anomalías frente la utilización de los sistemas en periodos normales y fuera de lo normal, hora habitual de acceso, ubicación del acceso, frecuencia de acceso, a que páginas están ingresando, que información están descargando y/o almacenando en los equipos, entre otras.

6.59. Sincronización de Relojes

La Dirección de Tecnología garantizará la sincronización de los relojes de los servidores, sistemas de información, plataformas de telefonía, sistemas de videovigilancia (CCTV), estaciones de trabajo y demás ítems de configuración (CI), con una única fuente oficial de referencia de tiempo. Con el propósito de asegurar la coherencia y exactitud de los registros de auditoría, facilitando la trazabilidad, el análisis forense y el cumplimiento de los requisitos normativos aplicables.

6.60. Uso de Programas de Utilidad privilegiados

La Dirección de Tecnología garantizará que el uso de programas de utilidad no perjudique los controles del sistema y de las aplicaciones, teniendo en cuenta:

a) Establecer controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información, no tengan instalados en sus equipos de cómputo utilitarios que permitan escalar privilegios o evadir controles de seguridad informáticos.
b) Monitorear a los administradores de los recursos tecnológicos y servicios de red, para que no hagan uso de utilitarios que permitan acceso a los sistemas operativos, firmware o conexión a las bases de datos para anular la seguridad de los sistemas de información alojados sobre la plataforma tecnológica.
c) Generar y actualizar programas utilitarios privilegiados de la plataforma tecnológica, los servicios de red y sistemas de información.
d) Retirar o deshabilitar los programas utilitarios privilegiados no autorizados de la plataforma tecnológica, los servicios de red y sistemas de información

6.61. Instalación de Software en Sistemas Operativos

La Dirección de Tecnología aplicará controles para administrar de forma segura la instalación de software en sistemas operativos con base en la Guía Instalación/desinstalación de software G172 y teniendo en cuenta:

a) Controlar y documentar los cambios en las librerías de programas propios del Icetex, software operacional y aplicaciones.
b) Mantener un registro de auditoría de todas las actualizaciones al sistema operativo.
c) La instalación y actualización de software será realizada exclusivamente por personal autorizado, conforme a los perfiles de acceso definidos por la Dirección de Tecnología

6.62. Seguridad de Redes

La Dirección de Tecnología debe asegurar la protección de la información transmitida en las redes de comunicación, los servicios relacionados y las instalaciones de procesamiento de información contra acceso no autorizado, aplicando los controles necesarios que permitan tener un adecuado nivel de seguridad en la red y de la información, teniendo en cuenta:

a) Contar con segmentación a nivel de redes físicos y lógicos para el despliegue de políticas y acceso a los recursos de red requeridos para el desarrollo de las actividades del Icetex.
b) Implementar mecanismos de control que permitan fortalecer la seguridad perimetral, minimizando la posibilidad de materialización de riesgos o reduciendo su impacto en caso de materialización.
c) Realizar monitoreo a los componentes de la infraestructura de red, de tal forma que se identifiquen de manera oportuna vulnerabilidades y fallas que puedan afectar la seguridad de la información.
d) Configurar y administrar el filtro de contenido que bloquee el acceso a sitios no productivos o clasificados dentro de listas negras por manejar temas tales como: pornografía, juegos, violencia, terrorismo, y demás páginas que no sean de uso laboral.
e) Realizar monitoreo a los servicios, protocolos y puertos permitidos en la red de datos de la entidad, inhabilitando o eliminando aquellos no identificados ni autorizados.
f) Establecer para los usuarios que utilizan las redes inalámbricas las mismas condiciones de seguridad de las redes cableadas en lo que respecta identificación, autenticación, control de contenido de internet y cifrado entre otros.
g) Proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de internet, bajo las restricciones de los perfiles de acceso establecidos; implementar mecanismos que permitan la continuidad o restablecimiento del servicio de internet en caso de contingencia.
h) Limitar o bloquear el acceso a sitios e impedir que se descarguen ciertos tipos de archivos que pueden afectar el servicio de internet y la información del Icetex.
i) Todas las conexiones para navegar en Internet desde la red corporativa se deben canalizar y monitorear a través una herramienta dispuesta por el Icetex.

