MANUAL DE LAS POLÍTICAS DE SEGURIDAD PARA LAS TECNOLOGÍAS DE LA INFORMACIÓN

INSTITUTO TÉCNICO NACIONAL DE COMERCIO

“SIMÓN RODRIGUEZ”

Santiago de Cali, Valle

2017

	ELABORÓ	REVISÓ	APROBÓ
FIRMA			
NOMBRE	Janeth Londoño		
CARGO	Profesional Universitario TI		
FECHA			

TABLA DE CONTENIDO

0. INTRODUCCIÓN

La Oficina de Tecnología de la información (TI), de INTENALCO, por medio de la resolución No 317 de 2 de Noviembre de 2016 adopta y establece la política del modelo de seguridad y privacidad de la información de la institución; para dar cumplimiento al decreto No 2573 de 2014 donde se establece los lineamientos generales de la estrategia de Gobierno en línea, con el objetivo de garantizar el máximo aprovechamiento de las tecnologías de la información.

A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.

INTENALCO requiere del fortalecimiento de la infraestructura de tecnologías de la información para garantizar la responsabilidad, la orientación y preservar los pilares fundamentales de la seguridad de la información como son la CONFIDENCIALIDAD, INTEGRIDAD y DISPONIBILIDAD de la información y establecer un Modelo de Sistema de Gestión de Seguridad de la Información (SGSI) que le permita reunir la sostenibilidad y el conjunto de lineamientos, políticas, normas, procesos e Instituciones que proveen y promueven la puesta en marcha, supervisión, mejora y control, tal como lo señala el Modelo de Seguridad y Privacidad de la Información alineado con la Estrategia de Gobierno en Línea definida en manual GEL versión 3.0; teniendo en cuenta que la Oficina de Tecnologías de la Información, brinda servicios de TI que deben ser gestionados y administrados, para lo cual se hace necesario contar con políticas y procedimientos de seguridad de la información.

1. ALCANCE

INTENALCO Instituto Técnico nacional, a través de su Modelo de Seguridad y Privacidad de la Información, dicta el cumplimiento de los requisitos y lineamientos, que tienen como objetivo, gestionar adecuadamente la seguridad de la información, la gestión de activos, la gestión de riesgos y la continuidad en la prestación del servicio de formación académica. Dichos requisitos y lineamientos serán aplicados a los procesos estratégicos, misionales y de apoyo, por tal motivo, deberán ser conocidos y cumplidos por todo el personal (funcionarios, colaboradores y terceros) que accedan a los sistemas de información e instalaciones físicas de la Institución.

El Modelo de Seguridad y Privacidad de la Información, se encuentran basados, en el marco de lo establecido, en la norma internacional ISO 27001 de 2013 y los componentes estratégicos de Gobierno en Línea, este último desarrollado por el Ministerio de Tecnologías de la Información y las Comunicaciones en Colombia.

2. OBJETIVOS

3.1. OBJETIVO GENERAL

Implementar un MSPI (Modelo de seguridad y privacidad de la información) y Protocolos de Seguridad Informática para la Oficina TI de INTENALCO, basados en la identificación previa de los riesgos informáticos por parte de la entidad.

3.2. OBJETIVOS ESPECÍFICOS

- Analizar los diferentes riesgos informáticos que actualmente se tienen identificados en la Oficina TI.
- Establecer un modelo de Sistema Gestión de Seguridad de la información, con base en los riesgos informáticos identificados.
- Desarrollar un documento con los pasos para la implementación del modelo de Sistema de Gestión de Seguridad de la información, de acuerdo a los riesgos identificados de TI.

3. TÉRMINOS Y DEFINICIONES

- **Acceso a la Información Pública:**

  Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

- **Activo**

  En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Activo de Información**

  En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

- **Archivo**

  Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

- **Auditoría**

  Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

- **Autorización**

  Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

- **Bases de Datos Personales**

  Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

- **Control**

  Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Datos Abiertos**

  Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

- **Datos Personales**

  Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Datos Personales Privados**

  Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

- **Privacidad**

  En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- **Riesgo**

  Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información**

  Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

4. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

RESOLUCIÓN NO. 317 del 2 de Noviembre 2016, "Por la cual se adopta la Política de Seguridad y privacidad de la información en INTENALCO"

Política de seguridad de la información. Para el instituto Técnico Nacional de comercio, Simón Rodríguez, INTENALCO la información es considerada como un activo de valor estratégico, por lo tanto es necesario identificar y proteger sus activos de información.
La institución se compromete a implementar un modelo de seguridad de la información MSPI herramienta que permite identificar y minimizar los riesgos a los cuales está expuesta la información, garantizando el cumplimiento de los requerimientos legales, contractuales regulatorios y de negocio vigentes.

