MANUAL DE POLÍTICAS DE SEGURIDAD DIGITAL

INSTITUTO COLOMBIANO DE CRÉDITO EDUCATIVO Y ESTUDIOS TÉCNICOS EN EL EXTERIOR

Septiembre 2020

Contenido

INTRODUCCION

El Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior – ICETEX identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la Entidad, por esta razón establece un modelo que asegura que la información es protegida de una manera adecuada para su recolección, manejo, procesamiento, transporte y almacenamiento.

Este documento describe las políticas y normas de seguridad digital definidas por el ICETEX. Para la elaboración del mismo, se toman como base las leyes y demás regulaciones aplicables, las políticas incluidas en este manual son parte integral del sistema de gestión de seguridad digital del ICETEX y son la base para la implantación de los controles, procedimientos y estándares.

La seguridad digital es una prioridad para el ICETEX y por tanto el cumplimiento de estas políticas es responsabilidad de todos sus colaboradores.

A lo largo del documento al emplear el término seguridad digital se agrupan los conceptos de seguridad de la información, seguridad informática, ciberseguridad y la protección de los datos personales.

1. OBJETIVO

El objetivo de este documento es establecer las políticas y lineamientos en seguridad digital del ICETEX, con el fin de regular su gestión al interior de la Entidad.

2. ALCANCE

Las políticas de seguridad digital cubren todos los procedimientos que tiene la Entidad y se gestionan a nivel nacional en búsqueda de una adecuada protección y calidad de la información.

3. 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.

Capacity Planning: es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la Entidad para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento 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 la misma 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.

Ciberiesgo 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 politicas, 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.

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.

Guías de clasificación de la información: directrices para catalogar la información de la Entidad y hacer una distinción entre la información que es calificada como pública clasificada o pública reservada y de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información

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.

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.

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 Digital.

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.

Sistemas de control ambiental: son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características del mismo, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.

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.

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.

4. POLÍTICA GLOBAL DE SEGURIDAD DIGITAL

En ICETEX es vital brindar la confianza a nuestros clientes y partes interesadas, propendiendo porque la información administrada está debidamente protegida, porque con ella, iniciamos el camino que impulsa a los colombianos a alcanzar sus sueños de una mejor educación.

Los productos y servicios están asegurados con un modelo de seguridad digital, que gestiona los riesgos para garantizar la confidencialidad, integridad, disponibilidad y privacidad que contribuyen al desarrollo de la estrategia de negocio y el cumplimiento de metas.

Nuestro personal, procesos e infraestructura están dispuestos con la finalidad de cumplir con los requisitos legales y de seguridad digital. Estudiamos las necesidades de nuestros clientes, nos capacitamos, revisamos el entorno de amenazas digitales y tendencias tecnológicas para mejorar continuamente la seguridad digital.

6. COMPROMISO DE LA DIRECCION

La Junta Directiva de ICETEX aprueba esta Política de Seguridad Digital como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad digital de la Entidad.

La Junta Directiva y la Alta Dirección de la Entidad demuestran su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad Digital contenidas en este documento.
- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de este manual a todos los funcionarios de la Entidad.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad digital.
- La verificación del cumplimiento de las políticas aquí mencionadas.

7. SANCIONES POR LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DIGITAL

El incumplimiento de las políticas de seguridad digital se gestiona a través de procedimientos administrativos que pueden conducir a procesos disciplinarios o penales según aplique de acuerdo con la gravedad de la falta. ICETEX cuenta con canales de comunicación donde el personal puede reportar posibles incumplimientos que afecten la seguridad digital.

La utilización indebida de perfiles de usuarios para obtener beneficio propio o en favor de terceros será sancionado de acuerdo con los procedimientos administrativos definidos.

8. POLÍTICAS DE LA ORGANIZACIÓN DE LA SEGURIDAD DIGITAL

Cada rol y responsabilidad para la seguridad digital está claramente definido y se realiza con las políticas institucionales.
La orientación, definición y revisión de la administración del Sistema de Gestión Seguridad Digital es liderada por el Comité de Seguridad de la Información.
A cada una de funcionarios y contratistas se le ha asignado una responsabilidad con el Sistema de Gestión Seguridad Digital y las mismas están reflejadas en este documento.
La gestión de riesgos y la evaluación de riesgo residual es responsabilidad de los Líderes de Procesos con el apoyo de la Oficina de Riesgos.

8.1 POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DIGITAL

El ICETEX establece una estructura organizacional responsable de la seguridad digital, con roles y responsabilidades definidos, considerando actividades de gestión de riesgos, análisis de las tecnologías y del entorno, promueve la cultura de la seguridad e informa del desempeño del Sistema de Gestión de Seguridad Digital a la Alta Dirección.

Normas que rigen para la estructura organizacional de seguridad digital

Normas dirigidas a: ALTA DIRECCION

- Definir y establecer los roles y responsabilidades relacionados con la seguridad digital en los niveles directivo y operativo.
- Revisar y aprobar las Políticas de Seguridad Digital contenidas en este documento.
- Revisar y aprobar el presupuesto de seguridad digital.
- Promover una cultura de Seguridad Digital en todos los funcionarios de la Entidad y al personal provisto por terceras partes.
- Dirigir y apoyar a las personas para contribuir a la eficacia del Sistema de Gestión de Seguridad Digital.
- 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.
- Revisar el estado del Sistema de Gestión de Seguridad Digital.

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

- Actualizar y presentar ante la Junta Directiva las Políticas de Seguridad Digital.
- Analizar los incidentes de seguridad digital que le son escalados y activar el procedimiento de contacto con las autoridades y grupos de interés especial, cuando lo estime necesario.
- Verificar el cumplimiento de las políticas de seguridad digital del Instituto.
- Evaluar el estado del Sistema de Gestión de Seguridad Digital.

Normas dirigidas a: OFICINA DE RIESGOS

- 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.

- Actualizar las Políticas de Seguridad Digital con frecuencia anual, con sus roles y responsabilidades.
- Definir y establecer el procedimiento de contacto con las autoridades en caso de ser requerido, así como los responsables para establecer dicho contacto.
- Validar y monitorear con frecuencia anual la gestión de riesgos de seguridad.
- Formar en seguridad digital con frecuencia anual a todo el personal interno y contratistas, bajo un programa de educación y formación en aspectos de: Políticas, normas legales, procedimientos y manejo de incidentes.
- Gestionar los incidentes de seguridad digital y en caso de ser necesario dar aviso a autoridades competentes, de acuerdo con las normas legales establecidas.

Normas dirigidas a: OFICINA DE CONTROL INTERNO

- 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.
- 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.
- Socializar y Remitir el Informe de Auditoría Interna al Sistema de Gestión de Seguridad Digital, a la Oficina de Riesgos quien procederá a remitirlo a las áreas responsables.

Normas dirigidas a: TODOS LOS USUARIOS

- Los funcionarios y personal provisto por terceras partes que realicen labores en o para el ICETEX, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad digital.

8.2 POLITICA PARA USO DE DISPOSITIVOS MOVILES

El ICETEX provee las condiciones para el manejo de los dispositivos móviles (portátiles, teléfonos, inteligentes y tabletas, entre otros) institucionales y personales que hagan uso de servicios del Instituto. Así mismo, vela porque los funcionarios hagan un uso responsable de los servicios y equipos proporcionados por la Entidad.

Normas para uso de dispositivos móviles

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Investigar y probar las opciones de protección de los dispositivos móviles institucionales y personales que hagan uso de los servicios provistos por el Instituto.
- Establecer las configuraciones aceptables para los dispositivos móviles institucionales o personales que hagan uso de los servicios provistos por el ICETEX.

- Establecer un método de bloqueo para acceso al dispositivo y su memoria (contraseña, biometría, patrones gráficos, u otras opciones) para los dispositivos móviles institucionales que serán entregados a los usuarios.
- Definir mecanismos de protección de la información almacenada en dispositivos móviles para impedir su acceso en caso de robo o pérdida (borrado remoto y/o bloqueo permanente del dispositivo).
- Incluir en las políticas de copia de respaldo a los dispositivos móviles que por su naturaleza sean calificados como pública clasificada y pública reservada.
- Aplicar a los dispositivos móviles institucionales o personales que cumple funciones institucionales, los controles de protección contra código malicioso.
- Aplicar los controles de seguridad que eviten el uso de las SIM Card de las líneas móviles institucionales en equipos diferentes a los autorizados y registrados por el Instituto.
- Implementar los controles tecnológicos que impidan la conexión a redes y servicios del Instituto de equipos móviles con sistemas operacionales con modificaciones consideradas inseguras (Jailbreack, rooting, entre otros).
- Proveer los servicios que faciliten la actualización y aseguramiento de los sistemas operacionales y aplicaciones en los dispositivos institucionales.
- Monitorear el uso de los servicio y aplicaciones web del Instituto desde dispositivos móviles conectados a la red de datos del ICETEX.
- Implementar controles de seguridad en dispositivos móviles para monitorear, alertar y prevenir fugas de información.

<u>Normas dirigidas a: TODOS LOS USUARIOS</u>

- Para quienes tengan autorizado el uso de dispositivos móviles personales para tener acceso a la información institucional se suscribe un Acuerdo de Usuario Final de Dispositivo Móvil que incluye la renuncia de la propiedad de los datos institucionales, el borrado remoto en caso de incidentes con el dispositivo. En todo caso se preserva el derecho de la privacidad del propietario del dispositivo.
- Evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- No modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
- Evitar la instalación de programas desde fuentes desconocidas; Instalar aplicaciones en los dispositivos móviles únicamente desde repositorios seguros y previa consulta a la Dirección de Tecnología.
- Evitar hacer uso de redes inalámbricas de uso público inseguras para transmitir información institucional, así como conectar los dispositivos a equipos de uso compartido público (café internet, hoteles, computadores personales no institucionales).
- No almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.
- Preservando el derecho fundamental a la intimidad. las actividades realizadas con los dispositivos móviles institucional o los activos de información institucionales podrán ser

monitoreadas siguiendo los procedimientos administrativos del Instituto o los definidos por la normatividad vigente.

8.3 POLITICA PARA USO DE CONEXIONES REMOTAS

ICETEX define las circunstancias y requisitos para realizar conexiones remotas a su plataforma tecnológica y desde su plataforma a otras plataformas; así mismo, suministra las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

Normas para uso de conexiones remotas

Normas dirigidas a: OFICINA DE RIESGOS Y DIRECCION DE TECNOLOGIA

- Aprobar las conexiones remotas a la plataforma tecnológica del ICETEX en los formatos existentes

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica del ICETEX.
- Restringir las conexiones remotas a los recursos de la plataforma tecnológica; permitir los accesos solo a personal autorizado y por periodos de tiempo establecidos de acuerdo con las labores desempeñadas.
- Verificar la efectividad de los controles de seguridad aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica del ICETEX
- Monitorear los accesos de conexiones remotas a la plataforma tecnológica y alertar sobre potenciales amenazas internas y externas de acceso no autorizado a la información o recursos.
- Suministrar el soporte, mantenimiento y actualización del hardware y software empleado para realizar las conexiones remotas
- Implementar controles sobre herramientas de acceso remoto o nube para Monitorear, alertar y prevenir fugas de información.

Normas dirigidas a: OFICINA DE CONTROL INTERNO

- Dentro de su autonomía con el apoyo de la Dirección de Tecnología, podrá realizar auditorías sobre los controles implantados para las conexiones remotas a la plataforma tecnológica del ICETEX.

Normas dirigidas a: TODOS LOS USUARIOS

- Contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica del ICETEX y acatar las condiciones de uso establecidas para dichas conexiones.

- Los usuarios únicamente deben establecer conexiones remotas en computadores previamente identificados y, en ninguna circunstancia, en computadores públicos o de uso compartido, de hoteles o cafés internet, entre otros.

9. POLÍTICAS DE SEGURIDAD DEL PERSONAL

9.1 POLÍTICA RELACIONADA CON LA VINCULACIÓN DE FUNCIONARIOS

ICETEX reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con el personal mejor calificado, garantiza que la vinculación de nuevos funcionarios se realiza siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual está orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos.

Normas relacionadas con la vinculación de funcionarios

Normas dirigidas a: SECRETARIA GENERAL - GRUPO DE TALENTO HUMANO

- Realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo en ICETEX, antes de su vinculación definitiva.
- Certificar que los funcionarios del Instituto firmen el Compromiso de Confidencialidad y no divulgación de información y datos personales (F398) y almacenar dichas evidencias de acuerdo con las normas institucionales de gestión de archivo.

Normas dirigidas a: SUPERVISORES DE CONTRATO, ESTRUCTURADORES DE ESTUDIOS PREVIOS DE CONTRATOS, VICEPRESIDENTES, DIRECTORES Y JEFES DE OFICINA

- Asegurar la existencia de Acuerdos y/o Cláusulas de Confidencialidad y de la documentación de Aceptación de Políticas para el personal provisto por terceras partes, antes de otorgar acceso a la información del ICETEX.
- Especificar las responsabilidades del personal propuesto por el proponente durante el proceso de contratación.

Normas dirigidas a: PERSONAL PROVISTOS POR TERCERAS PARTES

- Firmar un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad digital, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.
- Garantizar el cumplimiento de los Acuerdos y/o Cláusulas de Confidencialidad y aceptación de las Políticas de Seguridad digital del Instituto.
- Proveer el personal de acuerdo con los perfiles definidos en los contratos suscritos con el ICETEX.

9.2 POLÍTICA APLICABLE DURANTE LA EJECUCION DEL EMPLEO

La Alta Dirección en su interés por proteger la información, fomenta la cultura de seguridad digital y la gestión de riesgos durante el desarrollo de las actividades de los funcionarios y contratistas, ejecutando jornadas de capacitación, sensibilización y promulgando la presente política.
Todos los funcionarios y personal provisto por terceros deben cuidar no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgos la seguridad y el buen nombre de la Entidad.

Normas aplicables durante la ejecución del empleo de funcionarios y personal provisto por terceros

Normas dirigidas a: ALTA DIRECCION

- Promover el fortalecimiento de la cultura en seguridad digital para el uso adecuado de la información y así afianzar la confianza con los clientes, funcionarios y terceras partes.

Normas dirigidas a: OFICINA DE RIESGOS

- Establecer los principios y lineamientos para promover la cultura de seguridad digital que incluye actividades de difusión, capacitación y concientización tanto al interior de la Entidad como frente a usuarios y terceros.
- Formular y coadyuvar en la ejecución y actualización del programa de capacitación, sensibilización y toma de conciencia en seguridad digital, políticas, procedimientos y controles de ingeniería social para los funcionarios y contratistas.