6.63. Filtrado Web

La Dirección de Tecnología establecerá controles para proteger los sistemas de información contra malware y accesos no autorizados, teniendo en cuenta:

a) Identificar los sitios web a los que los usuarios deberían tener o no acceso.
b) Definir e implementar los controles para reducir el riesgo de que los colaboradores accedan a sitios web que contienen información ilegal, virus o material de phishing.
c) Establecer perfiles de navegación de acuerdo con el rol, funciones del usuario o la dependencia, con el fin de asignar permisos para el ingreso a páginas.

6.64. Uso de la Criptografía

La Dirección de Tecnología definirá y establecerá los lineamientos y controles para el uso adecuado y efectivo del cifrado para proteger la confidencialidad, autenticidad e integridad de la información del instituto, teniendo en cuenta:

- Definir e implementar los mecanismos de cifrado en los sistemas de información que requieran para el almacenamiento y transmisión de información pública clasificada o pública reservada.
- Definir e implementar los mecanismos de cifrado para la información institucional catalogada como pública clasificada o pública reservada que requieran realizar almacenamiento y/o transmisión.
- Disponer de los mecanismos de cifrado para el aseguramiento de las conexiones de acceso remoto a la red del Icetex o recursos de la entidad.
- Todos los sistemas de información deben contar con certificados digitales vigentes que garanticen el cifrado de las comunicaciones entre entidades externas.
- Establecer los mecanismos de control y seguimiento para la creación, activación, distribución, recuperación y revocación de las llaves criptográficas.
- Deshabilitar las llaves criptográficas cuando estas se encuentren en riesgo de divulgación o cuando los colaboradores autorizados culminen la relación laboral o contractual con el Icetex.

6.65. Ciclo de Vida de Desarrollo Seguro

La Dirección de Tecnología definirá la metodología para planificar y ejecutar las actividades relacionadas con el ciclo de vida de desarrollo seguro, teniendo en cuenta, como mínimo lo siguiente:

a) Todo sistema de información adquirido o desarrollado debe utilizar herramientas de desarrollo licenciadas o libres reconocidas en el mercado.
b) Los desarrollos deben aplicar lo descrito en el Procedimiento gestión de requerimientos tecnológicos A7-1-04.
c) La plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información deben estar actualizados con las versiones LST (Long Support Term), las cuales deben estar en la última versión.
d) Todo desarrollo inhouse debe contar con mecanismos de seguridad (autenticación, autorización y auditoría) en todas las fases del desarrollo de software que utilice el Icetex.
e) Los desarrollos nuevos o sistemas de información adquiridos deben contar con pistas de auditoría que permitan como mínimo revisar los accesos (Login) exitosos y fallidos, así como las creaciones y modificaciones de usuarios y permisos.
f) El uso de información catalogada como “Pública Clasificada” o “Pública Reservada” está restringido para propósito de desarrollo y pruebas, por lo que se deben utilizar métodos o estrategias para la anonimización, enmascaramiento u ofuscación de la información.
g) Definir y mantener actualizado los roles, perfiles y usuarios de los sistemas de información.
h) Cada sistema de información deberá contar con los manuales de uso, técnicos y administrativos disponibles de acuerdo con los niveles de protección de la información dados por el Instituto.
i) Para desarrollos inhouse, el código fuente deberá almacenarse exclusivamente en el repositorio oficial designado por la Dirección de Tecnología, conforme a las directrices institucionales de seguridad, trazabilidad y control de versiones.
j) Asegurar que los sistemas de información adquiridos o desarrollados por contratistas cuenten con un acuerdo de licenciamiento, el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
k) Todos los desarrolladores internos o externos, contratados por el Icetex, deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de estos, iniciando desde la fase de diseño hasta la puesta en producción.

