

# **INSTITUTO DE DESARROLLO RURAL**



## **MANUAL DE POLÍTICAS DE TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN**

**marzo, 2018**

## Entendimiento

Como resultado del proyecto “IMPLEMENTACIÓN DE LAS NORMAS TÉCNICAS PARA LA GESTIÓN Y EL CONTROL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN (TI) EMITIDAS POR LA CONTRALORÍA GENERAL DE LA REPÚBLICA (NTCGR)” liderado por la Comisión de Normas Técnicas del Inder, la firma consultora *PricewaterhouseCoopers* apoyó con la definición de las políticas que conforman este documento, siendo, posteriormente, ampliadas por Tecnologías de la Información.

## Listado de políticas

En la siguiente tabla se detallan las 32 políticas definidas y aprobadas, el número de página donde se puede ubicar dentro de este manual y la referencia al objetivo de control de las NTCGR. En el nombre de la política se hace un enlace directo al detalle de dicha política.

Nombre de política	Número de página	Referencia NTCGR
<a href="#">PL-TI-001 – Planeación estratégica de TI</a>	9	1.1 Marco Estratégico de TI
<a href="#">PL-TI-002 – Administración de la calidad</a>	12	1.2 Gestión de la Calidad
<a href="#">PL-TI-003 – Administración de riesgos</a>	14	3. Administración de riesgos
<a href="#">PL-TI-004 – Seguridad de la información</a>	16	1.4 Gestión de la seguridad de la información
<a href="#">PL-TI-005 – Clasificación de la información</a>	19	1.4 Gestión de la seguridad de la información
<a href="#">PL-TI-006 – Uso de recursos tecnológicos</a>	21	1.4 Gestión de la seguridad de la información
<a href="#">PL-TI-007 – Administración de cuentas de usuario y contraseñas</a>	24	1.4 Gestión de la seguridad de la información
<a href="#">PL-TI-008 – Uso de correo electrónico</a>	29	1.4 Gestión de la seguridad de la información
<a href="#">PL-TI-009 – Uso del internet</a>	33	1.4 Gestión de la seguridad de la información
<a href="#">PL-TI-010 – Concienciación y Capacitación</a>	36	1.4 Gestión de la seguridad de la información
<a href="#">PL-TI-011 – Auditoría y Monitoreo</a>	36	1.4 Gestión de la seguridad de la información 5.1 Seguimiento de los procesos de TI 5.2 Seguimiento y evaluación de control interno de TI 5.3 Participación de la Auditoría Interna
<a href="#">PL-TI-012 – Seguridad Física y Ambiental</a>	38	1.4 Gestión de la seguridad de la información
<a href="#">PL-TI-013 – Administración de Amenazas y Vulnerabilidades</a>	40	1.4 Gestión de la seguridad de la información

Nombre de política	Número de página	Referencia NTCGR
<b><u>PL-TI-014 – Manipulación y Destrucción de Datos</u></b>	43	1.4 Gestión de la seguridad de la información
<b><u>PL-TI-015 – Privacidad y Protección de la Información</u></b>	45	1.4 Gestión de la seguridad de la información
<b><u>PL-TI-016 – Control de Virus y Software Malicioso</u></b>	47	1.4 Gestión de la seguridad de la información
<b><u>PL-TI-017 – Fin de la Relación Laboral</u></b>	49	1.4 Gestión de la seguridad de la información
<b><u>PL-TI-018 – Administración de la Infraestructura de Software</u></b>	52	1.4 Gestión de la seguridad de la información
<b><u>PL-TI-019 – Administración de la Infraestructura de Hardware</u></b>	54	1.4 Gestión de la seguridad de la información
<b><u>PL-TI-020 – Continuidad de TI</u></b>	58	1.4 Gestión de la seguridad de la información
<b><u>PL-TI-021 – Respaldos y recuperación</u></b>	61	1.4 Gestión de la seguridad de la información
<b><u>PL-TI-022 – Administración de proyectos de TI</u></b>	64	1.5 Gestión de Proyectos
<b><u>PL-TI-023 – Administración de la capacidad</u></b>	67	2.1 Planificación de las Tecnologías de Información 4.2 Administración y operación de la plataforma tecnológica
<b><u>PL-TI-024 – Segregación de funciones y responsabilidades de TI</u></b>	70	1.6 Decisiones sobre asuntos estratégicos de TI 2.4 Independencia y recurso humano de la función de TI 3.1 Consideraciones generales de la implementación de TI
<b><u>PL-TI-025 – Administración de niveles de servicio</u></b>	72	4.1 Definición y administración de acuerdos de servicios
<b><u>PL-TI-026 – Administración de cambios y liberaciones</u></b>	74	4.2 Administración y operación de la plataforma tecnológica
<b><u>PL-TI-027 – Atención de usuarios</u></b>	76	1.6 Decisiones sobre asuntos estratégicos de TI 4.4 Atención de requerimientos de los usuarios de TI
<b><u>PL-TI-028 – Administración de incidentes y problemas</u></b>	79	1.6 Decisiones sobre asuntos estratégicos de TI 4.5 Manejo de incidentes
<b><u>PL-TI-029 – Administración de terceros</u></b>	81	3.4 Contratación de terceros para la implementación y mantenimiento de software e infraestructura 4.6 Administración de servicios prestados por terceros
<b><u>PL-TI-030 – Monitoreo del desempeño de TI</u></b>	86	1.7 Cumplimiento de obligaciones relacionadas con TI 5.1 Seguimiento de los procesos de TI
<b><u>PL-TI-031 – Restringir el acceso a los servidores del Centro de Datos</u></b>	89	1.4 Gestión de la seguridad de la información
<b><u>PL-TI-032 – Cambio de equipo de cómputo</u></b>	92	2.1 Planificación de las Tecnologías de Información

Nombre de política	Número de página	Referencia NTCGR
		4.2 Administración y operación de la plataforma tecnológica