Normas dirigidas a: SECRETARIA GENERAL

- Aplicar las medidas administrativas del Instituto cuando se identifiquen violaciones o incumplimientos a las políticas de seguridad digital.

Normas dirigidas a: SECRETARIA GENERAL - GRUPO DE TALENTO HUMANO

- Convocar a los funcionarios y contratistas a las charlas y eventos programados como parte del programa de concienciación en seguridad digital.
- Proveer los recursos para la ejecución de las capacitaciones y controlar la asistencia a dichas charlas y eventos, y tomar las acciones correctivas por la falta de asistencia no justificada.

Normas dirigidas a: TODOS LOS USUARIOS

- Cumplir con las políticas y controles de seguridad y normatividad vigentes, aplicables al Instituto.
- Asistir a las capacitaciones y jornadas de educación y formación que programe el Instituto en materia de seguridad digital con el fin de adquirir las competencias necesarias para el debido manejo de la información.

9.3 POLÍTICA DE DESVINCULACIÓN, LICENCIAS, VACACIONES O CAMBIO DE LABORES DE LOS FUNCIONARIOS Y PERSONAL PROVISTO POR TERCEROS

ICETEX asegura que sus funcionarios y el personal provisto por terceros son desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura.

Normas para la desvinculación, licencias, vacaciones o cambios de labores de los funcionarios y personal provisto por terceros

Normas dirigidas a: SECRETARIA GENERAL - GRUPO DE TALENTO HUMANO

- Realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios del Instituto llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.

Normas dirigidas a: SUPERVISORES DE CONTRATO, VICEPRESIDENTES, DIRECTORES Y JEFES DE OFICINA

- Monitorear y reportar de manera inmediata la desvinculación o cambio de labores de los funcionarios o personal provistos por terceras partes a la Oficina de Riesgos.

Normas dirigidas a: OFICINA DE RIESGOS

- Verificar los reportes de desvinculación o cambio de labores y solicitar la modificación o inhabilitación de usuarios a la Dirección de Tecnología.

10. POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

10.1 POLÍTICA DE RESPONSABILIDAD POR LOS ACTIVOS

La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) son propiedad del ICETEX, y se proporcionan a los funcionarios y terceros autorizados para cumplir con los propósitos del negocio.

ICETEX como propietario de la información delega en los Jefes de áreas el cumplimiento de las directrices que regulan el uso adecuado de los activos de la información en su ciclo de vida.

Los recursos tecnológicos del ICETEX, deben ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen del Instituto.

Normas de responsabilidad por los activos

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

Los Vicepresidentes, Directores y Jefes de Oficinas Asesoras del ICETEX, deben actuar como propietarias de la información física y electrónica de la Entidad, para lo cual deben:

- Designar, autorizar o revocar el acceso a la información y a los recursos tecnológicos.
- Recibir los recursos tecnológicos asignados a sus colaboradores cuando estos se retiran del Instituto o son trasladados de área.
- Generar un inventario de dichos activos para los procesos que lideran, acogiendo las indicaciones de las Guía para la Clasificación de Activos de Información, así mismo, deben mantenerlo actualizado.
- Monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información.
- Ser conscientes que los recursos de procesamiento de información del Instituto, se encuentran sujetos a auditorías por parte de la Oficina de Control Interno y a revisiones de cumplimiento por parte de la Oficina de Riesgos.

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología es la propietaria de los activos informáticos del ICETEX y, en consecuencia, debe asegurar su apropiada operación y administración.
- La Dirección de Tecnología en conjunto con el Comité de Control de Cambios, son quienes deben autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica del ICETEX.
- Establecer, operar y mantener las configuraciones adecuadas para los recursos tecnológicos, con el fin de preservar la seguridad digital y hacer un uso adecuado de ellos.
- Preparar las estaciones de trabajo fijas y/o portátiles de los funcionarios y hacer entrega de las mismas a los autorizados.
- Recibir los equipos de cómputo para su reasignación o disposición final, y generar copias de seguridad digital de los funcionarios que se retiran o cambian de labores.

Normas dirigidas a: OFICINA DE RIESGOS

- La Oficina de Riesgos debe realizar un análisis de riesgos de seguridad de manera periódica, sobre los procesos del ICETEX.
- La Oficina de Riesgos debe definir las condiciones de uso y protección de los activos de información, tanto los tecnológicos como aquellos que no lo son.
- La Oficina de Riesgos debe realizar revisiones periódicas de los recursos de la plataforma tecnológica y los sistemas de información del instituto.

Normas dirigidas a: VICEPRESIDENTES, DIRECTORES Y JEFES DE OFICINA

- Los Vicepresidentes, Directores y Jefes de Oficina, o quien ellos designen, deben autorizar a sus funcionarios el uso de los recursos tecnológicos, previamente preparados por la Dirección de Tecnología.

Normas dirigidas a: TODOS LOS USUARIOS

- Los recursos tecnológicos del ICETEX provistos a funcionarios y personal suministrado por terceras partes, tienen como único fin llevar a cabo las labores del Instituto; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.
- No utilizar equipos fijos o móviles o software de propiedad personal para realizar labores propias del Instituto.
- Hacer uso adecuado y eficiente de los recursos tecnológicos para el cumplimiento de las labores asignados.
- En el momento de desvinculación o cambio de labores, los funcionarios deben realizar la entrega de su puesto de trabajo al Vicepresidente, Director o Jefe de Oficina o quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

10.2 POLÍTICA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

ICETEX define los niveles más adecuados para clasificar su información de acuerdo con los requisitos legales, criticidad, susceptibilidad a divulgación no autorizada, y genera la Guía para la clasificación de los activos de información con el fin de que los propietarios de la misma las apliquen y ejecuten los controles requeridos para su protección.

ICETEX proporciona los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de la misma, con el fin de promover el uso adecuado por parte de los funcionarios y personal provisto por terceras partes que se encuentren autorizados y requieran de ella para la ejecución de sus actividades.

La información, así como los activos donde ésta se almacena y se procesa, deben ser asignados a un responsable, inventariados y clasificados para darles una adecuada protección. Los propietarios de los activos de información deben llevar a cabo la actualización del inventario al interior de sus procesos o áreas, con frecuencia anual.

Normas para la clasificación y manejo de la información

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACION

- Recomendar los niveles de clasificación de la información propuestos por la Oficina de Riesgos y la Guía para la clasificación de los activos de Información del ICETEX.

Normas dirigidas a: OFICINA DE RIESGOS

- Definir los niveles de clasificación de la información para el ICETEX, de acuerdo con los lineamientos normativos.
- Socializar y divulgar la Guía para la clasificación de activos de la Información a los funcionarios y contratistas del Instituto.
- Monitorear con una periodicidad establecida la aplicación del Procedimiento Identificar y clasificar activos de información.

- Asesorar en el inventario y clasificación de los activos de información del ICETEX a las diferentes dependencias.
- Consolidar el Inventario y Clasificación de Activos de Información y asegurar su aprobación y publicación en el Portal Web – Ley de Transparencia.

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Proveer, ejecutar y monitorear los controles técnicos establecidos en la Guía para el manejo de los activos de información y normas legales de acuerdo con la clasificación de la información.
- Administrar el almacenamiento, respaldo, resguardo y pruebas de las cintas de backup y otros medios de almacenamiento.
- Administrar el almacenamiento y resguardo de los documentos físicos de la Entidad.

Normas dirigidas a: DIRECCION DE TECNOLOGIA Y OFICINA DE RIESGOS

- Asesorar en la definición de los controles de acuerdo con el nivel de clasificación de los activos de información.

Normas dirigidas a: SECRETARIA GENERAL – COORDINACION DE GESTION DOCUMENTAL

- Utilizar los medios de los cuales está dotada para realizar adecuadamente la disposición final de la documentación física y electrónica con base en lo establecido y dispuesto en las Tablas de Retención Documental de la entidad, con el fin de evitar la reconstrucción de la misma, acogiéndose a procedimiento establecido para tal fin.
- La información física y electrónica del ICETEX debe tener un período de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla su período de retención, debe aplicarse su disposición final de acuerdo con la normatividad aplicable.
- Administrar el almacenamiento y resguardo de los documentos físicos y electrónicos de archivo de la Entidad.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Generar un inventario de activos de información para los procesos que lideran, así como la clasificación de acuerdo con la Guía para la clasificación de los activos de Información establecida la cual está basada en las Tablas de Retención Documental de la entidad.
- Ejecutar y monitorear los controles de resguardo de la información de acuerdo con la Guía para el manejo de los activos información y etiquetado.

Normas dirigidas a: TODOS LOS USUARIOS (FUNCIONARIOS Y PERSONAL PROVISTO POR TERCERAS PARTES)

- Acatar los lineamientos de la guía para el manejo de los activos información y etiquetado para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación

de la información contenida en los recursos tecnológicos, así como de la información física Instituto.

- Impedir el acceso no autorizado a información impresa, digitalizada o almacenada en puestos de trabajo cuando quedan desatendidos
- Mantener los puestos trabajos libres de documentos y medios de almacenamiento utilizados para el desempeño de las labores cuando se finaliza la jornada laboral;
- Aplicar los controles de seguridad definidos por el Instituto para la preservación de la confidencialidad, integridad y disponibilidad de los activos de información tanto en estaciones de trabajo como en ambientes de procesamientos en nube de datos.

10.3 POLITICA PARA USO DE TOKENS DE SEGURIDAD

ICETEX provee las condiciones de manejo de los tokens de seguridad para los procesos que los utilizan y vela porque los colaboradores hagan un uso responsable de éstos.

Normas para uso de tokens de seguridad

Normas dirigidas a: AREAS USUARIAS DE TOKENS DE SEGURIDAD

- Cada área usuaria de tokens de seguridad debe asignar un funcionario administrador de los mismos con la potestad para autorizar su utilización.
- Para firmas digitales de documentos, el Jefe de cada área autoriza a los colaboradores para la asignación y/o desactivación de tokens, siendo el Administrador la Dirección de Tecnología.

Normas dirigidas a: ADMINISTRADORES DE LOS TOKENS DE SEGURIDAD

- Procesar las solicitudes de los tokens según los requerimientos de cada Entidad proveedora de éstos y adjuntar la documentación necesaria.
- Recibir los tokens y realizar la activación necesaria en los respectivos portales o sitios de uso para poder realizar las operaciones con ellos.
- Crear los usuarios y perfiles en cada portal o sitio de uso, según las actividades asignadas a cada funcionario.
- Entregar a los funcionarios designados los usuarios y seriales de los dispositivos que le son asignados para su uso, formalizando la entrega por medio de acta y tula (o sobre) de seguridad para custodia de los mismos.
- Avisar a las Entidades emisoras en caso de robo o pérdida de estos con el fin de efectuar el bloqueo respectivo y la reposición de los mismos.
- Realizar el cambio de token, cuando se presente mal funcionamiento, caducidad, cambio de funciones o cambio del titular, reportando a la Entidad emisora y devolviendo los dispositivos asignados.

Normas dirigidas a: USUARIOS DE TOKENS DE SEGURIDAD

- Contar con una cuenta de usuario en los portales o sitios de uso de los mismos; dichos tokens harán parte del inventario físico de cada usuario a quien se haya asignado.
- Devolver el token asignado en estado operativo al Administrador de los tokens cuando el vínculo laboral con el ICETEX se dé por terminado o haya cambio de cargo, para obtener paz y salvo, el cual será requerido para legalizar la finalización del vínculo con el Instituto.
- Cada usuario de los portales o sitios de uso de los tokens debe tener su propio dispositivo, el cual es exclusivo, personal e intransferible, al igual que la cuenta de usuario y la contraseña de acceso.
- El almacenamiento de los tokens debe efectuarse bajo estrictas medidas de seguridad, previendo su acceso o utilización no autorizada (almacenamiento en la tula, sobre asignado, caja fuerte, escritorio con llave, gaveta u otros).
- Prevenir su daño por contacto con líquidos, sustancias químicas, fuego o agentes que los puedan dañar (polvo, fuentes de calor extremo, campos magnéticos fuertes, etc.
- No realizar modificaciones físicas al dispositivo como cambio de baterías, apertura, grabación o borrado de datos.
- Almacenar de manera segura el token mientras no está en uso o cuando está desatendido el puesto de trabajo.
- Notificar al Administrador de los tokens en caso de robo, pérdida, mal funcionamiento o caducidad para que este a su vez, se comuniquen con las Entidades emisoras de dichos tokens.
- Mantener en secreto las claves de uso del token. Utilizar servicios de soporte únicamente de personal autorizado por los administradores de los token.
- Asumir la responsabilidad por las transacciones electrónicas que se efectúen con la cuenta de usuario, clave y el token asignado, en el desarrollo de las actividades como funcionarios del ICETEX.
- Asumir la responsabilidad administrativa, disciplinaria y económica en caso de uso no autorizado o irregularidad con los tokens asignados.

10.4 POLÍTICA DE USO DE PERIFERICOS Y MEDIOS DE ALMACENAMIENTO PORTÁTILES

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica del ICETEX es establecido, conjuntamente por la Dirección de Tecnología y la Oficina de Riesgos, considerando las labores realizadas por los funcionarios y su necesidad de uso.

Normas uso de periféricos y medios de almacenamiento

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica del Instituto, de acuerdo con las condiciones establecidas.
- Monitorear el uso de periféricos y medios de almacenamiento en la plataforma tecnológica y las estaciones de trabajo del Instituto.
- Mantener el inventario de funcionarios y personal provisto por terceros autorizados y habilitados para dar uso de dispositivos de almacenamiento con sus respectivos soportes.

Normas dirigidas a: OFICINA DE RIESGOS

- Autorizar y mantener actualizado los derechos de uso de periféricos o medios de almacenamiento en la plataforma tecnológica del Instituto de acuerdo con el perfil del cargo del funcionario solicitante.
- Generar los lineamientos para el uso de los medios de almacenamiento del Instituto, ya sea cuando son dados de baja o re-asignados a un nuevo usuario.

Normas dirigidas a: VICEPRESIDENTES, DIRECTORES Y JEFES DE OFICINA

- Realizar inventario los dispositivos de almacenamiento removibles.
- Reportar a la Oficina de Riesgos, los usuarios del área a su cargo que tienen habilitados permisos para acceso a dispositivos de almacenamiento removibles en sus estaciones de trabajo.

Normas dirigidas a: TODOS LOS USUARIOS (FUNCIONARIOS Y PERSONAL PROVISTOS POR TERCERAS PARTES)

- Cumplir las condiciones .de uso de los periféricos y medios de almacenamiento establecidos por la Oficina de Riesgos.
- No modificar la configuración de periféricos y medios de almacenamiento establecidos por la

Dirección de Tecnología

- Custodiar los medios de almacenamiento institucionales asignados.
- No utilizar medios de almacenamiento personales en la plataforma tecnológica del ICETEX.