6.66. Requisitos de Seguridad de las Aplicaciones

La Dirección de Tecnología definirá los lineamientos para la transferencia e intercambio de información, teniendo en cuenta, como mínimo:

a) Establecer controles que garanticen la integridad, confidencialidad y protección contra accesos no autorizados durante la transferencia de información.
b) Contar con mecanismos de autenticación robusta que incluyan información secreta del usuario.
c) Asegurar la confidencialidad de los datos intercambiados entre el Instituto y las partes involucradas.
d) Implementar cifrado en las comunicaciones, conforme a la criticidad de la información y el canal utilizado.
e) Verificar que los protocolos de comunicación utilizados estén asegurados y actualizados conforme a estándares vigentes.
f) Garantizar que la información relacionada con las transacciones no sea accesible públicamente ni expuesta a riesgos de divulgación no autorizada.

6.67. Arquitectura de Sistemas Seguros y Principios de Ingeniería

La Dirección de Tecnología definirá y establecerá los principios de ingeniería para asegurar que los sistemas de información se diseñan, implementan y operan de forma segura dentro del ciclo de vida del desarrollo, teniendo en cuenta como mínimo:

a) El desarrollo interno o externo de los sistemas de información deben garantizar la seguridad de la información con base en la confidencialidad, disponibilidad e integridad durante todo el ciclo de vida del desarrollo, teniendo en cuenta además el nivel de soporte requerido por el instituto para el caso de los desarrollos externos.
b) Generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas, entre otros.
c) En conjunto con los responsables y propietarios de los sistemas de información se deben realizar las pruebas necesarias para asegurar que los sistemas de información desarrollados cumplan con los requerimientos de seguridad establecidos antes del paso a producción, garantizando la seguridad de la información para este fin.
d) Los sistemas de información deben limitarse a recibir y validar los datos de entrada, gestionar los eventos y proporcionar los datos de salida adecuados para los usuarios, sin exponer ningún tipo de

información de la aplicación que pongan en riesgo la confidencialidad, integridad y/o disponibilidad de la información.

e) Implementar un mecanismo adecuado de gestión de errores, que permita un modo de recuperación seguro y que regrese mensajes adecuados, con mínima información que no afecte y/o comprometa la seguridad de la aplicación y/o sistema de información.
f) No se debe alojar credenciales de autenticación (por ejemplo: usuario y contraseña) en el código de la aplicación.
g) Toda aplicación nueva desarrollada deberá implementar un módulo de administración de usuarios, roles y privilegios.
h) Toda aplicación desarrollada deberá contar con un módulo de seguridad RECAPTCHA en el formulario de autenticación de usuarios, para evitar que un robot ejecute peticiones de manera automática; y/o ataques de fuerza bruta.
i) Utilizar mecanismos de cifrado para la transferencia de datos de forma segura como, por ejemplo, protocolos HTTPS, SFTP, FTPS, SSL/TLS, entre otros, con el fin que no se transmita información en texto plano, y que a su vez utilicen algoritmos de cifrado fuertes o reconocidos como seguros.
j) Establecer controles de seguridad de la información para el manejo de sesiones y cookies web.
k) Para servicios web ejemplo: webservices, se implementará mecanismos de autenticación y autorización mediante tokens.
l) No se debe exponer información de configuración y/o parametrización, que contenga datos personales o información pública clasificada y pública reservada en la documentación del código fuente.
m) Llevar un control de versiones del código fuente y documentación de los sistemas de información, con el objeto de verificar el funcionamiento del software y el respectivo control de su ciclo de vida, en un repositorio especializado para este tipo de información.
n) Deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.
o) Cerrar las sesiones activas de las aplicaciones luego que pasen como máximo (10) minutos sin actividad, terminándolas una vez se cumpla este tiempo.
p) Asegurar que no se permitan sesiones simultáneas a los sistemas de información con el mismo usuario.
q) Proteger los códigos ejecutables, código de desarrollo, compiladores del software operacional y aplicaciones propias del Icetex.
r) Implementar mecanismos de credenciales de acceso de usuario en todos los niveles de los sistemas de información, por ejemplo, Front-End y Back-End.
s) Asegurar el manejo de operaciones sensibles o críticas en los aplicativos desarrollados permitiendo el uso de dispositivos alternos como parámetros adicionales de verificación.
t) Asegurar que los aplicativos proporcionen y almacenen la mínima información de acciones de las sesiones que interactúan con el sistema.
u) No incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales deben estar cifrados.