## Glosario de términos

Términos	Definición
<b>Acuerdo de confidencialidad</b>	Es un acuerdo generalmente entre dos partes para compartir alguna información y conservar su carácter confidencial o secreto, como parte de una relación comercial o laboral.
<b>Administración Superior</b>	Grupo conformado por la Junta Directiva, la Presidencia Ejecutiva y la Gerencia General.
<b>Amenazas</b>	Factores físicos (incendios, inundaciones) o relacionados con personas (errores, fraudes, omisiones) capaces de causar daños por la existencia de vulnerabilidades.
<b>Análisis de riesgo</b>	Un uso sistemático de la información disponible para determinar qué tan frecuentemente pueden ocurrir eventos especificados y la magnitud de sus consecuencias.
<b>Análisis de Vulnerabilidades y Riesgo</b>	Proceso interactivo e iterativo basado en el conocimiento, evaluación y manejo de los riesgos y sus impactos, identificando las debilidades existentes en los activos de información, permitiendo valorar la exposición de los mismos a una amenaza existente.
<b>Antivirus</b>	Aplicación o grupo de aplicaciones dedicadas a la prevención, búsqueda, detección y eliminación de programas malignos en sistemas informáticos.
<b>Apetito de riesgo</b>	El nivel de riesgo que el Inder está dispuesta a aceptar.
<b>Aplicativo, aplicación o programa</b>	Es un programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajo. Algunos ejemplos de programas de aplicación pueden ser: multimedia (Windows Media Player), presentaciones (Power Point), diseño gráfico (GIMP), cálculo (Excel), correo electrónico (Outlook), compresión de archivos (WinZip), etc.
<b>Autenticación</b>	Acto de establecimiento o confirmación de un usuario o sistema como auténtico.
<b>Calidad</b>	Grado en el que un conjunto de características inherentes cumple con requisitos establecidos.
<b>Cambio</b>	De acuerdo con la definición del marco de referencia ITIL, un cambio es cualquier adición, modificación o eliminación de hardware, dispositivos de telecomunicaciones, software, aplicaciones, ambientes, sistemas o documentación relacionada.
<b>Cambio de emergencia</b>	Un cambio que debe ser introducido lo más pronto posible al ambiente de producción. En su mayoría corresponden a cambios cuyo objetivo es reparar un error que está impactando negativamente al negocio.
<b>Casos sospechosos</b>	Se define como alguna situación en la que respaldada por evidencia se pueda aseverar el incumplimiento de alguna de las políticas establecidas.
<b>Chat</b>	Distintas formas posibles de comunicarse en tiempo real con otras personas mediante mensajes escritos, bien sea empleando utilidades como los IRC, o bien mediante los servicios que muchos portales de Internet ponen a disposición de sus usuarios.
<b>Cinta magnética</b>	Es un tipo de medio o soporte de almacenamiento de información que se graba en pistas sobre una banda plástica con un material magnetizado, generalmente óxido de hierro o algún cromato. El tipo de información que se puede almacenar en las cintas magnéticas es variado, como vídeo, audio y datos.
<b>Claves</b>	Contraseña que un usuario emplea para acceder a un servicio, sistema o programa. Generalmente la clave de acceso está asociada a un nombre de usuario.
<b>Ciente de correo electrónico</b>	Es un programa usado para leer y enviar correos electrónicos (e-mails).

<b>Términos</b>	<b>Definición</b>
<b>Concienciación</b>	Hacer que alguien sea consciente de algo, que lo conozca y sepa de su alcance
<b>Confidencialidad</b>	Se garantiza que la información sea accesible sólo para aquellas personas autorizadas a hacerlo.
<b>Control</b>	Medidas adoptadas por la organización que reducen el riesgo de que una debilidad existente se concrete.
<b>Criterios de evaluación del riesgo</b>	Aquellos parámetros necesarios para realizar el análisis de riesgos. Incluye los criterios cualitativos/cuantitativos de impacto y probabilidad.
<b>Cuenta</b>	Una cuenta de usuario nos permite autenticarnos a los servicios de un sistema. A una cuenta se le identifica por un nombre de usuario (comúnmente conocido como login) y una contraseña (o password). El nombre de usuario es un nombre único que se identifica a cada usuario (aunque en ocasiones existen alguna clase de usuarios 'invitado'). Los nombres de usuario se basan por lo general en cadenas cortas alfanuméricas.
<b>Desmagnetización</b>	Proceso que se realiza para remover el magnetismo a un dispositivo.
<b>Desmenuzamiento</b>	Deshacer un objeto o elemento dividiéndolo en partes menudas.
<b>Dispositivos removibles</b>	Son aquellos elementos de hardware independientes a la computadora y que son portables. Ver Memory Stick y Llave Maya.
<b>Documento digitalizado</b>	Transformación de la información consignada en forma analógica en una secuencia de valores numéricos, es decir, en una representación electrónica que se puede almacenar y acceder por medio de una computadora.
<b>Documento electrónico</b>	Significa información que se encuentra almacenada en un medio tangible, o que se guarda en un medio electrónico y que se puede recuperar o reproducir en una forma perceptible inteligible.
<b>Evidencia</b>	Rastros existentes que debidamente preservados y puestos en relación con información existente o en el contexto de otras evidencias o de hechos probados permiten demostrar que se ha llevado a cabo una acción, permitiendo en muchos casos identificar quien o quienes la han llevado a cabo.
<b>Funcionario</b>	Entiéndase por los empleados activos del Inder
<b>Herramienta espía</b>	Herramienta utilizada con la finalidad de monitorear sin la debida autorización las actividades de uno o más usuarios en sus computadoras.
<b>Incidente</b>	Cualquier evento que no es parte de la operación normal de un servicio y que causa o podría causar una interrupción o reducción en la calidad del servicio.
<b>Incineración</b>	Combustión completa de la materia orgánica hasta su conversión en cenizas, usada sobre todo en el tratamiento de basuras.
<b>Integridad</b>	Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
<b>Liberación</b>	Hardware, software, documentación, procesos u otros componentes requeridos para implementar uno o más cambios aprobados en la infraestructura de de Tecnología de Información. Los contenidos de cada Liberación son administrados, probados y puestos en funcionamiento como una sola unidad.
<b>Llave maya o Memoria flash</b>	Son dispositivos de almacenamiento externo conectado a través de los puertos USB.
<b>Medida correctiva</b>	Medida orientada a solucionar los problemas en el momento que surgen.
<b>Medida preventiva</b>	Medida dirigida a identificar y resolver los problemas antes de que ocurran.

<b>Términos</b>	<b>Definición</b>
<b>Memory Stick</b>	Es un formato de tarjeta de memoria. Una tarjeta de memoria o tarjeta de memoria flash es un dispositivo de almacenamiento que conserva la información que le ha sido almacenada de forma correcta aun con la pérdida de energía, es decir, es una memoria no volátil.
<b>Mesa de ayuda</b>	Mesa de servicios o de ayuda encargada de servir como único punto de contacto entre el usuario y la organización de TI.
<b>Normas técnicas para la gestión y el control de las TI</b>	Normativa emitida por la Contraloría general de la República que establece los criterios básicos de control que deben observarse en la gestión de esas tecnologías y que tiene como propósito coadyuvar en su gestión, en virtud de que dichas tecnologías se han convertido en un instrumento esencial en la prestación de los servicios públicos, representando inversiones importantes en el presupuesto del Estado
<b>Parche</b>	En informática, un parche es una sección de código que se introduce a un programa. Dicho código puede tener varios objetivos; sustituir código erróneo, agregar funcionalidad al programa, aplicar una actualización, etc.
<b>Password</b>	Contraseña, clave, key, llave. Conjunto finito de caracteres limitados que forman una palabra secreta que sirve a uno o más usuarios para acceder a un determinado recurso.
<b>PETI (Plan Estratégico de Tecnología de Información)</b>	Instrumento que define y documenta el propósito de TI, con una visión de largo plazo y selecciona las mejores alternativas de gestión que tiene en un contexto determinado.
<b>Plan de retorno</b>	Proceso que explica de manera detallada cómo devolverse al estado anterior en caso de que la implementación del cambio falle.
<b>Plan estratégico</b>	Documento oficial en el que los responsables de una organización (empresarial, institucional, no gubernamental...) reflejan cual será la estrategia a seguir por su compañía en el medio plazo
<b>Plan operativo</b>	Posibilitan transformar en realidad los objetivos estratégicos de la Organización. En él se define con claridad qué se desea, cómo y cuándo se realizará, así como quién será el encargado de las diferentes tareas. Incluye metas con un horizonte de tiempo de 1 año.
<b>PMBOK</b>	Es un estándar en la gestión de proyectos desarrollado por el Project Management Institute (PMI). El PMBOK es una colección de procesos y áreas de conocimiento generalmente aceptadas como las mejores prácticas dentro de la gestión de proyectos y que provee los fundamentos de la gestión de proyectos que son aplicables a un amplio rango de proyectos, incluyendo construcción, software, ingeniería, etc.
<b>Política</b>	Las políticas desde de la gestión; marcan la filosofía y la estrategia del equipo directivo y constituyen el marco básico para las demás normas escritas. Las políticas son un conjunto de criterios generales que establece una organización.
<b>Prioridad</b>	Una categorización utilizada para identificar la importancia relativa de un cambio basado en la urgencia del mismo. Se utiliza para identificar los tiempos requeridos para tomar acciones.
<b>Problema</b>	Se refiere a un incidente repetitivo del cual no se tiene identificada la causa raíz.
<b>Procedimiento</b>	Los procedimientos son conjuntos de instrucciones que describen como implantar las políticas departamentales o empresariales. Debido a ello, los procedimientos están generalmente mucho más detallados que los informes de las políticas, añadiendo, incluso, instrucciones para seguir y llevar a cabo, paso a paso, determinadas tareas.
<b>Procesos</b>	Conjunto de tareas, actividades o acciones interrelacionadas entre sí que, a partir de una o varias entradas de información, materiales o de salidas de otros procesos, dan lugar a una o varias salidas también de materiales (productos) o información con un valor añadido.