10.5 POLÍTICA DE BORRADO SEGURO

El ICETEX vela porque se realice borrado seguro en los dispositivos que contengan información pública reservada o pública clasificada, tanto para funcionarios y contratistas, cuando se apliquen las siguientes acciones al dispositivo:

- Reasignar a otro funcionario, contratista.
- Enviar a bodega.
- Cambiar del dispositivo.
- Devolver por terminación de contrato laboral.
- Reparar por parte del proveedor o un tercero.
- Regresar al proveedor por fin de contrato de suministro.
- En caso de hurto del dispositivo

Normas de política de borrado seguro

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Definir el mecanismo de borrado o método de disposición final de acuerdo con el tipo de dispositivo, contemplando:
- Evidenciar del borrado o disposición final.
- Impedir la recuperación de la información del medio a través de controles de cifrado. Seleccionar de manera apropiada los servicios de borrado o destrucción por terceros en caso de contratación del servicio.

10.6 POLÍTICA DE ALMACENAMIENTO DE INFORMACIÓN DIGITAL

ICETEX proporciona los medios de almacenamiento seguros a nivel local como en la nube, con el fin de facilitar el acceso, uso y respaldo de la información, mitigando el riesgo de pérdida y acceso a la misma.

Normas para el Almacenamiento de información

Normas dirigidas a: DIRECCIÓN DE TECNOLOGIA

- Proveer el espacio de los recursos de almacenamiento en las carpetas compartidas del FileServer de acuerdo con los requerimientos de las distintas dependencias.
- Administrar la seguridad y capacidad de las carpetas compartidas mediante la asignación y retiro de usuarios y el acceso a la información contenida en la carpeta, de acuerdo con los permisos definidos por el Líder de Proceso, permitiendo la conexión únicamente a nivel local o por medio de VPN, así mismo gestiona el tamaño de las carpetas de acuerdo las necesidades de los procesos.
- Realizar copias de respaldo de la información alojada en carpetas compartidas.
- Proveer y administrar las cuentas de Office 365 a los funcionarios y contratistas dentro de las cuales se incluye un espacio de almacenamiento en OneDrive, donde se implementa los controles de acuerdo con las políticas de seguridad.

Normas dirigidas a: OFICINA DE RIESGOS

- Coordinar con la Dirección de Tecnología las recomendaciones de seguridad para el almacenamiento de información.
- Verificar el cumplimiento de las políticas en almacenamiento de información de manera aleatoria de acuerdo con el plan de seguimiento al Modelo de Seguridad y Privacidad Digital.

Normas dirigidas a: TODOS LOS USUARIOS

- Utilizar los servicios de almacenamiento únicamente para las labores asignadas por la Entidad.
- Los recursos compartidos en OneDrive o el que disponga la Entidad, son administrados por cada uno de los usuarios, quienes son los responsables del uso y accesos que se concedan a la información.

- La información catalogada como Pública Clasificada y Pública Reservada que requiera compartir desde OneDrive a nivel externo con proveedores o terceros y Entes de Control deberá tener la autorización del Líder de Proceso y la evaluación de la Oficina de Riesgos y la Dirección de Tecnología para determinar si es la mejor opción operativa y de seguridad para transmitir la información.
- Está prohibido compartir información desde OneDrive con personas que no tienen ningún vínculo contractual con la Entidad.
- La información que se almacena en la carpeta compartida tiene como fin el compartirla con una o más personas al interior de la Entidad.

Normas dirigidas a: VICEPRESIDENTES, DIRECTORES Y JEFES DE OFICINA

- Garantizar que el personal del área a cargo está realizando el debido almacenamiento en los repositorios definidos.
- Gestionar los permisos sobre las carpetas compartidas del FileServer a través de la herramienta de gestión.
- Gestionar los requerimientos de backup de la información del equipo de cómputo, del correo electrónico y OneDrive de los colaboradores, a través de la herramienta de gestión. El backup solicitado del funcionario o contratista retirado será almacenado en el repositorio temporal del Fileserver durante 6 meses el cual tendrá acceso el Jefe de Área y personal a su cargo que este asigne.

11. POLÍTICAS DE CONTROL DE ACCESO

ICETEX en busca de garantizar un adecuado control de acceso a sus activos de información, ha definido las políticas para garantizar un adecuado control de acceso a los sistemas, para ello se implementan mecanismos de control para acceder a la red, sistemas operativos, bases de datos, sistemas de información y en general a todo elemento que de alguna forma acceda a información de carácter público reservado o publico clasificado, cuyo origen sea el ICETEX. De igual manera, implementa procedimientos para la asignación de privilegios de acceso a los sistemas.

El acceso a los sistemas de información e información está determinado por el principio de mínimo privilegio necesario para el cumplimiento de las labores asignadas a funcionarios y contratistas.
El acceso a la información contempla el establecimiento de permisos específicos para leer, escribir, modificar, borrar o ejecutar utilidades que procesen información institucional.

11.1 POLÍTICA DE ACCESO A REDES Y RECURSOS DE RED

La Dirección de Tecnología del ICETEX, como responsable de las redes de datos y los recursos de red del Instituto, propende porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico y físicos monitoreados y con capacidad de generar alertas.

Normas de acceso a redes y recursos de red

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Establecer el procedimiento y los controles de acceso a los ambientes de producción, pruebas y desarrollo de los sistemas de información, redes de datos y los recursos de red del ICETEX.
- Asegurar que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
- Asegurar que las redes inalámbricas del Instituto cuenten con métodos de autenticación y cifrado que eviten accesos no autorizados.
- Asignar credenciales de acceso a los diferentes sistemas de forma separada, garantizando la segregación de tareas y limitando la autorización de acceso solo la información indispensable para la ejecución de las labores asignadas.
- Establecer en conjunto con la Oficina de Riesgos los controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red del ICETEX, así como velar por la aceptación de las responsabilidades sobre uso de activos, acuerdos de confidencialidad y las Políticas de Seguridad digital
- Monitorear, alertar y reportar actividades anómalas respecto al acceso y uso de los datos en los sistemas de información, redes de datos y los recursos de red del ICETEX a los responsables de los procesos de dichos sistemas de información.
- La Dirección de Tecnología, con la solicitud de cuentas de usuario debidamente aprobada por el Jefe de Área a la cual pertenece el solicitante y la validación de la Oficina de Riesgos, debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados, acorde con el procedimiento establecido.
- Configurar los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos del Instituto para que cumplan con todos los requisitos o controles para autenticase en ellas.

Normas dirigidas a: DESARROLLADORES (INTERNOS Y EXTERNOS)

- Los desarrolladores deben, a nivel de los aplicativos, restringir acceso a archivos de configuración u otros recursos, a direcciones URL protegidas, a funciones protegidas, a credenciales, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas por los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados.

Normas dirigidas a: OFICINA DE RIESGOS

- Validar la creación o modificación de las cuentas de acceso a las redes o recursos de red del ICETEX.

Normas dirigidas a: VICEPRESIDENTES, DIRECTORES Y JEFES DE OFICINA

- Solicitar la creación, modificación, bloqueo y eliminación de cuentas de usuario, para los funcionarios que laboran en sus áreas, acogiéndose al procedimiento establecido para tal fin.

Normas dirigidas a: TODOS LOS USUARIOS (Funcionarios y Terceras partes)

- Diligenciar el formato de creación de cuentas de usuario (F121 Formato de asignación / retiro de accesos a sistemas de información) y realizar los trámites de solicitud antes de contar con acceso lógico por primera vez a la red de datos del ICETEX.
- Informar oportunamente a la Oficina de Riesgos y al Líder de Proceso sobre cualquier inconveniente, ya sea por exceso o falta de permisos, para acceder a la información.
- Utilizar las redes y servicios de comunicación del Instituto únicamente para el cumplimiento de las funciones asignadas evitando usos no autorizados o en beneficio propio.

11.2 POLÍTICA DE ADMINISTRACIÓN DE ACCESO DE USUARIOS

ICETEX establece privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información del Instituto. Así mismo, vela porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

Normas de administración de acceso de usuarios

Normas dirigidas a: OFICINA DE RIESGOS

- Solicitar periódicamente a la Dirección de Tecnología los registros y seguimientos a las actividades sobre los sistemas de información por parte de usuarios con permisos elevados (administrator, root, etc.), para analizarlos y de esta forma, analizar los riesgos a los que se están exponiendo los sistemas de información y recursos de red del ICETEX, con las actividades de dichos usuarios.
- Revisar periódicamente los controles de acceso a los recursos tecnológicos y sistemas de información con el fin de verificar que los usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios de las plataformas tecnológicas para los que fueron autorizados.

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Establecer un procedimiento formal para la administración de los usuarios que asegure la creación, modificación, bloqueo o eliminación de cuentas de usuario, sobre los recursos

tecnológicos, los servicios de red y los sistemas de información de manera oportuna cuando los funcionarios se vinculan, desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.

- Verificar periódicamente los controles de acceso de los usuarios, con el fin de revisar que éstos tengan acceso permitido únicamente a aquellos recursos de red y servicios de las plataformas tecnológicas para los que fueron autorizados.

11.3 POLÍTICA DE RESPONSABILIDADES DE ACCESO DE LOS USUARIOS

Los usuarios de los recursos tecnológicos y los sistemas de información del ICETEX realizan un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

Normas de responsabilidades de acceso de los usuarios

Normas dirigidas a: TODOS LOS USUARIOS

- Ser responsables de las acciones realizadas con las cuentas de usuario asignadas, contraseña y los privilegios otorgados.
- No compartir sus cuentas de usuario y contraseñas con otros funcionarios o con personal provisto por terceras partes.
- Acogerse a lineamientos para la configuración de contraseñas implantados por el Instituto.
- Utilizar las cuentas de usuario únicamente para el desarrollo de las labores asignadas.
- Informar oportunamente a la Oficina de Riesgos y al Líder de Proceso sobre cualquier inconveniente con los accesos de usuario, ya sea por exceso o falta de permisos, para acceder a la información.

11.4 POLÍTICA DE USO DE ALTOS PRIVILEGIOS Y UTILITARIOS DE ADMINISTRACION

La Dirección de Tecnología del ICETEX vela porque los recursos de la plataforma tecnológica y los servicios de red del Instituto sean operados y administrados en condiciones controladas y de seguridad, implementa y opera controles para el monitoreo, alertamiento temprano y automático de actividades de los usuarios administradores, poseedores de los más altos privilegios sobre dichos plataforma y servicios.

Normas de uso de altos privilegios y utilitarios de administración

Normas dirigidas a: DIRECCION DE TECNOLOGIA, ADMINISTRADORES DE LOS RECURSOS TECNOLOGICOS Y SERVICIOS DE RED

- Otorgar los privilegios de acceso para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos funcionarios designados para dichas funciones.
- Establecer cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información.

- Verificar y asegurar que los desarrolladores, administradores de los recursos tecnológicos y servicios de red no tengan acceso a sistemas de información en producción. Restringir las conexiones remotas a los recursos de la plataforma tecnológica solo a personal debidamente autorizado y solo para las labores asignadas.
- Implementar líneas bases de aseguramiento a los sistemas de información y tecnologías, de acuerdo con la arquitectura definida para cada para los mismos.
- Establecer los 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 accesos privilegiados a dichos recursos, servicios, sistemas o ambientes tecnológicos.
- Generar y mantener actualizado un listado de las cuentas administrativas de los recursos de la plataforma tecnológica.

Normas dirigidas a: OFICINA DE RIESGOS

- Validar que las políticas de contraseñas establecidas sobre la plataforma tecnológica, los servicios de red y los sistemas de información son aplicables a los usuarios administradores; así mismo, verificar que el cambio de contraseña de los usuarios administradores acoja el procedimiento de Guía de Contraseñas seguras definido para tal fin.
- Revisar periódicamente la actividad de los usuarios con altos privilegios en los registros de auditoria de la plataforma tecnológica y los sistemas de información.

Normas dirigidas a: TODOS LOS USUARIOS

- No utilizar herramientas o software que permitan evadir los controles de seguridad de los recursos tecnológicos y servicios de red.

11.5 POLÍTICA DE CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

ICETEX vela porque todos los usuarios se identifiquen en los sistemas de información y recursos tecnológicos, se autentiquen con credenciales únicas y las autorizaciones se otorguen conforme a los niveles de acceso a la información.
Se registran los accesos exitosos y fallidos a los sistemas de información y tecnologías con el fin de identificar y alertar posibles amenazas de accesos y cambios no autorizados.

Normas de control de acceso a sistemas y aplicativos

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Establecer ambientes separados a nivel físico y lógico para desarrollo, pruebas y producción, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.
- Asegura que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción.
- Establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información;

- Asegurar que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
- Controlar el acceso al código fuente de los programas, sistemas de información o software desarrollado por el ICETEX solo al personal autorizado y llevar control de los cambios autorizados a código fuente.
- Definir en conjunto con la Oficina de Riesgos los lineamientos para la configuración de contraseñas que se apliquen sobre la plataforma tecnológica, los servicios de red y los sistemas de información del ICETEX, incluyendo longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso además de otros definidos en buenas prácticas o identificados por el Instituto.

Normas dirigidas a: DESARROLLADORES (INTERNOS Y EXTERNOS)

- Asegurar que los sistemas de información construidos exijan autenticación para todos los recursos y operaciones ejecutadas con el software.
- Certificar que no se almacenen contraseñas, cadenas de conexión u otra información pública clasificada y pública restringida en texto claro y que se implementen controles de integridad de dichas contraseñas.
- Establecer los controles de autenticación que eviten la visualización de contraseñas.
- Desarrollar el software siguiendo estándares de desarrollo seguro.
- Implementar en el software controles que eviten múltiples intentos de autenticación fallida.
- Implementar en el software controles que obliguen al usuario a cambiar la contraseña por defecto en el primer ingreso.

Normas dirigidas a: VICEPRESIDENTES, DIRECTORES Y JEFES DE OFICINA

- Definir los perfiles de usuario a los sistemas de información, de manera conjunta con la Dirección de Tecnología y la Oficina de Riesgos.
- Velar por la asignación controlada de privilegios de acceso, modificación, revocación a los sistemas de información bajo su responsabilidad.
- Monitorear periódicamente los perfiles definidos en los sistemas de información bajo su responsabilidad y los privilegios asignados a los usuarios que acceden a ellos.
- Verificar y ratificar semestralmente todas las autorizaciones sobre sus recursos tecnológicos.