6.68. Codificación Segura

La Dirección de Tecnología definirá, documentará y aplicará la metodología para la codificación segura tanto para los desarrollos inhouse como para los desarrollos subcontratados con el fin de mitigar posibles vulnerabilidades.

6.69. Pruebas de Seguridad en el Desarrollo y Aceptación

La Dirección de Tecnología ejecutara las pruebas de seguridad y pruebas de aceptación a los cambios y nuevos sistemas de información de acuerdo con lo establecido en el Instructivo plan de pruebas de aceptación I80.

6.70. Desarrollo Tercerizado

La Dirección de Tecnología definirá las medidas de seguridad de la información para el desarrollo de sistemas de información a través de terceros, teniendo en cuenta como mínimo:

a) Cuando se adquieran soluciones de software previamente desarrolladas, la Dirección de Tecnología deberá establecer, de manera previa a la adquisición, los procesos de administración de parches y actualizaciones de seguridad con el proveedor. Estos procesos deberán garantizar que la aplicación no presente vulnerabilidades conocidas y que se mantenga actualizada frente a nuevas amenazas.

b) Previo a la entrega de cualquier tipo de información de propiedad del Icetex al proveedor, se deberán establecer acuerdos de confidencialidad que respalden su uso adecuado, seguro y conforme a la normativa vigente.
c) Los sistemas de información adquiridos o desarrollados por terceros deben contemplar la definición y entrega de acuerdos de licenciamiento, propiedad de códigos, los cuales deben especificar las condiciones de uso del software y los derechos de propiedad intelectual.
d) Establecer en la documentación contractual y anexos técnicos los requisitos relacionados a prácticas seguras de diseño, codificación y pruebas.
e) Establecer acuerdos de niveles de servicio en cuanto a la calidad, oportunidad y seguridad de los entregables de los sistemas de información.
f) Solicitar al proveedor la generación y entrega de un informe de análisis y mitigación de vulnerabilidades realizado al sistema de información.
g) Documentar las características del ambiente de desarrollo usado para replicar ambientes similares.
h) Implementar o utilizar protocolos de comunicación cifrados para intercambiar datos o funcionalidad con los sistemas de información de la entidad.
i) Requerir en lo posible la integración del acceso a los sistemas de información a través de usuarios de dominio.
j) Para el caso de adquisición de software como servicios (SaaS) se deben contemplar requerimientos como: periodicidad y retención de las copias de respaldo de la información del Icetex, requerimientos de continuidad, redundancias, requisitos de seguridad a nivel de infraestructura, roles y privilegios, integración con el directorio activo, privacidad de la información, entre otros.
k) Para el caso de la información almacenada en SaaS cuando finalice la relación contractual entre el Icetex y el proveedor, se debe solicitar el borrado seguro de dicha información previa entrega de una copia de respaldo completa de la información con corte a la finalización del contrato.
l) En caso de que se realicen cambios a un sistema de información adquirido, se debe conservar la versión original para ser restaurado en caso de requerirse.
m) Planear y ejecutar pruebas técnicas y funcionales que les permitan contar con la aceptación de los desarrollos y funcionalidades solicitados.

6.71. Separación de Entornos de Desarrollo

La Dirección de Tecnología realizara la separación de los ambientes de desarrollo, pruebas y producción teniendo en cuenta:

a) Realizar la separación física y lógica de los ambientes de desarrollo, pruebas, preproducción y producción, con el fin de reducir los riesgos de acceso o cambios no autorizados que puedan afectar la confidencialidad, integridad y disponibilidad de los entornos productivos.
b) Garantizar que los desarrolladores realicen su trabajo exclusivamente en el ambiente de desarrollo y no en los ambientes de pruebas o producción.
c) Utilizar nombres de dominios diferentes para los ambientes de prueba, desarrollo y producción para evitar confusiones y diferenciar de manera clara cada ambiente.
d) En los ambientes de prueba utilizar datos que no sean sensibles para el Icetex, exceptuando aquellos casos en los que el usuario funcional solicita la restauración de datos de producción para verificar la correcta funcionalidad.