<b>Términos</b>	<b>Definición</b>
<b>Programas P2P</b>	Programas Peer-To-Peer (P2P), los cuales usan una red común (por lo general diferente para cada programa), para comunicar entre si las computadoras de sus usuarios, los que comparten ciertos directorios, donde se encuentran los archivos a intercambiar.
<b>Protector de pantalla</b>	Programa que se activa cuando la computadora se encuentra inactiva por un período determinado de tiempo y muestra efectos gráficos en la pantalla, generalmente ocultando el contenido con el que se está trabajando.
<b>Proyecto</b>	Un proyecto es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único.
<b>Recurso tecnológico</b>	Un recurso tecnológico hace referencia a cualquier equipo tecnológico (computadoras, laptops, faxes, impresoras, teléfonos, etc.) dentro del Inder que brindan soporte a los funcionarios para el buen desarrollo de sus labores.
<b>Respaldos</b>	Hacer una copia de seguridad o copia de respaldo (backup en inglés) se refiere a la copia de datos de tal forma que estas copias adicionales puedan restaurar un sistema después de una pérdida de información.
<b>Riesgo</b>	La posibilidad de que suceda algo que tendrá un impacto sobre los objetivos.
<b>Roles</b>	Un rol de usuario es el conjunto de permisos que se asignan a un usuario que se registra a un servicio, aplicación o sistema. De esta forma cada usuario representa un papel concreto con sus respectivos accesos a las funcionalidades.
<b>Seguridad de la información</b>	Conjunto de regulaciones, procedimientos y acciones dirigidas a preservar la confidencialidad, integridad y disponibilidad de la información, minimizar los riesgos y maximizar el retorno sobre la inversión y el aprovechamiento de oportunidades de negocios, a efecto de alcanzar los objetivos del Inder.
<b>Sistema de información</b>	Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su posterior uso, generados para cubrir una necesidad (objetivo). Todos estos elementos interactúan entre sí para procesar los datos (incluyendo procesos manuales y automáticos) dando lugar a información más elaborada y distribuyéndola de la manera más adecuada posible en una determinada organización en función de sus objetivos.
<b>SLA o Acuerdo de Nivel de Servicio</b>	Un acuerdo de nivel de servicio (SLA por el inglés Service Level Agreement) es un acuerdo negociado formalmente entre dos partes. Es un contrato que existe entre el cliente y su proveedor de servicio, o entre proveedores de servicio. Registra el entendimiento común de los servicios, prioridades, responsabilidades, garantías y demás, conocidos en forma colectiva como el "nivel de servicio".
<b>Tercero</b>	Persona que tiene un contrato por un periodo de tiempo definido, que no pertenece al Inder pero labora temporalmente para la institución, por ejemplo proveedores o entidades externas.
<b>Tolerancia de riesgo</b>	La variación aceptable (más o menos) del nivel riesgo que la Corporación está dispuesta a aceptar.
<b>Tunning de base de datos</b>	Proceso por medio del cual se homogeniza y optimiza el desempeño de una base de datos. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.
<b>Usuario</b>	Todas aquellas personas que utilicen sistemas, software, equipos informáticos y los servicios de Red provistos por el Inder.
<b>Virus</b>	Programa de computadora que tiene la capacidad de registrar, dañar eliminar datos y su característica más relevante es que puede replicarse a sí mismo y propagarse a otras computadoras.



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Planeación Estratégica de TI

Código: PL-TI-001

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

### 1. Objetivo

1.1 Regular la implementación y actualización de la estrategia de Tecnologías de Información, para administrar y dirigir todos los recursos de TI de acuerdo con la estrategia del negocio y sus prioridades.

### 2. Alcance

2.1 Esta política aplica para todos los funcionarios del Inder que participan en el proceso de creación, actualización y monitoreo de la Estrategia de Tecnologías de la Información.

### 3. Responsables

3.1 Administración Superior: Dar a conocer oportunamente el Plan Estratégico Institucional con el fin de que el PETI se alinee adecuadamente con dicho plan.

3.2 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.

3.3 Comité de TI: Revisar y aprobar las estrategias de TI.

3.4 Tecnologías de la Información: Definir la estrategia de TI y mantenerla alineada a los objetivos del Inder.

### 4. Pautas

4.1 La creación o actualización del PETI es responsabilidad de Tecnologías de la Información, considerando la alineación con el Plan Estratégico Institucional.

4.2 Para la creación y actualización del PETI, se debe realizar un diagnóstico de la situación actual y evaluación de los riesgos de la Función de TI.

4.3 Todo PETI que haya sido creado o actualizado, debe ser aprobado por el Comité de TI y por Junta Directiva.

4.4 Es responsabilidad de las áreas críticas del Inder proveer a TI de sus planes estratégicos, así como comunicar cuando surge algún cambio en éstos, con el fin de que sean tomados en cuenta en el momento de la definición o actualización del PETI.

4.5 Tecnologías de la Información debe registrar las alertas detectadas en el monitoreo del PETI y elaborar la propuesta de acciones correctivas o preventivas a ejecutar para presentar al Comité de TI.

4.6 Tecnologías de la Información es el encargado de realizar las comunicaciones y publicaciones requeridas como resultado de las decisiones tomadas por el Comité de TI en relación con la Estrategia de TI.

4.7 Es responsabilidad de TI velar por que el PETI cuente con planes operativos que contribuyan a alcanzar los objetivos estratégicos y las metas definidas en dicho plan.

4.8 El PETI debe incluir un portafolio de proyectos que permitan cumplir con los objetivos estratégicos del Inder. El portafolio de proyectos debe contener las acciones de mejora a desarrollar, los plazos



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Planeación Estratégica de TI

Código: PL-TI-001

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

de ejecución, los responsables y beneficios de estos proyectos y los indicadores de desempeño que permitan el monitoreo de dichos proyectos.

- 4.9 Es responsabilidad de Tecnologías de la Información velar porque el PETI sea revisado y actualizado anualmente o cuando ocurra alguno de los siguientes eventos:
- Como respuesta a una alerta generada durante el monitoreo de los indicadores de meta del PETI, cuya acción correctiva definida sea realizar un cambio a éste.
  - Cuando se detecte un cambio en la estrategia del Inder.
  - Cuando se den cambios en los planes operativos de TI, que impacten la estrategia de ésta y que impliquen un cambio en el PETI.
  - Cuando se den cambios en la normativa de los órganos reguladores.
- 4.10 El monitoreo de la ejecución del PETI deberá realizarse semestralmente, para asegurar que se estén cumpliendo las metas establecidas en dicho plan.
- 4.11 Una vez finalizado el monitoreo del PETI, la jefatura de Tecnologías de la Información, debe comunicar al Comité de TI las acciones estratégicas planteadas.