Normas dirigidas a: OFICINA DE RIESGOS

- Revisar la creación o modificación de los perfiles que acceden a los recursos tecnológicos y sistemas de información del Instituto.

Normas dirigidas a: TODOS LOS USUARIOS

- Informar oportunamente de cualquier inconveniente, ya sea por exceso o falta de permisos, para acceder a la información al responsable de la dependencia a la Oficina de Riesgos.
- Usar correctamente los perfiles asignados de acuerdo con las funciones asignadas.
- Está prohibido guardar contraseñas en lugares visibles, almacenar en navegadores, archivos o sitios no controlados.

12. POLÍTICA DE TRABAJO REMOTO

ICETEX permite realizar actividades a través de trabajo remoto a sus funcionarios y contratistas, validando los aspectos de seguridad digital en el uso de los activos de información.

Normas de Política de Trabajo Remoto

Normas dirigidas a: LIDERES DE PROCESO

- Autorizar a los funcionarios y contratistas los permisos de acceso remoto a sistemas de Información y medios de almacenamiento de los cuales dispondrán.
- Identificar los activos de información necesarios para realizar el trabajo remoto.

Normas dirigidas a: OFICINA DE RIESGOS

- Apoyar en la identificación, análisis y valoración de los riesgos asociados a las actividades de trabajo remoto.
- Verificar que se cumplan los controles sobre la infraestructura del ICETEX, establecidos para el trabajo remoto.

Normas dirigidas a: DIRECCIÓN DE TECNOLOGÍA

- Establecer los mecanismos de gestión y recursos técnicos de comunicación para proveer el servicio de conexión remota a los sistemas internos y acceso a la información a la que tendrán acceso los usuarios autorizados.
- Dar soporte técnico a los equipos, conexiones, sistemas de información, medios de almacenamiento y comunicación de propiedad del ICETEX usados en trabajo remoto.
- Restringir las conexiones remotas a los recursos de la plataforma tecnológica del ICETEX; únicamente a los equipos autorizados.
- Monitorear el uso de los recursos e infraestructura dispuesta para el trabajo remoto, previniendo y detectando vulnerabilidades, ataques cibernéticos y otras amenazas; así como incidentes de seguridad digital.

Normas dirigidas a: FUNCIONARIOS, CONTRATISTAS Y PERSONAL DE TERCEROS

- En los equipos de cómputo utilizados para realizar el trabajo remoto configurar el inicio de sesión con algún medio de autenticación como password, pin, y/o huella.
- Almacenar la información tratada durante el trabajo remoto en el servicio en la nube que disponga la Entidad para almacenar, proteger y compartir los archivos.
- Resguarda y proteger la información de acuerdo con la clasificación de los activos de información.
- Contar con un lugar seguro para almacenar documentos físicos y otros activos de información de propiedad de ICETEX.

- ❖ Proteger la información a la que se tiene acceso en los lugares en los que se realiza trabajo remoto.
- ❖ Informar inmediatamente de cualquier evento de riesgo que pueda generar compromiso sobre: el equipo del ICETEX, la información, credenciales de acceso, los sistemas de información, los medios de almacenamiento y las comunicaciones usados para el trabajo remoto.
- ❖ Proteger físicamente los equipos del ICETEX que se utilicen para realizar trabajo remoto para prevenir el robo de éstos, transportándolos y guardándolos en un lugar seguro, usando guaya siempre que sea posible, y protegiéndolos, en especial en lugares públicos.
- ❖ No conectarse a los sistemas de información, medios de almacenamiento y comunicación usados para el trabajo remoto desde redes públicas, en lo posible usar redes cableadas.
- ❖ Usar unicamente las aplicaciones colaborativas y de teleconferencia permitidas por el Instituto, así como sus condiciones de uso, está prohibido ingresar a programas no controlados o autorizados por la Entidad.
- ❖ Para videoconferencia incluir mejores prácticas como: activar la sala de espera y bloquear la reunión, de manera que el administrador brinde acceso solo a usuarios permitidos, evitar compartir información confidencial en estos entornos y si se va a grabar la reunión, comunicar previamente a todos los participantes.
- ❖ Reforzar las políticas de seguridad aplicables, como evitar hacer clic en enlaces que parecen sospechosos, descargar anexos solamente de fuentes conocidas, no abrir correos de remitentes desconocidos, evitar el uso de redes sociales y aplicaciones de mensajería no corporativa, evitar navegar por páginas no seguras, así como evitar el uso de soportes externos de almacenamiento como dispositivos USB y en caso de utilizarlos, escanearlos con el software antivirus.
- ❖ En caso de utilizar equipo personal para el desarrollo de trabajo remoto, es necesario cumplir con las siguientes condiciones:
  - Mantener actualizado el Sistema Operativo.
  - Garantizar el buen funcionamiento del equipo.
  - Se recomienda contar con antivirus instalado, activo y actualizado y licenciamiento de software instalado en dicho equipo de cómputo.

13. POLÍTICAS DE CRIPTOGRAFIA

ICETEX vela por proteger la información pública clasificada y pública reservada mediante mecanismos de cifrado al momento de ser transferida o transmitidas a terceras partes.

Las claves de acceso a sistemas de información y sistemas operacionales se almacenas en forma cifrada para preservar su confidencialidad.

13.1 POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

ICETEX vela porque la información del Instituto, calificada como clasificada y reservada, sea cifrada al momento de transferirse y/o transmitirse por cualquier medio.

Normas de controles criptográficos

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Almacenar, transferir y/o transmitir la información digital calificada como clasificada y reservada, por el dueño de la información, bajo técnicas de cifrado fuerte con el propósito de proteger su confidencialidad e integridad.
- Aplicar con base en buenas prácticas de la industria mecanismos de verificación de integridad de la información con herramientas de cifrado.
- Mantener activos y documentados los controles sobre el ciclo de vida de las llaves criptográficas incluidas la generación, almacenamiento, archivo, recuperación, distribución, retiro y destrucción de las mismas.
- Verificar que las llaves de cifrado solo puedan ser utilizadas para una sola función, (firma electrónica o cifrado de datos, autenticación, etc.), nunca para varias funciones o sean reutilizadas. Como caso especial, se acepta el uso de la misma llave de cifrado para elementos que ofrecen más de un servicio criptográfico, por ejemplo: una llave de firma digital puede ser utilizada, para tener integridad, autenticidad y no repudio.
- Definir la vigencia durante la cual son válidas las llaves criptográficas fechas, periodo después del cual son desactivadas.
- En los casos en los que existan solicitudes de entes de control, organismos de seguridad del Estado u órdenes judiciales, la información cifrada puede ser puesta a disposición en forma no cifrada previa autorización de la Oficina de Riesgos y Líder de Procesos.
- Definir las directrices y herramientas de software que se utilizarán para implementar técnicas de cifrado de información en los desarrollos de software.
- Autorizar el uso de herramientas de cifrado en los desarrollos de software cuando han sido aprobados por estándares conocidos de la industria.
- Aprovisionar y entregar los equipos de cómputo portátiles con las correspondientes medidas de seguridad como son el cifrado de disco y guaya de seguridad cuando deban almacenar información calificada como clasificada o reservada, para dispositivos móviles se debe cifrar.

Normas dirigidas a: OFICINA DE RIESGOS

- Verificar que las normas sobre controles criptográficos se ejecuten y apliquen adecuadamente con frecuencia anual.

14. POLÍTICAS DE SEGURIDAD FISICA Y MEDIOAMBIENTAL

14.1 POLÍTICA DE AREAS SEGURAS

ICETEX provee la implantación y vela por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus sedes. Así mismo, controla las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

Se considera áreas restringidas las siguientes: Dirección de Tesorería, Oficina de Control Interno, centros de cómputo, centro de cableado, centro de monitoreo y vigilancia, Grupo de Archivo, Grupo de Contratos, Grupo de Recursos Físicos - Bodega.

Normas de áreas seguras

Normas dirigidas a: DIRECCION DE TECNOLOGIA

Aprobar las solicitudes de acceso al centro de cómputo o a los centros de cableado:

- Autorizar y gestionar el acompañamiento permanente de los visitantes a las áreas de procesamiento de información y centros de comunicaciones.
- Registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia, en una bitácora ubicada en la entrada de estos lugares de forma visible.
- Descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.
- Proveer las condiciones físicas y medioambientales necesarias para garantizar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo, que deben ser monitoreados de manera permanente.
- Propender en conjunto con la Coordinación de Recursos Físicos, porque las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del centro de cómputo y otras áreas de procesamiento de información.

Normas dirigidas a: VICEPRESIDENTES, DIRECTORES Y JEFES DE OFICINA QUE SE ENCUENTREN EN AREAS RESTRINGIDAS

- Velar mediante monitoreo por la efectividad de los controles de acceso físico y equipos de vigilancia implantados en su área.
- Autorizar los ingresos temporales a sus áreas, evaluando la pertinencia del ingreso; y definir los responsables del registro y supervisión de los ingresos autorizados a sus áreas.
- Velar porque las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a sus áreas solo sean utilizados por los funcionarios autorizados y, salvo situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran, estos no sean transferidos a otros funcionarios del Instituto.

Normas dirigidas a: SECRETARIA GENERAL – GRUPO DE RECURSOS FISICOS

- Proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones del ICETEX.

- Identificar mejoras a los mecanismos implantados y, de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones del Instituto.
- Almacenar y custodiar los registros del sistema de control de acceso a las instalaciones del ICETEX.
- Asegurar la efectividad de los mecanismos de seguridad física y control de acceso al centro de cómputo, centros de cableado y demás áreas de procesamiento de información o carga y despacho.
- Verificar que los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
- Controlar el acceso a las áreas de despacho y carga e implementar mecanismos que permitan la separación de éstas de las áreas de almacenamiento o procesamiento de información.
- El Grupo de Recursos Físicos debe verificar que el cableado se encuentra protegido con el fin de disminuir las intercepciones o daños.
- Asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

Normas dirigidas a: TODOS LOS USUARIOS (FUNCIONARIOS Y PERSONAL PROVISTO POR TERCERASPARTES)

- Los ingresos y egresos de personal a las instalaciones del ICETEX deben ser registrados; por consiguiente, todos los funcionarios, contratistas, proveedores, terceras partes y visitantes deben cumplir completamente con los controles físicos implantados.
- Portar el carné que los identifica en un lugar visible mientras se encuentren en las instalaciones del Instituto; en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.
- Aquellos funcionarios o personal provisto por terceras partes para los que aplique, debido al servicio prestado, deben utilizar prendas distintivas que faciliten su identificación además del carné de identificación de la compañía.
- No ingresar a áreas a las cuales no tengan autorización.

14.2 POLÍTICA DE SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES

ICETEX, para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica del Instituto que se encuentren dentro o fuera de sus instalaciones, provee los recursos que garantizan la mitigación de riesgos sobre dicha plataforma tecnológica.

Normas de seguridad para los equipos institucionales

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones del ICETEX.

- Generar y aplicar estándares de configuración segura para los equipos de cómputo de los funcionarios del Instituto.
- Establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos del Instituto y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.
- Aislar los equipos de la Dirección de Tesorería para proteger su acceso de los demás funcionarios de la red de la Entidad.

Normas dirigidas a: OFICINA DE RIESGOS

- Evaluar y analizar los informes de verificación de equipos de cómputo de las diferentes áreas del Instituto, en particular de las áreas restringidas.

Normas dirigidas a: SECRETARIA GENERAL – GRUPO DE RECURSOS FISICOS

- Revisar los accesos físicos en horas no hábiles a las áreas donde se procesa información.
- Restringir el acceso físico a los equipos de cómputo de áreas de procesamiento o almacenamiento de información o áreas que prestan servicios esenciales para el ICETEX.
- Velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones del ICETEX cuenten con la autorización documentada y aprobada previamente por el Coordinador de Recursos Físicos.
- Velar porque los equipos que se encuentran sujetos a traslados físicos fuera del Instituto posean pólizas de seguro.

Normas dirigidas a: TODOS LOS USUARIOS

- La Dirección de Tecnología es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos del Instituto.
- Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios y personal provisto por terceras partes deben acoger las instrucciones técnicas que proporcione la Dirección de Tecnología.
- Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico propiedad del ICETEX, el usuario responsable debe informar a la Mesa de Ayuda en donde se atenderá o escalará al interior de la Dirección de Tecnología, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.
- La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos del Instituto, solo puede ser realizado por los funcionarios de la Dirección de Tecnología, o personal de terceras partes autorizado por dicha dirección.
- Bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.
- Apagar las estaciones de trabajo u otros recursos tecnológicos en horas no laborables o cuando se deban ausentar por largos periodos de su puesto de trabajo.

- Los equipos de cómputo, en ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.
- Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.
- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos, calor excesivo, humedad o condiciones físicas que los puedan dañar (movimientos bruscos, impactos, peso, entre otros).
- En caso de pérdida o robo de un equipo de cómputo del ICETEX, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.
- Asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.
- No almacene documentos con información confidencial en la pantalla del escritorio.

15. POLITICAS DE SEGURIDAD EN LAS OPERACIONES

ICETEX vela por la protección de operaciones y el procesamiento de la información, ello incluye la gestión de capacidad, gestión de cambios, controles contra código malicioso, respaldo de la información, registro de eventos, protección de la información de registro, registro del administrador y operadores, sincronización de relojes, instalación de softwares en sistemas operativos, gestión de vulnerabilidades técnicas, restricción sobre la instalación de software y controles de auditorías de sistemas de información.

La seguridad en las operaciones se encuentra documentados y con las responsabilidades asignadas.

15.1 POLÍTICA DE ASIGNACIÓN DE RESPONSABILIDADES OPERATIVAS

La Dirección de Tecnología, encargada de la operación y administración de los recursos tecnológicos que apoyan los procesos del ICETEX, asigna funciones específicas a sus funcionarios, quienes deben efectuar la operación y administración de dichos recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades. Así mismo, vela por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la información manejada y asegura que los cambios efectuados sobre los recursos tecnológicos son adecuadamente controlados y debidamente autorizados.

La Dirección de Tecnología provee la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información del Instituto, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida.

La Dirección de Tecnología provee y ejecuta los controles de seguridad informática y ciberseguridad a fin de resguardar los servicios tecnológicos y la información.

Normas de asignación de responsabilidades operativas

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Elaborar y actualizar la documentación de procedimientos relacionados con la operación y administración de la plataforma tecnológica del Instituto a través de la Oficina de Planeación.
- Poner a disposición de sus funcionarios manuales de configuración y operación de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica del ICETEX de acuerdo con las funciones asignada al usuario.
- Proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de desarrollo y producción, la inexistencia de compiladores, editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.
- Realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados (capacity planning) de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.