6.72. Gestión de Cambios

La Dirección de Tecnología debe establecer los lineamientos para controlar y reducir al mínimo, el impacto sobre los cambios normales y de emergencia que se generen sobre los servicios, infraestructura y aplicativos de TI que administra, teniendo en cuenta como mínimo:

a) Documentar, formalizar y divulgar los procedimientos operativos que garanticen la disponibilidad, integridad, privacidad y confidencialidad de la información.
b) Gestionar los cambios normales, estándares y de emergencia a nivel de infraestructura, aplicativos, sistemas de información, bases de datos, servicios tecnológicos y en general a los activos de información tecnológicos y los recursos informáticos, como lo establece el procedimiento A7-1-12 Procedimiento control de cambios y despliegue.
c) Analizar los riesgos, impactos y requisitos de seguridad de la información de los cambios en los componentes tecnológicos, con el fin de no afectar la correcta operación de estos ni de otros servicios.
d) Cumplir con la gestión de cambios de TI para los sistemas de información, estableciendo como mínimo, justificación, ventana de mantenimiento, indisponibilidad de los servicios, rollback, puntos de retorno, riesgos y responsables.

6.73. Información de las Pruebas

La Dirección de Tecnología establecerá los lineamientos para proteger los datos de prueba, teniendo en cuenta:

a) Definir los lineamientos para la gestión de los datos de pruebas a nivel institucional
b) Garantizar que la información a ser entregada a los desarrolladores para sus pruebas se enmascare y no revele información calificada como clasificada y reservada de los ambientes de producción.
c) Realizar la adecuada disposición final la información de los ambientes de pruebas, una vez éstas han concluido las mismas.

6.74. Protección de los Sistemas de Información

La Dirección de Tecnología garantizara la protección de los sistemas de información durante las pruebas de auditoría, teniendo en cuenta como mínimo:

a) Planificar actividades que involucren auditorías a los sistemas críticos en producción, limitando el acceso al sistema de información y a los datos de solo de lectura (en caso de acceso diferente al de solo lectura se deberá acordar previamente).
b) Definir y gestionar los planes de mejoramiento que se generen de los resultados de las auditorías a los sistemas de información del Icetex.

6.75. Uso de Inteligencia Artificial

La Dirección de Tecnología - VOT establecerá los lineamientos y controles de seguridad y privacidad de la información para el uso de las herramientas de inteligencia artificial, teniendo en cuenta como mínimo:

a) Implementar controles tecnológicos preventivos en la protección de datos personales en proyectos de herramientas digitales de inteligencia artificial.
b) Asegurar que el acceso a los sistemas de IA y a los datos debe estar disponible a usuarios autorizados, utilizando mecanismos de autenticación robustos, garantizando que toda información del Icetex sea gestionada de manera segura conforme a las políticas de seguridad digital y gestión de riesgo institucional.
c) Informar a los colaboradores del Icetex cuales herramientas de inteligencia artificial están autorizadas para su uso.
d) Implementar controles para evitar la descarga y el uso de herramientas digitales de inteligencia artificial que no estén autorizadas.
e) Implementar controles que permitan el bloqueo de complementos para el uso de herramientas de inteligencia artificial que no estén autorizadas.
f) Garantizar que el software operativo, complementos o funcionalidades especialmente aquellas que incluyan servicios de inteligencia artificial se utilicen de conformidad con la legislación sobre privacidad y protección de datos los cuales deben estar alienados a todo servicio que se diseñe, implemente y opere conforme a las políticas de seguridad digital y gestión de riesgo institucional.
g) Asegurar que el desarrollo e implementación de modelos de inteligencia artificial cumplan con los principios definidos en este documento, los cuales deben estar alienados a que todo servicio que se diseñe, implemente y opere este conforme a las políticas de seguridad digital y gestión de riesgo institucional.
h) Garantizar que los sistemas de inteligencia artificial se desarrollen cumplan con la legislación sobre privacidad y protección de datos personales.
i) Liderar la definición de requerimientos de modelos de inteligencia artificial y demás herramientas tecnológicas emergentes, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones.
j) Proteger el código fuente del modelo de Inteligencia Artificial con el fin de evitar manipulaciones no deseadas lo que podría cambiar el comportamiento del modelo.
k) Documentar el modelo de Inteligencia Artificial, como mínimo en su análisis de riesgos, las entradas del modelo, los resultados propuestos del modelo, limitaciones del modelo, criterios de liberación del modelo.
l) Establecer y documentar y socializar los usos previstos del modelo de Inteligencia Artificial determinando los problemas a resolver, los requisitos de datos para su funcionamiento y los procedimientos para la recolección y tratamiento de datos personales.