### 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

### 6. Aprobación

#### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i Tecnologías de la Información	

#### 6.2 Aprobación por el Comité de Tecnologías de la Información

##### Acuerdo de aprobación por el Comité de Tecnologías de la Información

Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.

#### 6.3 Aprobación por la Junta Directiva del Inder

##### Acuerdo de aprobación por Junta Directiva

Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.

### 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
---------	-------	-------	-------	-----------------



**TECNOLOGIAS DE LA INFORMACIÓN**  
**Política: Planeación Estratégica de TI**

Código: PL-TI-001

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

<b>2.0</b>	Carmen Zuñiga Córdoba Manuel Montero Ureña	Contraparte Técnica TI	30/06/2017	Creación de las políticas PL-TI-031 y PL-TI-032.
------------	---	---------------------------	------------	---



## **TECNOLOGÍAS DE LA INFORMACIÓN**

### **Política: Administración de la Calidad de TI**

Código: PL-TI-002

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

#### **1. Objetivo**

1.1 Garantizar que las Tecnologías de la Información del Inder están dando valor al negocio, mejora continua y transparencia para los interesados.

#### **2. Alcance**

2.1 Esta política es aplicable a todos los funcionarios del Inder, incluyendo a todos los niveles de la estructura organizacional del Inder.

#### **3. Responsables**

3.1 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.

3.2 Tecnologías de la Información: Garantizar la calidad en los servicios ofrecidos de acuerdo con los requerimientos del negocio.

3.3 Funcionarios: Conocer y aplicar lo estipulado en esta política.

#### **4. Pautas**

4.1 Tecnologías de la Información debe establecer las metas de calidad en relación a su función y los planes para su cumplimiento.

4.2 Es responsabilidad de las Unidades Administrativas asumir los roles delegados por la Administración Superior, que los involucran en la gestión de los procesos de TI, con el fin de garantizar el cumplimiento de sus requisitos de calidad.

4.3 Como parte del proceso de Planificación Estratégica de TI, durante las sesiones de análisis del contexto estratégico institucional, se debe velar por que se capturen los requisitos de calidad para TI, expresados por los directores y jefes de los procesos críticos del Inder.

4.4 Es responsabilidad de cada Unidad Administrativa comunicar oportunamente todo requisito de calidad, con el fin de que la función de TI valore la factibilidad de incorporarlo al plan de calidad vigente.

4.5 Los lineamientos, procesos, organización, metodologías y herramientas formalizados en el plan de calidad de TI deben ser de aplicación universal para todos los funcionarios que ejecuten actividades de gestión de las tecnologías de la información del Inder.

4.6 Los directores y jefes de los procesos de negocio y demás funcionarios clave que sean definidos como clientes de los servicios de TI, deben atender oportuna y confiablemente la evaluación de la satisfacción con respecto a la calidad de la gestión de las tecnologías de la información.

4.7 Las Unidades Administrativas y las instancias usuarias de los servicios de TI que sean convocados a las sesiones de concientización, lanzamiento y seguimiento de iniciativas de calidad, deben atender éstas oportunamente, con el fin de retroalimentar sobre el alineamiento entre la calidad gestionada por TI y los requisitos del negocio.

4.8 Cada proyecto de TI debe contar con objetivos claros en relación con la calidad requerida tanto en los entregables como en el proyecto en forma integral.



## TECNOLOGÍAS DE LA INFORMACIÓN

### Política: Administración de la Calidad de TI

Código: PL-TI-002

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

#### 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

#### 6. Aprobación

##### 6.1 Aprobación y dictamen de conformidad técnica Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

##### 6.2 Aprobación por el Comité de Tecnologías de la Información

###### Acuerdo de aprobación por el Comité de Tecnologías de la Información

Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.


##### 6.3 Aprobación por la Junta Directiva del Inder

###### Acuerdo de aprobación por Junta Directiva

Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.

#### 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica TI		

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b> <b>Política: Administración de Riesgos</b>	
	Código: PL-TI-003 Versión 2.0	Fecha de vigencia: 02/03/2011 Fecha de última actualización: 30/06/2017

## 1. Objetivo

1.1 Reducir el impacto de los riesgos de TI que puedan afectar los procesos del negocio, por medio de la identificación, análisis, evaluación y tratamiento de los mismos.

## 2. Alcance

2.1 Esta política aplica para todos aquellos riesgos propios de los procesos y activos de Tecnologías de la Información.

## 3. Responsables

3.1 Auditoría Interna: Fiscalizar el cumplimiento de las medidas para la gestión de riesgos

3.2 Tecnologías de la Información: Administrar, identificar y monitorear los riesgos asociadas a TI.

## 4. Pautas

4.1 Tecnologías de la Información debe definir el alcance de la administración de riesgos de TI, definiendo cuáles serán los activos tecnológicos (aplicaciones e infraestructura) y los procesos que se incluirán dentro del mismo.

4.2 El proceso de Administración de Riesgos de Tecnologías de Información debe estar alineado a las metas y objetivos de Tecnologías de la Información.

4.3 El apetito y la tolerancia de riesgo de Tecnologías de la Información debe ser aprobados por la Gerencia General del Inder.


4.4 Es responsabilidad de Tecnologías de la Información ejecutar evaluaciones de riesgos de TI en forma periódica.

4.5 Tecnologías de la Información debe documentar un catálogo de riesgos de Tecnologías de Información, el cual debe ser formalmente aprobado por el Comité de TI.

4.6 El catálogo de riesgos debe revisarse/actualizarse al menos una vez al año o cuando existan cambios significativos en la organización, procesos o controles de Tecnologías de la Información. Es responsabilidad de TI asegurar la ejecución de esta tarea.

4.7 Los criterios de evaluación de los riesgos de Tecnologías de la Información deben ser revisados/actualizados al menos una vez o cuando existan cambios significativos en la organización, procesos o controles de Tecnologías de la Información.

4.8 Para el cálculo de los valores de impacto y probabilidad debe utilizarse una escala de valoración de al menos 3 niveles (Bajo, Medio, Alto) que se encuentre alineado a las directrices brindadas por Auditoría Interna.

	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b>	
	<b>Política: Administración de Riesgos</b>	
	Código: PL-TI-003	Fecha de vigencia: 02/03/2011
	Versión 2.0	Fecha de última actualización: 30/06/2017

## 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

## 6. Aprobación

### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

### 6.2 Aprobación por el Comité de Tecnologías de la Información

<b>Acuerdo de aprobación por el Comité de Tecnologías de la Información</b>	Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.
---	--

### 6.3 Aprobación por la Junta Directiva del Inder.

<b>Acuerdo de aprobación por Junta Directiva</b>	Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.
--	--

## 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica T.I		



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Seguridad de la Información

Código: PL-TI-004

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

### 1. Objetivo

1.1 Establecer la dirección y el soporte de Seguridad de la Información de acuerdo a los requerimientos del Inder, las leyes y regulaciones respectivas.

### 2. Alcance

5.1 Esta política es aplicable a todos los funcionarios del Inder, terceros y usuarios de los recursos de tecnología de información, incluyendo a todos los niveles de la estructura organizacional del Inder.