Normas dirigidas a: OFICINA DE RIESGOS

- Emitir concepto y generar recomendaciones acerca de las soluciones de seguridad seleccionadas para herramientas colaborativas y sistemas de información del Instituto.

15.2 POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

El ICETEX proporciona los mecanismos necesarios que garantizan la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso y amenazas cibernéticas. Además, proporciona los mecanismos para generar cultura de seguridad entre sus funcionarios y personal provisto por terceras partes frente a los ataques de software malicioso.

Normas de protección frente a software malicioso

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- 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.

- 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.
- 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.
- Asegurar que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.
- Garantizar que el software de, antimalware y antispam, posea las últimas actualizaciones y parches de seguridad para evitar que sean explotadas ciertas vulnerabilidades.
- Normas dirigidas a: TODOS LOS USUARIOS
- No cambiar o eliminar la configuración del software de antimalware y antispam definida por la Dirección de Tecnología.
- 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.
- Ante sospechas o detección de alguna infección por software malicioso deben notificar a la Mesa de Ayuda, para que, a través de ella, la Dirección de Tecnología tome las medidas de control correspondientes.
- Evitar abrir correos de fuentes desconocidas, y publicidad engañosa.

15.3 POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN

La Dirección de Tecnología certifica la generación de copias de respaldo y almacenamiento de la información considerando las medidas de contingencia, seguridad y necesidades del negocio y proporciona los recursos necesarios, los procedimientos y mecanismos para la realización de estas actividades.

Así mismo, el Instituto vela porque los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo cuenta con los controles de seguridad física y medioambiental apropiados.

Los lineamientos de copias de respaldo están documentados, incluyen los requisitos de retención y protección.
Las copias de respaldo tienen un proceso de verificación de completitud, exactitud y restauración.

Normas de copias de respaldo de la información

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Proveer los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.
- Disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.
- Ejecutar los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.
- Definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.
- Definir en conjunto con la Oficina de Riesgos las estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.

Normas dirigidas a: VICEPRESIDENTES, DIRECTORES Y JEFES DE OFICINA

- Identificar las funciones críticas que contienen la información a ser respaldada y almacenada.

15.4 POLÍTICA DE REGISTRO DE EVENTOS Y MONITOREO DE LOS RECURSOS TECNOLÓGICOS Y LOS SISTEMAS DE INFORMACIÓN

ICETEX realiza monitoreo permanente del uso que dan los funcionarios y el personal provisto por terceras partes a los recursos de la plataforma tecnológica y los sistemas de información del Instituto. Además, vela por la custodia de los registros de auditoria cumpliendo con los períodos de retención establecidos para dichos registros.

El monitoreo contempla una definición de los registros de auditoria sobre los aplicativos donde se opera los procesos misionales del Instituto y análisis de los logs de auditoria para establecer posibles anomalías.

Los logs de los eventos generados por los componentes informáticos capturan y retiene con base en criticidad de los sistemas y el valor de los datos, aspecto relevante para la revisión periódica en beneficio de identificar posibles anomalías, generar alertas tempranas conducentes a reconstruir operaciones sensibles y tomar acciones en lo pertinente a la gestión de riesgos en la Entidad.

Los registros de auditoria requieren de condiciones de preservación similares a las establecidas para los datos y operaciones que los generan y ser consistentes con los criterios de respaldo y recuperación fundamentados en los requerimientos de retención de la información.

Los logs deben tener mecanismos de seguridad y control administrativo resistentes a ataques para evitar la adulteración de los mismos, también deben generar las capacidades suficientes

para detectar y grabar eventos significativos en aspectos de seguridad de información (control a través de un detector de intrusos para los archivos de configuración y Logs).

Normas de registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de información

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos a auditar establecidos.
- Velar por la integridad y disponibilidad de los registros de auditoria 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.
- Definir un usuario con privilegios únicamente para administración y control de los Logs, adicional dicho usuario debe realizar el correspondiente seguimiento y revisiones periódicas.
- Establecer los registros de auditoría en los recursos tecnológicos y los sistemas de información considerando los estándares de desarrollo seguro para registros de auditoría.

Normas dirigidas a: DIRECCION DE TECNOLOGIA Y OFICINA DE RIESGOS

- Determinar los períodos de retención de los registros (logs) de auditoria de los recursos tecnológicos y los sistemas de información del Instituto.
- Definir y ejecutar las tareas de revisión de logs de eventos.

Normas dirigidas a: DESARROLLADORES (INTERNOS Y EXTERNOS)

- Implementar en los desarrollos de software, los controles necesarios para generar y garantizar la integridad los registros (logs) de auditoría de las actividades realizadas por los usuarios finales y administradores en los sistemas de información desarrollados.
- 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.

Normas dirigidas a: ADMINISTRADORES DE SISTEMAS DE INFORMACIÓN E INFRAESTRUCTURA TECNOLÓGICA

- Los administradores de aplicaciones deben habilitar y generar logs de auditoría en las aplicaciones en la periodicidad establecida.
- Los administradores de sistemas operativos deben habilitar y generar en la periodicidad establecida los logs de auditoría del sistema operativo.
- 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 clasificada y reservada.
- 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).

- 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.
- El Coordinador de Infraestructura es responsable de recopilar y revisar los resultados de los reportes generados por los administradores de base de datos, aplicaciones, sistema operativo y consola de antivirus, correo electrónico con la finalidad de presentar al Sub-Comité de Logs propuestas de acciones y formular ajustes necesarios para la solución de las alarmas o incongruencias identificadas.
- Los administradores de sistemas de información e infraestructura tecnológica deben configurar el envío de log´s de auditoria generados al Correlacionador de Eventos para su revisión.

15.5 POLITICA DE CONTROL AL SOFTWARE OPERATIVO

ICETEX revisa la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de pruebas periódicas de vulnerabilidades, a fin de realizar la corrección sobre los hallazgos arrojados por dichas pruebas, de acuerdo con los criterios establecidos. La Dirección de Tecnología y la Oficina de Riesgos conforman el Comité de Vulnerabilidades encargado de revisar, valorar y gestionar las vulnerabilidades técnicas encontradas.

Normas de control al software operativo

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Establecer responsabilidades para controlar la instalación del software operativo, que interactúen con el procedimiento de control de cambios existente en el Instituto.
- Asegurar que el software operativo instalado en la plataforma tecnológica del ICETEX cuenta con soporte de los proveedores.
- Conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.
- Validar los riesgos que genera la migración hacia nuevas versiones del software operativo.
- Asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.
- Considerar los requisitos del negocio para la gestión de cambios sobre el software operacional.
- Establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo del Instituto.
- Mantener un inventario del software implementado, así como sus respectivas versiones y niveles de soporte por parte del proveedor.

15.6 POLÍTICA DE GESTIÓN DE VULNERABILIDADES

ICETEX revisa la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de pruebas periódicas de vulnerabilidades, a fin de realizar la corrección sobre los hallazgos arrojados por dichas pruebas, de acuerdo con los criterios establecidos. Estas dos áreas conforman en Comité de Vulnerabilidades encargado de revisar, valorar y gestionar las vulnerabilidades técnicas encontradas.

Normas para la gestión de vulnerabilidades

Normas dirigidas a: OFICINA DE RIESGOS

- Adelantar los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético, por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de las mismas.
- Generar los lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas de vulnerabilidades y hacking ético.

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Revisar y hacer seguimiento a la aparición de nuevas vulnerabilidades técnicas y reportar a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de que se evalúe las acciones necesarias para corregir las mismas de acuerdo con los criterios definidos en el procedimiento, de Pruebas de Vulnerabilidad.

Normas dirigidas a: DIRECCION DE TECNOLOGIA Y OFICINA DE RIESGOS

- Evaluar los resultados de las pruebas de vulnerabilidades y hacking ético y definir acciones para su resolución de hallazgos.
- Revisar las acciones ejecutadas para la resolución de vulnerabilidades técnicas y autorizar su cierre definitivo, en la Matriz de Vulnerabilidades.

15.7 POLÍTICA DE AUDITORIAS A SISTEMAS DE INFORMACIÓN

Las actividades de auditoria sobre los activos de información e infraestructura tecnológica se controlan para reducir el impacto sobre las operaciones del negocio y preservar la seguridad digital.

Estas actividades son planificadas y acordadas con la Dirección de Tecnología.

El acceso a sistemas de información y datos son acordados y controlados con el responsable del activo de información.

El alcance de las pruebas técnicas de auditoria se acuerda y controla con el responsable del activo de información.

El acceso diferente a solo lectura se autoriza para copias aisladas de los activos de información y se realiza borrado seguro una vez se ha finalizado la auditoria o en su defecto se establece protección apropiada en caso de necesidad de mantenerlos como documentación de prueba de auditoria.

Las pruebas de auditoria que puedan afectar disponibilidad en la prestación de servicios se realizan fuera de horas laborales.

Normas de política de auditorías a sistemas de información

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Brindar apoyo técnico al responsable de la auditoria para facilitar las actividades planificadas.
- A partir de los resultados de la auditoría gestiona los planes de mejoramiento.

15.8 POLÍTICA DE GESTIÓN DEL CAMBIO

ICETEX a través de la Dirección de Tecnología y la Oficina de Riesgos controla los cambios sobre sus activos de información, instalaciones y sistemas de procesamiento de información. Estas dos áreas conforman el Comité de Control de Cambios encargado de revisar, valorar y gestionar los cambios a través de un procedimiento que permite:

- Identificación y registro de los cambios.
- Planificación y prueba de los cambios.
- Valoración del impacto potencial de los cambios.
- Aprobación formal del cambio.
- Verificación de requisitos de seguridad del cambio y de continuidad.
- Comunicación del cambio a las partes pertinentes.
- Actividades de apoyo ante cambios no exitosos o de emergencia.

Normas de políticas de gestión del cambio

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Ejecutar las pruebas técnicas y validar que el solicitante realice las pruebas funcionales de los cambios a aprobar.
- Revisar antes de la ejecución del cambio que el mismo haya sido aprobado por el solicitante y el Comité de Control de Cambios.
- Catalogar y ejecutar el cambio gestionando los riesgos que puedan afectar la operación.
- Participar en la aprobación de los cambios propuestos al Comité de Control de Cambios.
- Participar en el seguimiento de los resultados de los cambios ejecutados.

Normas dirigidas a: OFICINA DE RIESGOS

- Participar en la evaluación y análisis de impacto del riesgo del cambio.
- Participar en la aprobación de los cambios propuestos al Comité de Control de Cambios.
- Participar en el seguimiento de los resultados de los cambios ejecutados.

16. POLÍTICAS DE SEGURIDAD EN LAS COMUNICACIONES

Las redes y servicios de comunicaciones, así como las instalaciones que le dan soporte se gestionan y controlan para evitar accesos no autorizados. La información transmitida o transferida mediante redes públicas se salvaguarda a través de controles para prevenir la pérdida de confidencialidad, integridad y la pérdida de disponibilidad de estos.

La conexión de equipo o estaciones de trabajo a las redes del Instituto está controlada y supervisada.

16.1 POLÍTICA DE GESTIÓN Y ASEGURAMIENTO DE LAS REDES DE DATOS

ICETEX establece los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, vela por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.
De igual manera, propende por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información clasificada y clasificada reservada del Instituto.

Normas de gestión y aseguramiento de las redes de datos

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red del ICETEX.
- Implantar controles para minimizar los riesgos de seguridad digital transportada por medio de las redes de datos.
- Identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando éstos se contraten externamente.
- Establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica del Instituto, acogiendo buenas prácticas de configuración segura.
- Identificar, justificar y documentar los servicios, protocolos y puertos permitidos por el Instituto en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.
- Instalar protección entre las redes internas del ICETEX y cualquier red externa, que este fuera de la capacidad de control y administración del Instituto.
- Definir los parámetros técnicos requeridos para la conexión segura de los servicios de red, así como las reglas de conexión de seguridad y controles para cifrado de información que circule sobre redes.

16.2 POLÍTICA DE USO DEL CORREO ELECTRÓNICO

ICETEX, teniendo en cuenta la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios y terceras partes, proporciona un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad, autenticidad y privacidad de quienes realizan las comunicaciones a través de este medio.

Normas de uso del correo electrónico

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Gestionar el acceso a las cuentas de correo electrónico Mediante el procedimiento de Asignación / Retiros de acceso a los sistemas de información
- Proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.
- Adoptar medidas de seguridad que permiten proteger la plataforma de correo electrónico contra código malicioso.
- Establecer mecanismos para el monitoreo y alertamiento de envío de información calificada como clasificada y clasificada reservada.
- Habilitar los controles que faciliten el etiquetado de la información digital en los servicios de correo electrónico.

Normas dirigidas a: OFICINA DE RIESGOS

- Generar las campañas para concientizar a los funcionarios y contratistas respecto al uso adecuado y las precauciones que deben adoptar en el intercambio de información calificada como clasifica y clasificada reservada por medio del correo electrónico.

Normas dirigidas a: TODOS LOS USUARIOS

- Usar la cuenta de correo electrónico de manera individual e intransferible y no usar la cuenta de correo electrónico de otro(s) usuarios
- Usar el servicio de correo, los mensajes y la información contenida en los correos para el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional del ICETEX. El correo institucional no debe ser utilizado para actividades personales.
- Los mensajes y la información contenida en los buzones de correo son propiedad del ICETEX y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- Está prohibido el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana, vayan en contravía de los derechos humanos y resulten ofensivos para los funcionarios del Instituto y contratistas .
- No es permitido en ninguna circunstancia el envío de archivos que contengan extensiones ejecutables o aquellos que puedan afectar sistemas de información o recursos internos o externos, Todos los mensajes enviados deben respetar el estándar de formato e imagen

corporativa definidos por el ICETEX y conservar en todos los casos el mensaje legal corporativo de confidencialidad.

- Todo correo sospechoso debe ser reportado a la Oficina de Riesgos y la Dirección de Tecnología.
- Los servicios colaborativos como One Drive, Sharepoint no podrán ser usados para almacenar información personal ni ser utilizados desde redes de Internet externas. Toda excepción es manejada considerando los riesgos y responsabilidades del área solicitante, siguiendo los respectivos procedimientos de solicitud y autorizaciones.
- Todo usuario que produzca, transmita o transfiera información, debe asegurar la adecuada clasificación de la misma y aplicar los parámetros de seguridad señalados por el instituto.

16.3 POLÍTICA DE USO ADECUADO DE INTERNET

ICETEX consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporciona los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en el Instituto.