Se deberá preservar la seguridad de la información dando cumplimiento a los principios de:

- ***Confidencialidad***, asegurando que solo aquellos que estén autorizados puedan acceder a la información.
- ***Integridad,*** asegurando que la información y sus métodos de procesos son exactos y completos.
- ***Disponibilidad de la información***, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

Esta política será revisada con regularidad como parte del proceso de revisión de la Dirección, o cuando se identifiquen cambios en el negocio, estructura, objetivos u otra condición que afecte la política; para asegurar que siguen siendo adecuada y ajustada a los requerimientos identificados.

La Vicerrectoría Administrativa y Financiera adelantará las acciones requeridas para la divulgación, socialización y sensibilización en las diferentes dependencias de la política adoptada y establecida.

5. COMPROMISO DE LA DIRECCIÓN

La Alta Dirección de INTENALCO aprueba el Manual de Seguridad y privacidad de la Información, como muestra de su compromiso y apoyo hacia la gestión de seguridad de la información que se lleva a cabo en la Institución, mediante el SGSI y el MSPI de GEL.

La Alta Dirección de INTENALCO demuestran su compromiso de apoyo a través de:

1- La revisión y aprobación del Manual de Seguridad y privacidad de la Información para la Institución.

2- La promoción activa de una cultura de seguridad de la información en los funcionarios, contratistas, docentes, estudiantes, proveedores y/o terceros, que tengan acceso a los sistemas de información, repositorios e instalaciones físicas de INTENALCO.

3- Facilitar la divulgación de este manual a todos los funcionarios, contratistas, docentes, estudiantes, proveedores y/o terceros del instituto.

4- El aseguramiento de los recursos adecuados para implementar y mantener la política y directrices de seguridad de la información, contenidas en el manual.

5- La verificación del cumplimiento de la política y directrices aquí mencionadas.

6. SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los funcionarios, personal externo y proveedores del INTENALCO. Por tal razón, es necesario que las violaciones a las directrices de la Política de Seguridad y privacidad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones

administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

7. POLÍTICAS DE GESTIÓN DE ACTIVOS DE LA INFORMACIÓN

INTENALCO como propietario de la información física así como de la información generada, procesada, almacenada y transmitida en su página Web, otorgará responsabilidad a las oficinas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, Internet, correo electrónico) propiedad de INTENALCO, son activos de la institución y se proporcionan a los funcionarios y terceros autorizados, para cumplir con los propósitos de la entidad.

Toda la información sensible de INTENALCO, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos.

GESTIÓN DE ACTIVOS	
DIRECTRIZ	**ALCANCE**
Las Oficinas deben actuar como propietarias de la información física y electrónica de la entidad, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.	Propietarios activos de información
Los propietarios de los activos de información deben generar un inventario de dichos activos para las áreas o procesos que lideran, acogiendo las indicaciones de las guías de clasificación de la información; así mismo, deben mantener actualizado el inventario de sus activos de información.	Propietarios activos de información
La Oficina de Tecnología es responsable de preparar las estaciones de trabajo fijas y/o portátiles de los funcionarios y de hacer entrega de las mismas.	Oficina de TI
La oficina de Tecnología es responsable de recibir los equipos de trabajo fijo y/o portátil para su reasignación o disposición final, y generar copias de seguridad de la información de los funcionarios que se retiran o cambian de labores, cuando les es formalmente solicitado.	Oficina de TI
Los líderes de proceso, o quien ellos designen, deben recibir los recursos tecnológicos asignados a sus colaboradores cuando estos se retiran del instituto o son trasladados de área.	Líderes de proceso
Los recursos tecnológicos del INTENALCO, 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.	Todos los usuarios
Los funcionarios no deben utilizar sus equipos de cómputo y dispositivos móviles personales para desempeñar las actividades laborales.	Todos los usuarios
Los funcionarios no deben utilizar software no autorizado o de su propiedad en la plataforma tecnológica del INTENALCO.	Todos los usuarios
Todas las estaciones de trabajo, equipos portátiles y demás recursos tecnológicos son asignadas a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.	Todos los usuarios
En el momento de desvinculación o cambio de labores, los funcionarios deben realizar la entrega de su puesto de trabajo; así mismo, deben encontrarse a paz y	Todos los usuarios

salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.	
La contratación y vinculación de personal en INTENALCO, debe ser un proceso donde se garantice la idoneidad del perfil requerido y sean realizadas todas las consultas respecto a trayectoria y experiencia laboral, verificando las referencias de anteriores funcionarios, así como las respectivas investigaciones de seguridad (antecedentes penales, entre otros).	Talento Humano
Debe certificarse que los funcionarios y contratistas del instituto firmen un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo	Talento Humano
Los propietarios de los activos de información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su re-clasificación.	Propietarios activos de información
Los usuarios deben acatar los lineamientos guía de clasificación de la Información 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.	Propietarios activos de información
Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíes faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.	Todos los usuarios
La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo. (Procedimiento de identificación y clasificación de activos GTI-PDR-02). Ley 1581 de 2012	Todos los usuarios

Todos los funcionarios que presten servicios a INTENALCO, adoptarán una política de escritorio limpio con el objeto de prevenir el acceso no autorizado a activos de información cuando estos fuesen desatendidos. De esta manera se evitará la manipulación, pérdida o daño de información que se encuentre en soporte electrónico o en papel.	Todos los usuarios
Cada funcionario es responsable directo de la generación de los backups o copias de respaldo, asegurándose de validar la copia.	Todos los usuarios
Los desarrolladores deben 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.	Desarrolladores externos
La información de cada sistema debe ser respaldada regularmente sobre un medio de almacenamiento como Dvd, discos duros, memorias, etc.	Administradores de sistemas de información
Todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso.	Administradores de sistemas de información
Garantizar que toda información, etiquetada como Reservada para INTENALCO, sea almacenada, transmitida y recibida de manera segura, garantizando con esto la preservación de la confidencialidad e integridad de la misma	Desarrolladores externos Todos los usuarios

8. POLÍTICAS DE CONTROL DE ACCESO

La Política de Control de Acceso a la información deberá controlar los requisitos y seguridad; a través de la oficina de TI quien administrará el ciclo de vida de los usuarios, desde la creación automática de las cuentas, roles y permisos necesarios hasta su inoperancia; a partir de los requerimientos reportadas por Recursos Humanos y/o directamente de su Jefatura directa; lo anterior para que el funcionario tenga acceso adecuado a los sistemas de información y recursos tecnológicos, validando su autenticación, autorización y auditoría.

CONTROL DE ACCESO	
DIRECTRICES	**ALCANCE**
La oficina de TI debe asegurar que las redes inalámbricas del instituto cuenten con métodos de autenticación que evite accesos no autorizados	Oficina de TI
Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos del instituto deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.	Todos los usuarios
Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso.	Propietarios activos de información
Los desarrolladores deben certificar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles	Desarrolladores externos
Los medios de respaldo como memorias, discos y documentos, se deben ubicar en áreas restringidas y/ó en sitios con acceso únicamente a personas autorizadas	Todos los usuarios
Las Estaciones de trabajo, Servidores y Aplicativos que se tengan al interior de la INTENALCO deben ser protegidos mediante usuario y contraseña. Se debe establecer una caducidad específica para la contraseña, la cual será asignada inicialmente de forma confidencial y segura al usuario, quien debe realizar cambio en el primer login, además, tendrá una longitud mínima de 8 caracteres y será alfanumérica.	Todos los usuarios
Cambiar las contraseñas periódicamente con la frecuencia que se haya determinado para los distintos sistemas y aplicaciones, al menos cada 30 días y siempre que por configuración de los sistemas o aplicaciones se solicite expresamente	Todos los usuarios
Los usuarios deben responder 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 de INTENALCO. En caso de que suceda algún evento irregular con los tokens los usuarios deben asumir la responsabilidad administrativa, disciplinaria y económica.	Usuarios con firma Digital.
Los usuarios de la plataforma tecnológica y los sistemas de información de INTENALCO deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.	Todos los usuarios
Los funcionarios no deben compartir sus cuentas de usuario y contraseñas con otros funcionarios o con contratistas.	Todos los usuarios

9. POLÍTICAS DE SEGURIDAD FÍSICA

INTENALCO proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones. Así mismo, controlará las amenazas físicas externas e internas de sus oficinas. Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideras áreas de acceso restringido.