### 3. Responsables

3.1 Administración Superior: Apoyar la Gestión de Seguridad de la Información y los lineamientos establecidos en esta política.

3.2 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.

3.3 Comité de TI: Actuar en relación con sus funciones con respecto a productos de esta política.

3.4 Tecnologías de la Información: Establecer directrices para la gestión de la Seguridad de la Información del Inder.

3.5 Funcionarios, terceros y usuarios: Conocer y aplicar lo estipulado en esta política.

### 4. Pautas

4.1 Tecnologías de la Información debe asegurar que los objetivos y estrategias de la Seguridad de la Información del Inder se encuentren alineados con el Plan Estratégico Institucional.

4.2 Tecnologías de la Información debe promover la implementación de las normas de seguridad necesarias de acuerdo a las tecnologías en uso, contando con el apoyo de las áreas involucradas.


4.3 Todos los funcionarios del Inder, terceros y usuarios de los activos de información deben utilizar los recursos de acuerdo con los derechos que se les asignen de conformidad con sus funciones, así como conocer y cumplir las regulaciones en materia de Seguridad de la Información.

4.4 Todos los funcionarios del Inder, terceros y usuarios de los activos de información tienen la responsabilidad de reportar a la jefatura inmediata cualquier caso sospechoso que atente contra la Seguridad de la Información del Inder. La jefatura inmediata que recibe el reporte debe remitirlo a Tecnologías de la Información y este elevarlo al Comité de TI.

4.5 Toda la información del Inder, contenida en papel o medios de almacenamiento extraíbles, se debe guardar en gabinetes seguros, no quedando desatendidos en ningún momento o a la vista de personas no autorizadas en los escritorios de los funcionarios.

4.6 Al finalizar la jornada laboral o cuando el funcionario se retire del Inder, debe asegurarse que ningún documento con información sensible para el Inder quede al alcance de personas no autorizadas.

4.7 Capital Humano, en conjunto con el Comité de TI y Tecnologías de la Información, deben identificar y recomendar a la Gerencia General las necesidades de concienciación y capacitación del personal del Inder en temas de Seguridad de la Información. La implementación de esta pauta se detalla en la [Política de Concienciación y Capacitación](#).

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b> <b>Política: Seguridad de la Información</b>	
	Código: PL-TI-004 Versión 2.0	Fecha de vigencia: 02/03/2011 Fecha de última actualización: 30/06/2017

- 4.8 Capital Humano, en conjunto con el Comité de TI, deben definir las campañas de capacitación en los temas identificados.
- 4.9 Tecnologías de la Información debe establecer los mecanismos de identificación de incidentes de seguridad de la información y dar el seguimiento necesario para su solución, esto alineado con lo establecido en la [Política de Administración de Incidentes](#).
- 4.10 Tecnologías de la Información es responsable por la elaboración del análisis de vulnerabilidades y riesgos en la plataforma tecnológica, así como la realización de evaluaciones externas sobre la misma al menos una vez al año, alineado con la [Política de Administración de Vulnerabilidades y Amenazas](#).
- 4.11 Capital Humano será responsable de desarrollar y gestionar los documentos necesarios de entrega al personal de primer ingreso, en materia de Seguridad de la Información.
- 4.12 Tecnologías de la Información debe promover la asociación e integración con grupos especialistas en temas de seguridad, así como también establecer la coordinación con apropiadas autoridades que fortalezcan la gestión de Seguridad de la Información.
- 4.13 Asuntos Jurídicos, en conjunto con el Comité de TI, deben establecer los acuerdos de confidencialidad requeridos con las diferentes instancias que requieren intercambio de información institucional, considerando funcionarios internos y terceros.

## 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

## 6. Aprobación

6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información.

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

6.2 Aprobación por el Comité de Tecnologías de la Información

<b>Acuerdo de aprobación por el Comité de Tecnologías de la Información</b>	Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.
---	--

6.3 Aprobación por la Junta Directiva del Inder

<b>Acuerdo de aprobación por Junta Directiva</b>	Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.
--	--

## 7. Historial de revisiones



## TECNOLOGIAS DE LA INFORMACIÓN Política: Seguridad de la Información

Código: PL-TI-004

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Clasificación de la Información

Código: PL-TI-005

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

### 1. Objetivo

1.1 Clasificar la información en el Inder para su apropiada manipulación.

### 2. Alcance

2.1 Esta política es aplicable a todos los funcionarios del Inder, terceros y usuarios de los recursos de tecnología de información, incluyendo a todos los niveles de la estructura organizacional del Inder.

### 3. Responsables

3.1 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.

3.2 Dueños de los datos: Identificar y clasificar la información, con el fin de asegurar que reciba un apropiado nivel de protección según su sensibilidad y criticidad, de acuerdo con la metodología establecida por TI.

3.3 Comité de TI: Actuar en relación con sus funciones con respecto a lo estipulado en esta política.

3.4 Tecnologías de la Información: Liderar el proceso de clasificación de la información.

3.5 Funcionarios, terceros y usuarios: Conocer y aplicar lo estipulado en esta política.

### 4. Pautas

4.1 La información debe ser clasificada en función de su valor, sensibilidad y criticidad para el Inder, con el fin de determinar el grado de protección requerida al ser manipulada.

4.2 Tecnologías de la Información debe definir un método para la clasificación de la información donde se definan las categorías a utilizar. Para esta definición se deben tomar en cuenta las diferentes Direcciones del Inder.

4.3 El método de clasificación de la información debe considerar información impresa o digital, independientemente del tipo de almacenamiento o medio de transferencia.

4.4 Tecnologías de la Información en una labor conjunta con las Direcciones del Inder, deben definir revisiones periódicas del método de clasificación de la información.

4.5 Tecnologías de la Información debe desarrollar los procedimientos establecidos para la revisión del método de clasificación de la información, los cuales deben incluir la valoración de las necesidades del negocio para compartir y restringir la información, las obligaciones legales en caso de que existan y el nivel de impacto asociado.

4.6 Toda información clasificada debe ser rotulada. La etiqueta debe reflejar su clasificación. Esto aplica para reportes impresos y en pantalla, medios de almacenamiento (cintas magnéticas, discos, llaves mayas), mensajes electrónicos y archivos transferidos.

4.7 Los dueños de los documentos impresos, digitalizados y electrónicos, así como las personas que los manipulen, son responsables de mantenerlos seguros de acuerdo al método de clasificación definido.



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Clasificación de la Información

Código: PL-TI-005

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

4.8 Los acuerdos con otras organizaciones que compartan información con el Inder, deben incluir procedimientos para identificar la clasificación de dicha información e interpretar la marca de clasificación de otras organizaciones.

4.9 Información sensible del Inder no debe encontrarse en mensajes de voz internos o externos o dispositivos de almacenamiento externo, salvo casos en los que sea estrictamente necesario y justificados.

### 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

### 6. Aprobación

6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

6.2 Aprobación por el Comité de Tecnologías de la Información

#### Acuerdo de aprobación por el Comité de Tecnologías de la Información

Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.


6.3 Aprobación por la Junta Directiva del Inder

#### Acuerdo de aprobación por Junta Directiva

Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.

### 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba			

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b> <b>Política: Uso de Recursos Tecnológicos</b>	
	Código: PL-TI-006 Versión 2.0	Fecha de vigencia: 02/03/2011 Fecha de última actualización: 30/06/2017

## 1. Objetivo

1.1 Proteger y hacer uso adecuado de los recursos tecnológicos del Inder.

## 2. Alcance

2.1 Esta política es aplicable a todos los funcionarios del Inder, terceros y usuarios de los recursos de tecnología de información, incluyendo a todos los niveles de la estructura organizacional del Inder.