Normas de uso adecuado de internet

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet.
- Diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
- Monitorear continuamente los canales del servicio de Internet manteniendo la calidad del servicio para los usuarios.
- Establecer los procedimientos e implementar controles para evitar la descarga de software no autorizado, código malicioso proveniente de Internet y el acceso a sitios catalogados como restringidos.
- Generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet, preservando el derecho fundamental a la intimidad.

Normas dirigidas a: OFICINA DE RIESGOS

- La Oficina de Riesgos debe generar campañas para concientizar tanto a los funcionarios internos, como al personal provisto por terceras partes, respecto a las precauciones que deben tener en cuenta cuando utilicen el servicio de Internet.

Normas dirigidas a: TODOS LOS USUARIOS

- Evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.
- Está prohibido por mandato legal, visitar páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que no esté relacionada con las labores asignadas.

- Hacer uso del mismo en relación con las actividades laborales que así lo requieran.
- Está prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Hotmail, Facebook, P2P, MSN, Yahoo, Skype, FTP, HTTP, Net2phone y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio del ICETEX.
- Está prohibido la descarga, uso, intercambio y/o instalación de juegos, música, películas, 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 y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo y la Dirección de Tecnología, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.
- Está prohibido el intercambio no autorizado de información de propiedad del ICETEX, de sus clientes, funcionarios y proveedores.

16.4 POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

ICETEX asegura la protección de la información transferida o transmitida con Entidades externas y procesos internos, tiene procedimientos y controles implementados para el intercambio de datos; cuenta con Acuerdos de Confidencialidad con terceras partes con quienes interactúen con la información.

La información recibida de terceras partes se conserva por un período de tiempo equivalente al de retención de las bases de datos con información personal sobre las cuales se efectúen actualizaciones, cambios, supresiones con la información fuente, o el tiempo establecido por los requisitos legales aplicables al Instituto.

Normas de intercambio de información

Normas dirigidas a: SECRETARIA GENERAL – GRUPO DE CONTRATOS

- El Grupo de Contratos, en acompañamiento con la Oficina de Riesgos, define los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre el Instituto y terceras partes incluyendo los compromisos y acciones por el incumplimiento de dichos acuerdos. Entre los aspectos se incluye la prohibición de divulgar la información entregada por el ICETEX a los terceros con quienes se establecen estos acuerdos y la destrucción de dicha información una vez cumpla su cometido.
- Establecer con terceras partes, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información de beneficiarios del Instituto que les ha sido entregada debido al cumplimiento de los objetivos misionales.

Normas dirigidas a: OFICINA DE RIESGOS

- Definir y establecer el procedimiento de intercambio de información con Entidades externas que hacen parte de la operación del ICETEX, reciben o envían información de los beneficiarios del Instituto, que contemple la utilización de medios de transmisión confiables y la adopción de controles, con el fin de proteger la confidencialidad e integridad de la misma.
- Velar porque la transmisión y transferencia de información del ICETEX con Entidades externas se realice en cumplimiento de las Políticas de seguridad.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

- Resguardar la información del ICETEX o de sus beneficiarios de divulgación no autorizada por parte de los terceros a quienes se entrega, verificando el cumplimiento de las cláusulas relacionadas en los contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos.
- Asegurar que los datos requeridos de los beneficiarios sólo puedan ser entregados a terceros, previo consentimiento de los titulares de los mismos, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.
- Los propietarios de los activos de información, o a quien ellos deleguen, verifican que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.
- Formular los requerimientos de solicitud/envío de información del ICETEX por/a terceras partes, salvo que se trate de solicitudes de entes de control o de cumplimiento de la legislación vigente.
- Asegurar que el Intercambio de información (digital) solamente se realice si se encuentra autorizada y dando cumplimiento a las Políticas de administración de redes, de acceso lógico y de protección de datos personales del ICETEX, así como del procedimiento de intercambio de información con Terceros.
- Verificar conjuntamente entre el proveedor y el propietario la ejecución de la disposición final de la información suministrada a los terceros, una vez esta ha cumplido el cometido por el cual compartida.

Normas dirigidas a: SECRETARIA GENERAL – COORDINACION DE CORRESPONDENCIA

- Operar el procedimiento para el intercambio, de información (medios de almacenamiento y documentos) con terceras partes y la adopción de controles a fin de proteger la información sensible contra divulgación, pérdida o modificaciones.
- Garantizar que todo envío de información física a terceros (documento o medio magnético) utilice únicamente los servicios de transporte o mensajería autorizados por el Instituto, y que estos permitan ejecutar rastreo y control de las entregas.

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Ofrecer servicios y herramientas, para el cifrado de información calificada como pública clasificada o pública reservada, para evitar la divulgación o modificaciones no autorizadas.

Normas dirigidas a: TERCEROS CON QUIENES SE INTERCAMBIA INFORMACION DEL ICETEX

- Dar manejo adecuado a la información recibida, y utilizarla en el marco de los servicios contratados sin extralimitarse a ellos, en cumplimiento de las Políticas de seguridad del Instituto.
- Realizar la disposición final segura la información suministrada, una vez esta cumpla con la función para la cual fue enviada y demostrar mediante acta la realización de las actividades de destrucción.

Normas dirigidas a: TODOS LOS USUARIOS

- No está permitido el intercambio de información clasificada y clasificada reservada del Instituto por vía telefónica.

17. POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

La adquisición, desarrollo y mantenimiento de sistemas de información incluye buenas prácticas de seguridad digital durante todo el ciclo de vida, los requisitos relacionados con la seguridad digital son incorporados a los sistemas de información tanto nuevos como ya existentes. Los servicios asociados a transacciones electrónicas se protegen para evitar transmisión incompleta, alteración o divulgación no autorizada o enrutamiento errado.

17.1 POLÍTICA PARA EL ESTABLECIMIENTO DE REQUISITOS DE SEGURIDAD

ICETEX asegura que el software adquirido y desarrollado tanto al interior del Instituto, como por terceras partes, cumpla con los requisitos de seguridad y calidad establecidos. Las áreas propietarias de sistemas de información, la Dirección de Tecnología y la Oficina de Riesgos incluyen requisitos de seguridad en la definición de requerimientos y, posteriormente se aseguran de que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido. Todos los sistemas de información o desarrollos de software deben tener un área propietaria dentro del Instituto formalmente asignada.

Normas para el establecimiento de requisitos de seguridad

Normas dirigidas a: PROPIETARIOS DE LOS SISTEMAS DE INFORMACIÓN, DIRECCION DE TECNOLOGIA Y OFICINA DE RIESGOS

- Establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad digital.
- La Dirección de Tecnología lidera la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.

Normas dirigidas a: DESARROLLADORES (INTERNOS O EXTERNOS)

- Documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.
- Certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas.
- Certificar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros.

17.2 POLÍTICA DE DESARROLLO SEGURO, REALIZACION DE PRUEBAS Y SOPORTE DE LOS SISTEMAS

ICETEX vela porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad definidos basado en buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad.
Se asegura que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido.
Todo sistema de información que capture información de los clientes incorpora mecanismo de autorización de tratamiento de datos personales.

Normas de desarrollo seguro, realización de pruebas y soporte de los sistemas

Normas dirigidas a: PROPIETARIOS DE LOS SISTEMAS DE INFORMACIÓN

- Realizar las pruebas para asegurar que se cumplen con los requerimientos de seguridad establecidos en ambientes de pruebas y producción, utilizando metodologías establecidas para este fin, documentando las pruebas realizadas y aprobando los pasos a producción, considerando nuevos sistemas, nuevas funcionalidades, mantenimientos en aplicaciones construidas internamente, construidas por proveedores, aprovisionadas en la nube o híbrido de las anteriores.
- Aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos, cambios, o nuevas funcionalidades.

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- Implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.
- Contar con sistemas de control de versiones para administrar los cambios de los sistemas de información del ICETEX.
- Asegurar que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

- Generar, adoptar o recomendar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.
- Asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión estable publicada por el fabricante.
- Asegurar que las aplicaciones y desarrollos se diseñen y construyan en versiones vigentes y estables emitidas por el fabricante respecto a las herramientas, componentes, lenguajes de programación.
- Almacenar las copias de seguridad del código fuente de manera segura previendo riesgos asociados a pérdida de disponibilidad, confidencialidad o integridad.
- Aplicar el procedimiento de control de cambios a los cambios para el software aplicativo y los sistemas de información del Instituto.

Normas dirigidas a: DESARROLLADORES (INTERNOS O EXTERNOS)

- Considerar y aplicar las buenas prácticas y lineamientos de desarrollo seguro durante todo el ciclo de vida de los mismos sistemas de información.
- Proporcionar un nivel adecuado y oportuno de soporte para solucionar los problemas que se presenten en el software aplicativo del ICETEX.
- Construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.
- Asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla.

Normas dirigidas a: OFICINA DE RIESGOS

- Realizar pruebas de seguridad sobre los sistemas de información de acuerdo con los estándares de la industria.

17.3 POLÍTICA PARA LA PROTECCION DE LOS DATOS DE PRUEBA

ICETEX protege los datos de prueba que se entregan a los desarrolladores, asegurando que no revelan información calificada como clasificada y reservada de los ambientes de producción.

Normas para la protección de los datos de prueba

Normas dirigidas a: DIRECCION DE TECNOLOGIA

- 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.

- Realizar la adecuada disposición final la información de los ambientes de pruebas, una vez éstas han concluido las mismas.

18. POLÍTICAS DE RELACION CON TERCERAS PARTES

ICETEX establece mecanismos de control en sus relaciones con terceras partes, con el objetivo de asegurar que la información a la que tengan acceso, conocimiento o relación con los servicios o productos en el marco del contrato cumpla con las políticas, normas y procedimientos de seguridad digital.

Normas de inclusión de condiciones de seguridad en la relación con terceras partes

Normas dirigidas a: DIRECCION DE TECNOLOGIA, OFICINA ASESORA JURIDICA Y OFICINA DE RIESGOS

- Elaborar el modelo de Acuerdo de Confidencialidad y de Intercambio de Información con terceras partes. De dichos acuerdos deberá derivarse una responsabilidad tanto civil como penal para la tercera parte contratada.
- Generar un modelo base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad Digital, con los que deben cumplir los proveedores de servicios; dicho modelo, debe ser divulgado a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos.

Normas dirigidas a: DIRECCIÓN DE TECNOLOGIA

- Establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos del Instituto.
- Establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.
- Gestionar los riesgos relacionados con terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica del ICETEX.
- Verificar el cumplimiento de los controles de software base instalado y de licenciamiento de software y hacer extensivos los controles existentes en la red a equipos de cómputo de terceras partes cuando los proveedores que por necesidades o por acuerdos contractuales de la operación, incorporen equipos de cómputo a la red corporativa.

Normas dirigidas a: OFICINA DE RIESGOS

- Evaluar y emitir concepto de los accesos a la información y de los recursos tecnológicos del Instituto requeridos por terceras partes.
- Asesorar en la identificación de los riesgos relacionados con terceras partes.,
- Revisar el cumplimiento normativo de seguridad digital en los proveedores.

Normas dirigidas a: SUPERVISORES DE CONTRATOS CON TERCEROS

- Incluir en los contratos el cumplimiento de las normas legales y políticas pertinente al servicio contratado.
- Divulgar a sus proveedores las políticas, normas y procedimientos de seguridad digital de acuerdo con el servicio contratado.
- Asignar permisos al proveedor en los sistemas de información y recursos tecnológicos de acuerdo con las responsabilidades contractuales.
- Verificar el adecuado uso de los recursos tecnológicos y de la información suministradas al proveedor para el desarrollo de las obligaciones del contrato.
- Hacer seguimiento del cumplimiento de las normas legales, políticas, procedimientos y requisitos específicos de seguridad digital por parte del proveedor y reportar su resultado a la Oficina de Riesgos.
- Con respecto a seguridad digital, los funcionarios y personal provisto por terceras partes que por sus funciones hagan uso de la información del ICETEX, deben dar cumplimiento a las políticas, normas y procedimientos y recibir la sensibilización o capacitación que determine el Instituto en materia de seguridad digital.

18.1 POLÍTICA DE GESTION DE LA PRESTACION DE SERVICIOS DE TERCERAS PARTES

ICETEX propende por mantener los niveles acordados de seguridad digital y de prestación de los servicios de los proveedores, en concordancia con los acuerdos establecidos con éstos. Así mismo, vela por la adecuada gestión de cambios en la prestación de servicios de dichos proveedores.

Normas de gestión de la prestación de servicios de terceras partes

Normas dirigidas a: DIRECCION DE TECNOLOGIA Y OFICINA DE RIESGOS

- Verificar las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

Normas dirigidas a: OFICINA DE RIESGOS Y SUPERVISORES DE CONTRATOS CON TERCEROS

- Notificar a los proveedores que todos los cambios en los servicios tecnológicos deben ser informados a su correspondiente Supervisor, para que dichos cambios se analicen en Comité de Control de Cambios.

18.2 POLÍTICA DE CADENA DE SUMINISTRO

ICETEX realiza revisión de seguridad digital a la cadena de suministro de los proveedores que participan en la operación misional del Instituto.
Define los requisitos de seguridad digital de la operación realizadas con terceras partes en lo referente a la adquisición de productos y servicios.
Exige la divulgación de los requisitos de seguridad a los proveedores a lo largo de la cadena de suministro que éste tenga y a sus colaboradores.

Se tiene formalizado mediante procedimiento la revisión periódica de los requisitos de seguridad de la cadena de suministro. Dentro de la revisión se contempla los componentes de hardware y software crítico para el desarrollo del servicio.

Normas de política de cadena de suministro

Normas dirigidas a: DIRECCIÓN DE TECNOLOGÍA

- Identificar con el proveedor los componentes de hardware y software crítico para el desarrollo del servicio.

Normas dirigidas a: OFICINA DE RIESGOS Y SUPERVISORES DE CONTRATOS

- Revisar los requisitos de seguridad de la cadena de suministro de proveedores que participan en la operación misional.
- Revisar el cumplimiento de la divulgación de los requisitos de seguridad de la cadena de suministro de proveedores.

19. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD

ICETEX asegura la gestión de incidentes de seguridad digital incluyendo la comunicación interna y autoridades competentes de ser necesario.
Se tienen definidas las responsabilidades a través de procedimientos de gestión de incidentes para asegurar una respuesta eficaz y oportuna.

19.1 POLÍTICA PARA EL REPORTE Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD

ICETEX promueve entre los funcionarios y contratistas el reporte de incidentes de seguridad digital en sus medios de procesamiento, medio de almacenamiento, la plataforma tecnológica, los sistemas de información y las personas.