SEGURIDAD FÍSICA	
DIRECTRICES	**ALCANCE**
Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por funcionarios de la oficina de TI; no obstante, los visitantes siempre deberán estar acompañados de un funcionario de dicha oficina durante su visita al centro de cómputo o los centros de cableado.	Oficina de TI
La Oficina de TI debe 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.	Oficina de TI
Se debe velar porque los recursos de la plataforma tecnológica de INTENALCO ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.	Vicerrectoría Administrativa y Financiera
Se debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de INTENALCO.	Vicerrectoría Administrativa y Financiera
La oficina de TI debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica del instituto (Plan de mantenimiento preventivo anual)	Oficina TI
Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la oficina de TI	Oficina TI
El instituto debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de INTENALCO	Vicerrectoría Administrativa y Financiera

La oficina de TI 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.	Todos los usuarios
Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico propiedad del INTENALCO el usuario responsable debe informar a la oficina de TI realizará una asistencia adecuada. El usuario no debe intentar solucionar el problema.	Todos los usuarios
La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, y demás recursos tecnológicos del instituto, solo puede ser realizado por los funcionarios de la oficina de TI, o personal de terceras partes autorizado por dicha dirección.	Todos los usuarios
Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física	Todos los usuarios
En caso de pérdida o robo de un equipo de cómputo del INTENALCO, 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	Todos los usuarios
Garantizar que todo Funcionario, Contratista, Proveedor, Docente, Estudiante, Ciudadano y/o Visitante, que necesite utilizar las instalaciones físicas de INTENALCO, realice su ingreso y salida, cumpliendo con los lineamientos de seguridad física adecuados y aprobados por la Alta Dirección de la Institución.	Alta dirección

10. POLÍTICAS DE SOFTWARE

INTENALCO proporcionará los mecanismos necesarios que garanticen 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. Además, proporcionará los mecanismos para generar cultura de seguridad entre sus funcionarios y personal provisto por terceras partes frente a los ataques de software malicioso.

SOFTWARE	
DIRECTRICES	**ALCANCE**
Se debe proveer herramientas tales como antivirus, antimalware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en los servicios que se ejecutan en la misma	Oficina de TI
La Oficina de Tecnología de la información debe asegurar que el software de antivirus, 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.	Oficina de TI
La oficina de TI debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios del instituto y configurar dichos equipos acogiendo los estándares generados.	Oficina TI
Los usuarios de recursos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, definida por TI; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.	Todos los usuarios
Los usuarios deben asegurarse 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.	Todos los usuarios
Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar a la oficina de TI, para que a través de ella, se tomen las medidas de control correspondientes.	Todos los usuarios
Generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.	Web master

La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario del instituto o provisto por un tercero, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya	Todos los usuarios
Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional de INTENALCO. El correo institucional no debe ser utilizado para actividades como: 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 y resulten ofensivas para los funcionarios del instituto.	Todos los usuarios
Todo correo electrónico debe tener la siguiente información básica como: Nombres y apellidos, cargo, dependencia, número de teléfono y extensión.	Todos los usuarios
Los usuarios del servicio de Internet de INTENALCO deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.	Todos los usuarios
Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo.	Todos los usuarios
No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.	Todos los usuarios
Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN, Yahoo, Skype, y otros	Todos los usuarios

similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de INTENALCO.	
No está permitido 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	Todos los usuarios
No está permitido el intercambio no autorizado de información de propiedad de INTENALCO, de sus ESTUDIANTES y/o de sus funcionarios, con terceros	Todos los usuarios
No es permitido el uso de redes, sistemas o equipos de INTENALCO para la creación, ejecución o propagación intencionada de virus o código malicioso	Todos los usuarios

11. POLÍTICAS DE INTEGRIDAD

La Política de integridad de los datos deberá controlar el intercambio de información entre INTENALCO y otras entidades o personas externas, para mantener los datos libres de modificaciones no autorizadas ya sea por usuarios de la entidad o externos.

INTEGRIDAD	
DIRECTRICES	**ALCANCE**
Se debe definir los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre el instituto y tercera partes incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar se debe incluir la prohibición de divulgar la información entregada por INTENALCO a los terceros con quienes se establecen estos acuerdos y la destrucción de dicha información una vez cumpla su cometido.	Secretaria General
Se debe establecer en los contratos que se realicen 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 en razón del cumplimiento de los objetivos misionales de INTENALCO.	Secretaria General
Los propietarios de los activos de información deben velar porque la información de INTENALCO o de sus beneficiarios sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información, verificando el cumplimiento de las clausulas relacionadas en los contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos.	Todos los usuarios
Los propietarios de los activos de información, o a quien ellos deleguen, deben verificar 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.	Todos los usuarios

12. POLÍTICAS DE CONTINUIDAD, CONTINGENCIA, RECUPERACIÓN Y RETORNO A LA NORMALIDAD

INTENALCO proporcionará los recursos suficientes para proporcionar una respuesta efectiva de funcionarios y procesos en caso de contingencia o eventos catastróficos que se presenten en el instituto y que afecten la continuidad de su operación. Además, responderá de manera efectiva ante eventos catastróficos según la magnitud y el grado de afectación de los mismos; se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos.