## 3. Responsables

3.1 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.

3.2 Comité de TI: Actuar en relación con sus funciones con respecto a productos de esta política.

3.3 Funcionarios, terceros y usuarios: Conocer y aplicar lo estipulado en esta política.

3.4 Tecnologías de la Información: Proveer los mecanismos necesarios para la adecuada utilización de los recursos tecnológicos.

## 4. Pautas

4.1 El Inder debe brindar a sus funcionarios los equipos de cómputo y recursos tecnológicos necesarios para el cumplimiento de sus funciones. Estos recursos deben ser funcionales y contar con las características necesarias para suplir las necesidades del negocio y el desempeño de las actividades diarias.

4.2 Tecnologías de la Información: debe definir los requerimientos para el mantenimiento preventivo y correctivo de los equipos tecnológicos, así como de los controles para su implementación y velar por su cumplimiento.

4.3 Tecnologías de la Información es responsable de realizar las pruebas de funcionalidad e integridad que correspondan a los equipos tecnológicos.

4.4 Es responsabilidad de Tecnologías de la Información y del Comité de TI definir e informar acerca del software y hardware autorizado, estableciendo los mecanismos respectivos para instituir su operatividad. Esta definición debe estar alineada con los objetivos estratégicos del Inder.

4.5 Auditoría Interna debe llevar a cabo revisiones periódicas del software instalado. En caso de que se detecte la presencia de software no autorizado, la Auditoría debe investigar y recomendar lo que corresponda.

4.6 Todo equipo de cómputo propiedad del Inder debe contar con el software oficial de antivirus, el cual debe ser actualizado de forma periódica y es el único que se puede utilizar para este propósito.

4.7 Tecnologías de la Información debe establecer los lineamientos a seguir con respecto a la recepción de archivos y software provenientes de redes externas, correo electrónico o cualquier otro medio.

4.8 Los equipos de cómputo deben estar asignados a un funcionario, quien debe velar por el buen estado del mismo, así como de la demás infraestructura tecnológica que éste utiliza, asegurando que se les preste el oportuno y cuidadoso mantenimiento, así como que se realicen las pruebas de funcionalidad que correspondan.



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Uso de Recursos Tecnológicos

Código: PL-TI-006

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

- 4.9 Es responsabilidad de cada funcionario apagar los equipos tecnológicos asignados al finalizar su jornada laboral o durante periodos de inactividad, salvo casos en los que sea estrictamente necesario mantenerlos funcionando.
- 4.10 Está prohibida la descarga, instalación, implementación o uso de software no autorizado y/o sin licenciamiento.
- 4.11 En caso de funcionarios externos, que por sus labores necesiten hacer uso de la red o recursos tecnológicos del Inder con equipos de su propiedad, la Jefatura responsable de los trabajos a realizar debe solicitar a Tecnologías de la Información la revisión de las herramientas de antivirus y sistema operativo debidamente parchado, antes de que dicho funcionario tenga acceso a la red o recursos requeridos.
- 4.12 Los funcionarios deben seguir el proceso de verificación de virus definido por Tecnologías de la Información antes de proceder a la lectura de la información obtenida de fuentes externas en cualquier medio electrónico o de almacenamiento (discos flexibles, CD's, DVD's, Cintas magnéticas, Memory Sticks, llaves mayas) o archivos adjuntos al correo electrónico.
- 4.13 La computadora asignada a los funcionarios del Inder debe estar configurada de forma que se requiera ingresar el nombre de usuario y contraseña para salir del modo protector de pantalla, y debe ser bloqueada después de un intervalo de tiempo de inactividad definido
- 4.14 El funcionario debe bloquear la computadora cuando ésta se encuentra desatendida, con el fin de evitar el acceso no autorizado.
- 4.15 Los usuarios deberán abstenerse de fumar, comer o beber cerca de cualquier equipo tecnológico.
- 4.16 Tecnologías de la Información regulará el uso de archivos tales como: música, video y fotografías en las computadoras de escritorio y portátiles del Inder.
- 4.17 Los usuarios no deben ensayar o implementar redes locales en redes internas de comunicación o conexiones de cableado y tarjetas de red sin ser aprobados por Tecnologías de la Información.

### **Teléfonos:**

- 4.18 Cuando se utilice un teléfono, especialmente un altavoz o teléfono de uso compartido, para discutir cualquier información, los funcionarios deben asegurarse de no proveer detalles de datos sensibles del Inder.
- 4.19 Durante una conferencia telefónica, el funcionario debe procurar que únicamente individuos autorizados se encuentran conectados.
- 4.20 Cuando un usuario requiera de un cambio en los privilegios de llamadas, lo debe solicitar mediante una nota aprobada por la Jefatura inmediata y el visto bueno del Departamento Administrativo. La nota debe indicar la justificación del cambio. Si el cambio es aprobado se comunica al Tecnologías de la Información el cual procede con la solicitud.
- 4.21 TI es el responsable de extender los reportes de las extensiones telefónicas los primeros cinco días hábiles de cada mes a la Presidencia Ejecutiva. El informe visualizará las veinte extensiones con mayor duración en tiempo y costo y que sobrepasen los 5 minutos.

### **Fotocopiadoras, impresoras y faxes:**



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Uso de Recursos Tecnológicos

Código: PL-TI-006

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

- 4.22 Las fotocopiadoras, faxes e impresoras deben ubicarse en áreas de acceso restringido, donde no se exponga la integridad de los datos que por esos medios se procesan.
- 4.23 La información que no deba ser fotocopiada deberá indicarlo explícitamente, según lo estipulado en la [Política de Clasificación de la Información](#).
- 4.24 Todo el material de desecho o sobrantes que se genera durante el proceso de fotocopiado, impresión y transmisión de información del Inder, debe ser destruido según lo estipulado en la [Política de Manipulación y Destrucción de Datos](#).
- 4.25 Los equipos de fax no deben ser desatendidos mientras información del Inder está siendo transmitida.

### 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

### 6. Aprobación

6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

6.2 Aprobación por el Comité de Tecnologías de la Información


<b>Acuerdo de aprobación por el Comité de Tecnologías de la Información</b>	Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.
---	--

6.3 Aprobación por la Junta Directiva del Inder

<b>Acuerdo de aprobación por Junta Directiva</b>	Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.
--	--

### 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b> <b>Política: Administración de Cuentas de Usuario y Contraseñas</b>	
	Código: PL-TI-007	Fecha de vigencia: 02/03/2011
	Versión 4.0	Fecha de última actualización: 30/06/2017

## 1. Objetivo

- 1.1 Administrar adecuadamente las cuentas de usuarios y contraseñas de acceso a los sistemas y aplicaciones por parte de funcionarios y terceros en el Inder, con el fin de impedir el acceso a los servicios o equipos del Inder a personas no autorizadas.

## 2. Alcance


- 2.1 Esta política es aplicable a todos los funcionarios del Inder, terceros y usuarios de los recursos de tecnología de información, incluyendo a todos los niveles de la estructura organizacional del Inder.