De igual manera, asigna responsables para el tratamiento de los incidentes de seguridad digital, quienes tienen la responsabilidad aislar, investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad. Los responsables con sus respectivas actividades están establecidos en el Procedimiento de Incidentes y en la Guía para el manejo de posible delito informático.

La Alta Dirección o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante Entidades externas.

Normas para el reporte y tratamiento de incidentes de seguridad

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Informar a la Oficina de Riesgos, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

Normas dirigidas a: OFICINA DE RIESGOS

- Evaluar todos los incidentes de seguridad de acuerdo con sus circunstancias particulares y escala al Comité de Seguridad digital aquellos en los que se considere pertinente.
- Designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su re-ocurrencia.
- Generar campañas de concientización a todos los usuarios del Icetex para que conozcan los mecanismos para el reporte de incidentes de seguridad.
- Activar el plan de contingencia tecnológica, de acuerdo con los criterios del Manual del Plan de continuidad del negocio del Instituto para aquellos incidentes que afecten la disponibilidad y/o integridad de información y de los servicios tecnológicos.

Normas dirigidas a: DIRECCIÓN DE TECNOLOGÍA

- Analizar el incidente con el fin de establecer las posibles causas del mismo, identifica el impacto y ejecuta las acciones para contener el incidente.
- Proponer los planes de mejora e implementar medidas correctivas.

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACION

- Analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

Normas dirigidas a: TODOS LOS USUARIOS

- Reportan a la Oficina de Riesgos cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos, para que se registre y se le dé el trámite necesario.

20. POLÍTICAS DE INCLUSIÓN DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

ICETEX incorpora las medidas de seguridad digital en sus procesos de gestión de incidentes de continuidad, protegiendo la información del Instituto.

20.1 POLÍTICA DE CONTINUIDAD, CONTINGENCIA, RECUPERACIÓN Y RETORNO A LA NORMALIDAD CON CONSIDERACIONES DE SEGURIDAD DIGITAL

ICETEX responde ante eventos de contingencia conforme a los escenarios identificados en el Manual de Administración de Plan de Continuidad de Negocio y proporciona los recursos suficientes para dar una respuesta efectiva y así continuar la operación de procesos críticos, preservando los niveles de seguridad equivalente a los proporcionados en situación normal.

ICETEX mantiene canales de comunicación adecuados hacia funcionarios, proveedores y partes interesadas ante un incidente de continuidad.
Normas de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad digital

Normas de política de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad digital

Normas dirigidas a: COMITE SARO-SARLAFT Y OFICINA DE RIESGOS

- Reconocer los escenarios que son identificadas como emergencia o desastre para el Instituto, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.
- Liderar los aspectos relacionados con la continuidad del negocio y la recuperación ante desastres
- La Oficina de Riesgos realiza el análisis de impacto al negocio y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad digital a que haya lugar.
- El Comité SARO-SARLAFT, junto con la Oficina de Riesgos, asegura la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad digital durante su realización y la documentación de dichas pruebas.

Normas dirigidas a: DIRECCION DE TECNOLOGIA Y OFICINA DE RIESGOS

- Asegurar un plan de recuperación ante desastres para la infraestructura tecnológica 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.
- Participar activamente en las pruebas de los procedimientos de contingencia y notifica los resultados al Comité SARO-SARLAFT.

20.2 POLÍTICA DE REDUNDANCIA

ICETEX propende por la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para el Instituto.

Normas de redundancia

Normas dirigidas a: DIRECCION DE TECNOLOGIA Y OFICINA DE RIESGOS

- Analizar y establecer los requerimientos de redundancia para los sistemas de información que se usan en los procesos críticos y la plataforma tecnológica.
- Realizar pruebas sobre las soluciones de redundancia, para asegurar el cumplimiento de los requerimientos de disponibilidad.
- La Dirección de Tecnología selecciona de las soluciones de redundancia tecnológica sobre los sistemas de información de acuerdo con las necesidades del negocio.

- La Dirección de Tecnología administra las soluciones de redundancia tecnológica del Instituto.

21. POLÍTICAS DE CUMPLIMIENTO

ICETEX vela por la identificación, documentación y cumplimiento de las obligaciones legales estatutarias, de reglamentación y contractuales relacionadas con la seguridad digital, como son: derechos de propiedad intelectual y el uso de software patentado, privacidad y protección de datos personales, transparencia y acceso a la información, requerimientos mínimos de seguridad, calidad y ciberseguridad para Entidades vigilados por la Superintendencia Financiera de Colombia y el marco de seguridad digital emitido por el Ministerio de las Tecnologías y las Comunicaciones – MinTic.

Se realiza la verificación de cumplimiento normativo con el fin de identificar posibles falencias de seguridad y optimizar o implementar controles aplicables a la operación, aspecto que es extendido para los proveedores de procesos misionales.

El cumplimiento normativo es informado a la Alta Dirección con el fin de dar a conocer su estado y para que orienten la asignación de recursos para la implementación de controles.

21.1 POLÍTICA DE CUMPLIMIENTO DE DERECHO DE PROPIEDAD INTELECTUAL Y USO DE SOFTWARE PATENTADO

ICETEX propende porque el software instalado y en uso en los recursos de la plataforma tecnológica del Instituto cumpla con los requerimientos legales y de licenciamiento aplicables.

En el procedimiento de Inventario de software y hardware y control de software legal se cumple con los requisitos legislativos relacionados con los derechos de propiedad intelectual y uso de software patentados.

Normas de cumplimiento con requisitos legales y contractuales

Normas dirigidas a: SECRETARIA GENERAL - GRUPO DE CONTRATOS

- Los contratos deben Incluir una cláusula donde el proveedor garantiza que tiene las patentes o derechos de propiedad sobre el bien o servicio adquirido o contratado por la Entidad.
- Se deben desarrollar cláusulas de indemnidad con el propósito de asegurar que el proveedor defienda a la Entidad en sus derechos ante reclamos sobre infracciones sobre patentes (hardware) o derechos de autor (software). En el supuesto que se compruebe una infracción, deberá asegurarse una solución que no afecte los servicios del Icetex y la definición de los cargos por daños y perjuicios.
- En los contratos con proveedores de desarrollo se debe aclarar los derechos de explotación y propiedad de los desarrollos enumerando los derechos de explotación cedidos:

reproducción, distribución, comunicación pública y transformación sobre el resultado del desarrollo a favor de la Entidad.

Normas dirigidas a: DIRECCIÓN DE TECNOLOGIA

- Asegurar que todo el software que se ejecuta en el Instituto cumpla con los requisitos de derechos de autor y licenciamiento de uso
- Mantener un inventario con el 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 verifica periódicamente que el software instalado corresponda únicamente al permitido. Este inventario debe contener la evidencia de la propiedad de las licencias.
- Definir controles que garanticen la continuidad en el uso del software bajo el riesgo de desaparición del proveedor.
- Establecer la reserva de los derechos de propiedad intelectual, donde se plasme de forma expresa la reserva de todos los derechos existentes sobre el sitio web institucional.
- Para las aplicaciones Web de la Entidad que son ejecutadas de forma remota por los usuarios, no siendo necesaria la descarga o instalación de software alguno 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 la misma.
- Definir e implementar mecanismos que impidan la instalación de software no autorizado por parte de los usuarios finales.
- Vigilar el software instalado por usuarios privilegiados como administradores de los equipos de cómputo y servidores.

Normas dirigidas a: OFICINA DE RIESGOS

- Emitir concepto de seguridad sobre los sistemas de información de libre distribución con la intención de ser utilizados en el Instituto, basados en las especificaciones técnicas del producto y sus debilidades reconocidas en el mercado.
- Sensibilizar a los funcionarios y contratistas en la instalación y uso de software legal para proteger los derechos de propiedad intelectual y sus acciones disciplinarias en caso de incumplir la normativa.

Normas dirigidas a: TODOS LOS USUARIOS

- Está prohibido instalar software o sistemas de información en sus estaciones de trabajo o equipos móviles suministrados para el desarrollo de sus actividades.
- Cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software.

21.2 POLÍTICA DE PRIVACIDAD Y PROTECCION DE DATOS PERSONALES

En cumplimiento de la Ley 1581 de 2012, el ICETEX propende por la protección de los datos personales de sus beneficiarios, deudores solidarios, funcionarios, contratistas y demás terceros de los cuales reciba y administre información.

Se adoptan las medidas administrativas, técnicas y de procesos para resguardar la privacidad y proteger los datos durante la captura, almacenamiento y procesamiento en las operaciones.

Se establecen las políticas de protección de datos personales de acuerdo con los lineamientos de la ley y se encuentran documentadas en la Política de Tratamiento de Datos Personales, disponible en el sitio web institucional.

Normas de privacidad y protección de datos personales de beneficiarios, funcionarios, proveedores y otras partes

Normas dirigidas a: AREAS QUE PROCESAN DATOS PERSONALES

- Obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades del Instituto.
- Asegurar que solo aquellas personas que por sus funciones pueden tener acceso a dichos datos.
- Establecer condiciones contractuales y de seguridad a las Entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.
- Acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.
- Acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.

Normas dirigidas a: OFICINA DE RIESGOS

- Apoyar en la formulación de controles para el tratamiento y protección de los datos personales de los beneficiarios, funcionarios, proveedores y demás terceros del ICETEX de los cuales reciba y administre información.
- Mantener la política de tratamiento de datos personales y sus finalidades relacionadas en la autorización de datos personales vigente, actualizada y alineada con los requisitos legales vigentes.
- Asesorar en la identificación de riesgos relacionados con la privacidad y protección de datos personales a las áreas de ICETEX.
- Identificar y reportar incidentes referentes a la protección de datos personales a la Superintendencia de Industria y Comercio.
- Capacitar y sensibilizar en los lineamientos de la ley de protección de datos personales al personal de ICETEX, y coordinar la divulgación de estos lineamientos a los proveedores y terceras partes interesadas.

Normas dirigidas a: DIRECCIÓN DE TECNOLOGIA

- Implantar los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, proveedores u otras terceras partes y ejecuta los controles sobre el almacenamiento de las bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.
- Custodiar la base de datos de autorización de datos personales.

Normas dirigidas a: TODOS LOS USUARIOS

- Guardar la discreción correspondiente, o la reserva absoluta con respecto a la información del Instituto o de los beneficiarios, deudores solidarios, funcionarios y proveedores de cual tengan conocimiento en el ejercicio de sus funciones.
- Aplicar los controles de seguridad definidos por el Instituto para el suministro de información de beneficiarios, funcionarios, contratistas o proveedores.

21.3 POLÍTICA DE CUMPLIMIENTO DE LEY DE TRANSPARENCIA

ICETEX garantiza el derecho de acceso a la información pública a través de los canales habilitados por el Instituto excluyendo solo aquella que está sujeta a las excepciones constitucionales, legales y bajo el cumplimiento de los requisitos establecidos en Ley 1712 de Transparencia.

Normas de cumplimiento de la Ley de Transparencia

Normas dirigidas a: OFICINA DE RIESGOS

- Generar los Instrumentos de Gestión y tramitar su publicación.

Normas dirigidas a: VICEPRESIDENTES, JEFES DE OFICINA Y DIRECTORES

- Actualizar periódicamente la información pública bajo su responsabilidad a través de los procedimientos establecidos en la Entidad.
- La Oficina de Comercial y Mercadeo atiende las solicitudes de acceso a la información pública.

22. POLÍTICA DE SERVICIOS DE COMPUTACIÓN EN LA NUBE

ICETEX propende por mantener la seguridad de los activos de información del Instituto cuando se autoriza el uso de servicios de computación en la nube a fin de garantizar la disponibilidad, privacidad, confidencialidad, integridad y cumplimiento de los requisitos legales en materia de protección de información personal.

Esta política se aplica a los servicios de computación en nube que sean utilizados o contratados por el ICETEX, así como a los procesos que hagan uso de dichos servicios.

La utilización de servicios de computación en la nube con licenciamiento de carácter gratuito o abierto debe ser aprobada por el Comité de Control de Cambios, quienes contemplarán la estrategia de Gobierno Digital.

En los contratos celebrados con proveedores de servicios de computación en la nube se debe incluir la necesidad de cumplir las políticas de seguridad digital, el cumplimiento de los acuerdos de niveles de servicio, responsabilidades legales y derechos de propiedad intelectual sobre la información, leyes y regulaciones sobre la protección de la información de la Entidad e información de carácter personal.

El uso de plataformas internacionales de almacenamiento o procesamiento en la nube para datos de carácter personal deben contar con la autorización del titular de los datos. No se debe almacenar datos personales en servicios de computación en la nube sin la autorización del titular para la transmisión internacional de datos.

Normas de la Política de Servicios de Computación en la Nube

Normas dirigidas a: OFICINA DE RIESGOS

- Realizar la identificación, valoración y evaluación de los riesgos asociados al uso de servicios de computación en la nube en conjunto con la Dirección de Tecnología.
- Emitir y/o evaluar controles para mitigar los riesgos de seguridad digital cuando se autorice el uso de servicios de computación en la nube para el tratamiento de información institucional, almacenamiento de información personal, protección de secretos comerciales, riesgos legales, técnicos, de continuidad y asociados a la transmisión transfronteriza de información institucional o personal.

Normas dirigidas a: DIRECCIÓN DE TECNOLOGIA

- Participar en la identificación y tratamiento de riesgos de seguridad digital asociados al uso de computación en la nube.
- Proveer servicios de copia de respaldo para la información del ICETEX que está autorizada para almacenamiento en computación en la nube.
- Implementar controles de seguridad digital para preservar los accesos a los servicios de computación en la nube autorizados por el Instituto.
- Definir e implementar plan de contingencia para preservar la información almacenada en servicios de computación en la nube.
- Mantener inventario de los servicios de computación en la nube autorizados para uso dentro de las redes corporativas.
- Mantener inventario de los usuarios a los que se les autoriza el uso de servicios de computación en la nube.
- Realizar monitoreo de seguridad digital utilizando las tecnologías de correlación aprovisionadas por el Instituto.
- Asegurar que todo servicio de computación en la nube se diseñe, implemente y opere conforme a las políticas de seguridad digital y gestión de riesgo institucional.

Normas dirigidas a: SUPERVISORES DE CONTRATO, VICEPRESIDENTES, DIRECTORES Y JEFES DE OFICINA

- Asegurar la existencia de Acuerdos y/o Cláusulas de Confidencialidad con proveedores de servicios de computación en la nube.
- Especificar responsabilidades sobre el uso de servicios de computación en la nube (almacenamiento y/o procesamiento) del personal a su cargo.
- Asegurar en contratos que los proveedores disponen capacidades para demostrar que los servicios ofrecidos cuentan con certificación en ciberseguridad emitida por ente independiente al prestador de servicios.
- Incluir el derecho de auditoría independiente al cumplimiento de seguridad y requisitos legales aplicables al Instituto.