CONTINUIDAD, CONTINGENCIA, RECUPERACIÓN Y RETORNO A LA NORMALIDAD	
DIRECTRICES	**ALCANCE**
Se deben liderar los temas relacionados con la continuidad del negocio y la recuperación ante desastres	Vicerrectoría Administrativa y Financiera
Elaborar un plan de recuperación ante desastres para el centro de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados.	Oficina de TI
Los líderes de proceso deben identificar y, al interior de sus áreas, generar la documentación de los procedimientos de continuidad que podrían ser utilizados en caso de un evento adverso, teniendo en cuenta la seguridad de la información. Estos documentos deben ser probados para certificar su efectividad.	Líderes de proceso
Todas las estaciones de trabajo se deben equipar con unidades suplementarias de energía eléctrica (UPS), filtros eléctricos, supresores de picos de corriente y en lo posible, eliminadores de corriente estática.	Todos los usuarios

13. POLÍTICAS DE CUMPLIMIENTO REQUISITOS LEGALES

Se establecerán los términos, condiciones y finalidades para las cuales INTENALCO, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que en algún momento, por razones de la actividad que desarrolla el instituto, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, INTENALCO exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales. Así mismo, buscará proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información que el instituto conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias del instituto y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

INTENALCO velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

CUMPLIMIENTO REQUISITOS LEGALES	
DIRECTRICES	**ALCANCE**
Certificar que todo el software que se ejecuta en el instituto esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso	Supervisor contrato
Establecer un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo del instituto para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo corresponda únicamente al permitido.	Oficina de TI
Los usuarios no deben instalar software o sistemas de información en sus estaciones de trabajo suministrados para el desarrollo de sus actividades	Todos los usuarios
Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada	Todos los usuarios
Las áreas que procesan datos personales de estudiantes, funcionarios, proveedores u otras terceras partes deben 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.	Todos los usuarios
Establecer los controles para el tratamiento y protección de los datos personales de los estudiantes, funcionarios, proveedores y demás terceros de INTENALCO de los cuales reciban y administre información.	Secretaria General

Implantar los controles necesarios para proteger la información personal de los estudiantes, funcionarios, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.	Secretaria General Vicerrectorías
Es deber de los usuarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por correo electrónico o por correo certificado, entre otros.	Todos los usuarios

14. PROCEDIMIENTOS QUE APOYAN LA POLÍTICA DE SEGURIDAD

Los procedimientos son uno de los elementos dentro de la documentación del Manual de Seguridad de la Información. Un procedimiento describe de forma más detallada lo que se hace en las actividades de un proceso, en él se especifica cómo se deben desarrollar las actividades, cuáles son los recursos, el método y el objetivo que se pretende lograr o el valor agregado que genera y caracteriza el proceso.

15.1. Procedimiento de Respaldo de la información

Establece las directrices de respaldo y recuperación de información, con objeto de proteger los datos y sistemas necesarios para la continuidad operacional de INTENALCO. Este procedimiento define la información que se respalda en la institución y es aplicable a todos los funcionarios.
Aparece en los procedimientos de la institución como **GTI-PRD-01.**

15.2. Procedimiento Activos de Información

Define la metodología para la realización el inventario, clasificación y etiquetado de activos de información, que permita establecer un nivel de importancia en INTENALCO. Aplica a todos los activos de información de INTENALCO. Aparece en los procedimientos de la institución como **GTI-PRD-02.**

15.3. Procedimiento de Ingreso y egreso de equipos tecnológicos

Lograr una correcta administración, coordinación, registro y control en el ingreso y salida de los equipos tecnológicos de las instalaciones de INTENALCO. Aplica para todos los funcionarios, contratistas, proveedores, estudiantes y visitantes que ingresan a las instalaciones de INTENALCO. Aparece en los procedimientos de la institución como **GTI-PRD-03.**