Colaboradores:

m) Está prohibido utilizar o transferir información de la Entidad, por ejemplo, bases de datos, matrices, información general, entre otros, en herramientas digitales de inteligencia artificial, que no estén autorizadas o aprobadas por la Dirección de Tecnología.
n) Asegurar que las fuentes de datos o repositorios originales utilizados para el entrenamiento de modelos de inteligencia artificial sean confiables, verificables y pertinentes, mediante una evaluación previa de su idoneidad técnica, legal y ética.
o) No está permitido el uso de inteligencia artificial para los siguientes casos: Aspectos que vayan en contra o detrimento del código de ética y conducta del Icetex, Incumplimiento de la legislación colombiana, Situaciones que provoquen daños a terceros, Manipulación comportamental de los usuarios de los sistemas de IA, Monitoreo indiscriminado a terceros por parte de la IA sin supervisión humana, Generación de contenido o información engañosa.

Terceras partes:

p) Todo servicio que se diseñe, implemente y opere con tecnologías de inteligencia artificial y demás herramientas tecnologías emergentes para el procesamiento de datos, deben pasar por la aprobación de la Dirección de Tecnología y el correspondiente análisis de la Oficina de Riesgos, así como ser socializados en la mesa de cambios para su aprobación y puesta en producción.
q) Establecer controles robustos para el acceso a los servicios y cambios proporcionados por terceros que involucren el uso de herramientas de inteligencia artificial y analítica de datos para el procesamiento de estos, almacenamiento de datos de la entidad y el cifrado de los datos tanto en reposo como en tránsito.

6.76. Ciberseguridad

La Dirección de Tecnología - VOT, establecerá los controles para gestionar las etapas de prevención, protección, detección, respuesta, comunicación, recuperación y aprendizaje de ciberseguridad, teniendo en cuenta como minino:

a) Implementar, operar y mantener controles para mitigar los riesgos que pudieran afectar la seguridad digital.
b) Gestionar la ciberseguridad en los proyectos que impliquen la adopción de nuevas tecnologías.
c) Gestionar y documentar la seguridad en la plataforma tecnológica del Icetex.
d) Mantener dentro del plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques cibernéticos y realiza las respectivas pruebas a dicho plan.
e) Adoptar los mecanismos necesarios para recuperar los sistemas de información al estado en que se encontraban antes del ataque cibernético.
f) Mantener actualizadas y en operación las herramientas y/o servicios que permitan hacer correlación de eventos que puedan alertar sobre incidentes de seguridad.
g) Monitorear los canales de atención, volumen transaccional y número de clientes y diferentes fuentes de información tales como sitios web, blogs y redes sociales, con el propósito de identificar posibles ataques cibernéticos contra la Entidad.
h) Colaborar con las autoridades que hacen parte del modelo nacional de gestión de ciberseguridad en los proyectos que se adelanten con el propósito de fortalecer la gestión de la ciberseguridad en el sector financiero y a nivel nacional.
i) Gestionar las vulnerabilidades de aquellas plataformas que soporten los procesos críticos y que estén expuestos en el ciberespacio.
j) Monitorear continuamente la plataforma tecnológica con el propósito de identificar comportamientos inusuales que puedan evidenciar ciberataques contra la Entidad.
k) Aplicar el procedimiento de gestión de incidentes cuando se presenten incidentes de seguridad digital, identificando los dispositivos que pudieran haber resultado afectados.
l) Preservar cuando sea factible, las evidencias digitales para que las autoridades puedan realizar las investigaciones correspondientes.