Normas dirigidas a: TODOS LOS USUARIOS

- Cuando se use almacenamiento en la nube, toda información calificada como publica clasificada o publica reservada y toda información de carácter personal esta debe permanecer cifrada de acuerdo con las políticas de cifrado institucional, para evitar su divulgación o acceso no autorizadas.
- Solicitar ante la Dirección de Tecnología la autorización de uso de servicios de computación en la nube, teniendo en cuenta para ello el uso de Guía para la evaluación de necesidades de herramientas de software.
- Utilizar los servicios de computación en nube autorizados, únicamente para el cumplimiento de las labores asignadas institucionalmente.
- Evitar el uso de servicios de computación en la nube desde equipos de cómputo de uso compartido inseguros como café internet o centros de alquiler de equipos públicos.
- No almacenar información sujeta a derechos de autor (videos, imágenes, audio, libros, entre otros) en las cuentas de servicios de computación en la nube autorizadas para el ICETEX.

23. POLITICA DE CIBERSEGURIDAD

ICETEX protege y asegura los datos, sistemas y aplicaciones, provenientes y los que viajan, en el ciberespacio que son esenciales para la operación de la Entidad, para prevenir, mitigar y disminuir los impactos negativos potenciales de amenazas o ataques cibernéticos mediante los controles tecnológicos, las políticas de seguridad digital, los procedimientos y el trabajo conjunto con Entidades de apoyo en ciberseguridad y ciberdefensa.

La gestión de ciberseguridad contempla las etapas de prevención, protección y detección, respuesta y comunicación, recuperación y aprendizaje, las cuales están enfocadas a la adecuada administración de riesgos de ciberseguridad y al mejoramiento continuo de la seguridad digital.

Principios de Ciberseguridad

- Prevención: La gestión de la ciberseguridad es preventiva, para lo cual implementa controles adecuados para velar por la gestión de la ciberseguridad a través de un análisis de riesgos de sus activos de información. La función de prevención admite la capacidad de limitar o contener el impacto de un posible incidente de ciberseguridad.
- Protección y detección: ICETEX implementa actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad.
- Respuesta: Aún con las medidas de seguridad adoptadas, ICETEX desarrolla e implementa actividades para mitigar los incidentes relacionados con ciberseguridad y los comunica a los entes competentes.
- Recuperación: Se desarrolla e implementa actividades apropiadas para restaurar cualquier servicio que se haya deteriorado debido a un incidente de ciberseguridad, así como se busca un aprendizaje del mismo a través de un análisis de causa raíz del riesgo.

Lineamientos

- La gestión de la ciberseguridad debe alinearse con la gestión de las TIC y las estrategias de negocio.
- Los roles y responsabilidades asociadas a la gestión de la ciberseguridad deben estar claramente definidas y aceptadas por los diferentes responsables.
- los resultados de la gestión de ciberseguridad se deben comunicar a todas las partes interesadas pertinentes incluida la organización interna, organismos de control y terceras partes involucradas.
- La gestión de la ciberseguridad de contribuir a mantener la continuidad de las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para el instituto ante el evento de una interrupción significativa.
- Los procesos de recuperación ante incidentes de seguridad digital deben ser mejorados continuamente mediante las lecciones aprendidas.

Procedimientos

Los procedimientos que apoyan la Gestión de Ciberseguridad son:

- Gestionar riesgos de seguridad de la información.
- Guía metodológica de gestión de riesgos de seguridad de la información.
- Procedimiento para reportar y gestionar incidentes de seguridad de la información.
- Manual de Plan de Continuidad del Negocio.

Normas de la Política de Ciberseguridad

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA NFORMACIÓN

❖ Actualizar y presentar ante la Junta Directiva las políticas y gestión de ciberseguridad

- Analizar los incidentes de ciberseguridad que le son escalados y activar el procedimiento de contacto con las autoridades y grupos de interés especial, cuando lo estime necesario.

Normas dirigidas a: OFICINA DE RIESGOS

- Elaborar y proponer las políticas de ciberseguridad.
- La ciberseguridad se apoya en los procedimientos de gestión de riesgos e incidentes de seguridad digital, así como del Manual de Plan de Administración de Continuidad del Negocio.
- Monitorear y verificar del cumplimiento de las políticas y procedimientos en materia de ciberseguridad.
- Mediante la ejecución de un programa de capacitación y sensibilización en materia de seguridad digital ICETEX, prepara regularmente a sus funcionarios y contratistas en temas relacionados con ciberseguridad para mantenerlos actualizados sobre las nuevas ciberamenazas, las políticas de seguridad, los controles, procedimientos y acciones a seguir en caso de incidentes de seguridad digital.
- Mantener actualizado al personal responsable de los riesgos de ciberseguridad para que se mantenga a la vanguardia de las nuevas modalidades de ciberataques que pudieran llegar a afectar a la Entidad.
- Identificar, y en la medida de lo posible, medir, los riesgos cibernéticos emergentes que puedan llegar a afectar a la Entidad y establecer controles para su mitigación.
- Gestionar los riesgos de ciberseguridad que puedan constituir riesgo cibernético.
- Proponer los controles para mitigar los riesgos que pudieran afectar la seguridad digital.
- Reportar a la Junta Directiva y a al Comité de Seguridad digital, los resultados de las gestiones adelantadas para el tratamiento de los riesgos de ciberseguridad,
- Sugerir anualmente los proyectos y/o presupuestos en materia de seguridad digital.
- Establecer la estrategia de comunicación ante incidentes de ciberseguridad a los Entes de Control.
- Proponer ajustes sus sistemas de gestión de riesgo, de seguridad digital y controles de seguridad como consecuencia de los incidentes presentados.
- Establecer y gestionar los indicadores de la seguridad digital.
- Suministrar los lineamientos para el cumplimiento de obligaciones de terceras partes.
- Informar a los consumidores financieros de la Entidad sobre las medidas de seguridad y recomendaciones que deberán adoptar para su ciberseguridad

Normas dirigidas a: DIRECCIÓN DE TECNOLOGÍA

- Implementar, operar y mantener controles para mitigar los riesgos que pudieran afectar la seguridad digital.
- Gestionar la ciberseguridad en los proyectos que impliquen la adopción de nuevas tecnologías.
- Gestionar y documentar la seguridad de la plataforma tecnológica.
- 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.

- Adoptar los mecanismos necesarios para recuperar los sistemas de información al estado en que se encontraban antes del ataque cibernético.
- Mantener actualizadas y en operación las herramientas y/o servicios que permitan hacer correlación de eventos que puedan alertar sobre incidentes de seguridad.
- 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.
- 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.
- Gestionar las vulnerabilidades de aquellas plataformas que soporten los procesos críticos y que estén expuestos en el ciberespacio.
- Monitorear continuamente la plataforma tecnológica con el propósito de identificar comportamientos inusuales que puedan evidenciar ciberataques contra la Entidad.
- Aplicar el procedimiento de gestión de incidentes cuando se presenten incidentes de seguridad digital, identificando los dispositivos que pudieran haber resultado afectados.
- Preservar cuando sea factible, las evidencias digitales para que las autoridades puedan realizar las investigaciones correspondientes.

Normas dirigidas a: SECRETARIA GENERAL - GRUPO DE CONTRATOS

- Incluir en los contratos que se celebren con terceros que harán parte de los procesos operativos, las medidas y obligaciones pertinentes para la adopción y el cumplimiento de políticas para la gestión de los riesgos de seguridad digital.

Normas dirigidas a: SUPERVISORES DE CONTRATOS CON TERCEROS

- Verificar el cumplimiento de las obligaciones y medidas establecidas para la adopción y el cumplimiento de políticas de seguridad digital.

24. POLÍTICA PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD DIGITAL

ICETEX brinda el marco de gestión de riesgos de seguridad digital por medio del cual identifica, gestiona, trata y mitiga los riesgos de seguridad digital en sus procesos y actividades, alineándolo con los modelos, guías y buenas prácticas suministradas por el Gobierno Nacional.

Los lineamientos relacionados en esta política abarcan a todos los procesos de la entidad con el fin de garantizar un manejo sistemático y unificado que aplique de manera transversal.

Para facilitar los propósitos y requerimientos de administración de riesgos de seguridad digital, se mantiene una adecuada estructura organizacional, el modelo de operación por procesos, los roles y responsabilidades de cada uno de los funcionarios y contratistas de la entidad.

Principios

- Salvaguardar los derechos de los clientes, funcionarios y contratistas, gestionando los riesgos de seguridad digital, asegurando el adecuado flujo y la confidencialidad de la información y la protección de la privacidad y los datos personales.
- La gestión de riesgos de seguridad digital se realiza con la participación de los funcionarios, contratistas, y pasantes, a través de la comunicación y la consulta, con el fin de promover la seguridad digital y aumentar la capacidad de resiliencia frente a eventos no deseados en el entorno digital.
- Asegurar que las partes interesadas conocen sus responsabilidades frente a la gestión de riesgos de seguridad digital, mediante la concientización y educación.
- La gestión de riesgos de seguridad digital es constante debido a la exposición de amenazas y vulnerabilidades del entorno digital.
- La gestión de riesgos de seguridad digital es parte de la toma de decisiones para los nuevos proyectos, el intercambio de información con terceros, la implementación o mejora de controles.
- La Oficina de Riesgos lidera la gestión de riesgos de seguridad digital de acuerdo con lo establecido con esta política, el procedimiento de gestión de riesgos de seguridad digital y la guía metodológica de riesgos de seguridad digital.

Lineamientos

- Se realiza gestión de riesgos de seguridad digital para los activos de información que cumplan con las siguientes características en su clasificación:
  - La confidencialidad sea público clasificado o público reservado y
  - La integridad sea alta o crítica y
  - La disponibilidad sea alta o crítica

  Los activos de información que aunque no se encuentren en esta clasificación, se le aplican controles para su adecuada protección.

- El nivel de aceptación de riesgo de seguridad digital determinado por el ICETEX es el siguiente: riesgos en los niveles "Aceptable" y "Tolerable", dejando como nivel máximo de aceptación del riesgo residual la tipificación de "Tolerable".
- A todos los riesgos identificados se les definen controles que permitan mitigar el impacto o la probabilidad y en caso de que éstos no sean efectivos se establece un plan de tratamiento que permita llegar a un nivel de riesgo residual aceptable.
- ICETEX identifica la infraestructura crítica cibernética en el proceso de inventario y clasificación de activos de información y los riesgos asociados a éstas, en aplicación de la Guía para la Identificación de Infraestructura Crítica Cibernética del Comando Conjunto de las Fuerzas Militares de Colombia
- La gestión de riesgos de seguridad digital se lleva a cabo en el aplicativo de Administración de Riesgos.

- La Entidad comunica y capacita sobre la gestión de riesgo de seguridad digital al personal de la entidad, las partes interesadas y la ciudadanía en general, para que cuenten con la preparación y entendimiento y para realizar su adecuada gestión.

Normas para la Gestión de Riesgos de Seguridad Digital

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

- Actualizar y presentar ante la Junta Directiva las Políticas de Seguridad Digital, acorde con el numeral 6 de este documento.
- Analizar y aprobar el presupuesto para la gestión de riesgo de seguridad digital, y con ello contar con los recursos necesarios para el desarrollo de medidas mitigantes de riesgos de seguridad digital, acorde con el numeral 8.1 de este documento.

Normas dirigidas a: OFICINA DE RIESGOS

- Proponer la política de gestión de riesgo de seguridad digital.
- Definir la metodología de riesgos de seguridad digital, de acuerdo con los lineamientos normativos.
- Definir los roles y responsabilidades para la gestión de riesgos de seguridad digital, de acuerdo con los lineamientos normativos.
- Divulgar la Guía de metodología de riesgos de seguridad digital a los funcionarios y contratistas del Instituto y asegurarse de su permeabilización en todos los niveles de la Entidad, de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad frente a la gestión del riesgo.
- Definir los recursos para el desarrollo de la gestión de riesgo de seguridad digital y presentar al Comité de Seguridad de la Información de manera periódica el seguimiento y control de la ejecución del presupuesto asignado.
- Asesorar y acompañar a los Líderes de Proceso en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles y planes de tratamiento de riesgo.
- Monitorear y revisar los riesgos de seguridad digital con frecuencia anual con el fin preservar la confidencialidad, integridad y disponibilidad de los activos de información y propender por minimizar los impactos que se puedan derivar de estos riesgos.
- Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que esté por fuera del perfil de riesgo de la entidad.
- Consolidar los riesgos de seguridad digital de la Entidad.
- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo de seguridad digital.
- Realizar el reporte de gestión de los riesgos de seguridad digital y suministrar los resultados al Comité de Seguridad de la Información, a la Junta Directiva y a los grupos de interés especial.
- Administrar la información en la aplicación de Gestión de Riesgos.

Normas dirigidas a: VICEPRESIDENTES, DIRECTORES Y JEFES DE OFICINA

- Los Líderes de proceso cumplen el rol de "dueños del riesgo" y en este sentido, son los responsables de la identificación, análisis y evaluación, en conjunto con sus equipos de trabajo; todo lo cual contará con la orientación, guía, liderazgo del Líder de Riesgo delegado para tal fin. Las actividades que cubre son: identificación, análisis y evaluación, tomando como base la Guía para la metodología de identificación y valoración de riesgos de seguridad digital, acción en la cual se pueden apoyar con la Oficina de Riesgos.
- Diseñar, implementar, monitorear adecuadamente los controles y planes de tratamiento a su cargo, además de gestionar de manera directa y permanente los riesgos de seguridad digital de su proceso.
- Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los correspondientes procedimientos.
- Gestionar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos.
- Reportar a la Oficina de Riesgos el estado de avance del plan de tratamiento del riesgo en la operación.
- Valorar los riesgos de seguridad digital una vez implementados los planes de acción y de tratamiento, para verificar su efectividad.
- Evaluar la actualización de la gestión de los riesgos de seguridad digital en los procesos a cargo, de acuerdo con los cambios en el "Direccionamiento estratégico" o en el entorno.

Normas dirigidas a: OFICINA DE CONTROL INTERNO

- Realizar evaluación independiente sobre la gestión del riesgo en la entidad.
- Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos.

Normas dirigidas a: TODOS LOS USUARIOS

- Conocer los riesgos de seguridad digital del proceso y aplicar los controles tal como han sido definidos,
- Apoyar al Líder de Riesgos y al Líder de Proceso en la gestión del riesgo de seguridad digital.
- Reportar a la Oficina de Riesgos los eventos de riesgos de seguridad digital.