## 3. Responsables

- 3.1 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.
- 3.2 Tecnologías de la Información: Gestionar las credenciales que serán utilizadas por los usuarios en la red del dominio Inder.
- 3.3 Unidades Administrativas Responsables: Gestionar las credenciales que serán utilizadas por los usuarios en los sistemas informáticos del Inder.
- 3.4 Funcionarios, terceros y usuarios: Conocer y aplicar lo estipulado en esta política.


## 4. Pautas

- 4.1 Todo usuario que ingrese a la red del Inder debe hacerlo mediante una cuenta de acceso propia gestionada por Tecnologías de la Información.
- 4.2 Todo usuario que ingrese a los sistemas de información del Inder debe hacerlo mediante una cuenta de acceso propia gestionada por la Unidad Administrativa Responsable.
- 4.3 Cada usuario es responsable de las transacciones que sean realizadas bajo su cuenta de usuario, tanto en el dominio de la red Inder, como en los sistemas de información que le sean asignados.
- 4.4 Las contraseñas a los sistemas de información e ingresos a la red del dominio Inder no deben ser reutilizadas en sitios de Internet como correos externos o cualquier otro sitio que solicite clave de ingreso.
- 4.5 Las contraseñas no pueden ser compartidas entre usuarios. Queda bajo responsabilidad del usuario dueño de la contraseña, el uso indebido de la misma.
- 4.6 Las contraseñas no se deben portar por escrito y deben ser totalmente confidenciales, de tal forma que no puedan ser accedidas por otros funcionarios o por personas ajenas al Inder (por ejemplo, en una carpeta del escritorio, en la pantalla del equipo o archivos digitales).
- 4.7 Todo usuario deberá hacer el cambio periódico de su contraseña, dependiendo de las características definidas en el sistema de información, red y correo electrónico.
- 4.8 Tanto la contraseña inicial de la cuenta de usuario de dominio de la red entregada por Tecnología de Información, como la contraseña inicial de la cuenta de los Sistemas de Información entregada por las Unidades Administrativas dueñas de los sistemas, deben ser cambiadas inmediatamente, como primera actividad de interacción con el sistema. Si esta actividad no es realizada en el transcurso de


 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b> <b>Política: Administración de Cuentas de Usuario y Contraseñas</b>	
	Código: PL-TI-007	Fecha de vigencia: 02/03/2011
	Versión 4.0	Fecha de última actualización: 30/06/2017

tres días, la misma deberá ser bloqueada. Así mismo para la generación de la nueva contraseña, el usuario debe tener en cuenta las pautas establecidas en esta política.

- 4.9 Las contraseñas no pueden ser guardadas en cache, es decir, no es permitido habilitar el recordatorio de contraseñas que viene implementado en algunas páginas de Internet, correo electrónico y sistemas de información.
- 4.10 Todo usuario es responsable de reportar inmediatamente las deficiencias de seguridad que observe en los sistemas de información, o en la red Inder, tanto a su Coordinador de Área o Jefe, como al personal de Tecnología de Información.
- 4.11 Tecnología de Información es responsable de la creación, modificación y suspensión de las cuentas de usuario de red o dominio institucional, así como la revisión periódica de cuentas inactivas para tomar las acciones respectivas sobre ellas.
- 4.12 Las Unidades Administrativas serán responsables de la creación, modificación y suspensión de las cuentas de usuario de los sistemas de información, así como la revisión periódica de cuentas inactivas para tomar las acciones respectivas sobre ellas.
- 4.13 Las cuentas y contraseñas de acceso a los sistemas de información, y dominio de la red del Inder únicamente serán entregadas al usuario correspondiente, utilizando mecanismos seguros para tal fin.
- 4.14 El nombre de la cuenta de usuario a los sistemas de información, o dominio de red institucional debe de ser única para cada usuario. Se deberán crear conforme al siguiente estándar:
- 4.14.1 La asignación y conformación de cuentas de usuarios para la red o dominio institucional y sus servicios, deberá considerar los siguientes elementos: La primera letra del nombre y el primer apellido.  
Ejemplo:  
Cvillalobos (Cecilia Villalobos)  
Gespinoza (Gustavo Espinoza)
- 4.14.2 Si se presentara el caso, que dos personas tuvieran la misma letra inicial y el mismo apellido se deberá agregar al final la primera letra del segundo apellido o agregar un número, para poder distinguirlos.  
Ejemplo:  
cvillalobos (Cecilia Villalobos)  
cvillalobosg ó cvillalobos1 (Carmen Villalobos García)
- 4.15 Los permisos y privilegios de acceso de cada usuario a los sistemas y los datos que éstos puedan acceder, deben estar alineados con las necesidades del negocio y adecuados para funciones que el usuario va a desempeñar sobre el sistema de información.
- 4.16 Tecnología de Información en coordinación con los Directores de cada área o Departamento, son los encargados de definir y crear los perfiles de usuarios. Asimismo, deben conceder diferentes niveles de acceso a estos perfiles y roles, según lo requieran las funciones laborales de cada usuario.
- 4.17 La lista de privilegios de cada perfil debe estar documentada, y se deberán identificar las excepciones, actualizaciones o cambios que se realicen a las mismas. Lo anterior bajo la supervisión y coordinación con cada Director.

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b>	
	<b>Política: Administración de Cuentas de Usuario y Contraseñas</b>	
	Código: PL-TI-007	Fecha de vigencia: 02/03/2011
Versión 4.0	Fecha de última actualización: 30/06/2017	

- 4.18 Todo usuario debe velar por que la definición de la contraseña de sus cuentas de usuario, sean lo más seguras posibles, para lo cual deberán cumplir con al menos las siguientes características:
- 4.18.1 Las contraseñas no podrán tener una longitud menor a ocho dígitos. No se deben utilizar espacios en blanco.
  - 4.18.2 Las contraseñas deben contener tanto caracteres alfabéticos como numéricos.
  - 4.18.3 Las contraseñas deben contener al menos cuatro caracteres distintos entre sí.
  - 4.18.4 La cuenta de usuario y la contraseña deben de ser diferentes entre sí.
  - 4.18.5 El usuario no podrá repetir ninguna de las últimas dos contraseñas utilizadas anteriormente.
- 4.19 Los recursos tecnológicos que se consideren críticos para el Inder, deberán contener contraseñas con un nivel más alto de complejidad con relación a los aspectos mencionados en el punto anterior. Así mismo, sólo Tecnología de Información custodiará dichas contraseñas y los administradores serán los únicos que tendrán acceso para hacer uso de las mismas.
- 4.20 Los equipos críticos son todos aquellos que están ligados a el dominio Inder y la red institucional y contemplarán el Sistema de Prevención de Riesgos - IPS, el muro de fuego - Firewall, el Administrador de Contenidos - Gate Gateway, y la Consola de Antivirus Institucional; los cuales nos resguardan tanto de las amenazas internas como externas.
- 4.21 Todos los dispositivos o recursos críticos deberán poseer una contraseña o password, de índole complejo la cual deberá ser definida por la encargada de Tecnologías de la información, para lo cual deberán cumplir con al menos las siguientes características:
- 4.21.1 Las contraseñas no podrán tener una longitud menor a ocho dígitos. No se deben utilizar espacios en blanco.
  - 4.21.2 Las contraseñas deben contener caracteres especiales, caracteres alfabéticos y caracteres numéricos.
  - 4.21.3 Las contraseñas deben contener al menos cinco caracteres distintos entre sí.
  - 4.21.4 La cuenta de usuario y la contraseña deben de ser diferentes entre sí.
  - 4.21.5 No se podrán repetir ninguna de las últimas cinco contraseñas utilizadas anteriormente.
- 4.22 Para el manejo de las contraseñas generadas para dichos equipos, se tomarán en cuenta los siguientes puntos:
- 4.22.1 Las contraseñas y los nombres de las cuentas críticas a las que pertenecen, serán resguardadas adecuadamente en un sobre membretado y depositadas en un lugar seguro determinado por Tecnología de Información.
  - 4.22.2 La utilización de las contraseñas críticas será registrada, documentando las causas que determinaron su uso, así como las actividades que se efectúan con la misma.

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b>	
	<b>Política: Administración de Cuentas de Usuario y Contraseñas</b>	
	Código: PL-TI-007	Fecha de vigencia: 02/03/2011
Versión 4.0	Fecha de última actualización: 30/06/2017	

- 4.22.3 Cada contraseña se renovará una vez utilizada y se definirá un periodo luego del cual, la misma será renovada en caso que no haya sido utilizado nunca.
- 4.23 Si se detecta que una contraseña es utilizada por una persona distinta al dueño, se procederá a la denegación de acceso a los sistemas o al dominio de la red del Inder, para evitar poner en riesgo la seguridad y la integridad de la información.
- 4.24 Durante la instalación de los dispositivos que son adquiridos por el Inder (por ejemplo, equipos de red y servidores), se deben cambiar las contraseñas por defecto del fabricante.
- 4.25 Para cambios en las contraseñas, el Jefe de cada Unidad Administrativa del Inder debe realizar la solicitud expresa a Tecnología de Información.
- 4.26 Las jefaturas de cada área serán responsables por la revisión periódica de las cuentas de usuario y privilegios otorgados a los funcionarios de su departamento.
- 4.27 La jefatura de cada Unidad Administrativa será responsable de notificar a Tecnología de Información acerca de la contratación de cualquier funcionario en su área. Éste deberá enviar por escrito el nombre del usuario, fecha de ingreso, descripción de trabajo e información o sistema que necesita acceder para realizar sus labores, y el tiempo durante el cual realizará esas labores, aunque sean o no por tiempo determinado.
- 4.28 Los Coordinadores de Área o Jefes deberán notificar por escrito a Capital Humano acerca de la suspensión o eliminación de los derechos de acceso de aquellos usuarios que se encuentren: de vacaciones, incapacidades, permisos o suspensión de sus funciones.
- 4.29 Será responsabilidad del Capital Humano notificar a Tecnología de Información y a las Unidades Administrativas responsables de los sistemas de información acerca de las situaciones mencionadas anteriormente, con el fin de revocar sus derechos de acceso, así como proceder con la revisión de documentos, archivos, directorios o recursos, para disponer de ellos o eliminarlos.
- 4.30 Capital Humano debe realizar la notificación al menos 3 días hábiles después de haberse presentado alguna de las situaciones antes mencionadas.
- 4.31 Tecnología de Información le concederá acceso temporal a un usuario cuando la jefatura inmediata del área al que éste pertenezca se lo pida por escrito. El acceso adicional será removido en cuanto el usuario termine las labores para las cuales necesitaba este acceso.


## 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

## 6. Aprobación

6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b> <b>Política: Administración de Cuentas de Usuario y Contraseñas</b>	
	Código: PL-TI-007	Fecha de vigencia: 02/03/2011
	Versión 4.0	Fecha de última actualización: 30/06/2017

## 6.2 Aprobación por el Comité de Tecnologías de la Información

<b>Acuerdo de aprobación por el Comité de Tecnologías de la Información</b>	Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.
---	--

## 6.3 Aprobación por la Junta Directiva del Inder

<b>Acuerdo de aprobación por Junta Directiva</b>	Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.
--	--

## Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Xiomara Castillo	Encargada Unidad de Tecnología	28 enero 2015	Cambio recomendado en Informe CG1-2013-TI, página 31.
3.0	Xiomara Castillo	Encargada Unidad de Tecnología	29 agosto 2016	Cambio recomendado según nota de la Gerencia General GG-430-2016.
3.0	Dixon Alvarez Valverde	TI- Gerencia General	5 abril 2016	Se solicita revisión según nota A-GG-029-2016 y remisión de documentos GG-430-2016, para ajustar la política acorde al lineamiento emitido en la circular N° 017-2015
4.0	Tecnologías de Información Manuel Montero Ureña	Revisión y Ajustes.	30 agosto 2016	Se modifica la pauta 4.3, 4.7, 4.10, 4.11, 4.13, 4.14 4.19 y 4.25, 4.27, se agregan las pautas 4,20 y 4,21 solicitadas y se ajusta la política acorde al lineamiento emitido en la circular N° 017-2015.



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Uso del Correo Electrónico

Código: PL-TI-008

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

### 1. Objetivo

1.1 Usar adecuadamente, de forma segura y eficiente el servicio de correo electrónico que el Inder brinda a sus funcionarios.

### 2. Alcance

2.1 Esta política es aplicable a todos los funcionarios del Inder, terceros y usuarios de los recursos de tecnología de información, incluyendo a todos los niveles de la estructura organizacional del Inder.

### 3. Responsables

3.1 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.

3.2 Jefaturas inmediatas: Velar por el cumplimiento de lo estipulado en esta política.

3.3 Tecnologías de la Información: Administrar el servicio de correo electrónico.

3.4 Funcionarios, terceros y usuarios: Conocer y aplicar lo estipulado en esta política.

### 4. Pautas

4.1 Todos los funcionarios del Inder y terceros que requieran del servicio de correo electrónico, recibirán una cuenta bajo el dominio “@inder.go.cr”.

4.2 Se debe definir un estándar para la generación de nombres de cuentas de correo.

4.3 Todas las cuentas de correo configuradas deben estar asociadas a un único usuario específico, siendo éstas personales e intransferibles.

4.4 Se debe definir el tamaño máximo de los correos electrónicos que se envían y se reciben, considerando tanto el cuerpo del mensaje como los archivos adjuntos que se añadan, de conformidad con las necesidades de cada Unidad Administrativa.

4.5 Cada cuenta de correo tendrá asociada una clave de acceso o contraseña para acceder al contenido de la misma. Dicha contraseña es de uso personal y confidencial.

4.6 Es responsabilidad de todos los usuarios de este servicio hacer un uso responsable y adecuado del mismo, en el contexto estricto de las actividades laborales asignadas por el Inder y para el fortalecimiento del flujo de información interna.

4.7 El comportamiento de todos los usuarios de este servicio debe apegarse a los valores éticos y morales, a las buenas costumbres y estándares de conducta socialmente aceptados, de tal forma que no se dañe la integridad moral de un tercero, interno o externo al Inder.

4.8 No se deben enviar mensajes con contenido ofensivo, amenazante, vulgar u obsceno, ni material que aliente la publicación de este tipo de mensajes. Está estrictamente prohibido intercambiar mensajes que representen acciones fuera de la ley nacional e internacional y que constituyan un riesgo para la Institución y para el sistema tecnológico del Inder.

4.9 El usuario debe acatar el lineamiento que dicte Tecnologías de la Información, en cuanto a la definición del cliente de correo a utilizar en las computadoras del Inder.



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Uso del Correo Electrónico

Código: PL-TI-008

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

- 4.10 Todo correo que sea enviado a través del sistema de correo electrónico del Inder, debe tener un asunto o “subject” claro y relacionado con el contenido del mismo.
- 4.11 El fondo utilizado para los correos electrónicos debe ser de color blanco y sin imágenes.
- 4.12 Todo correo que sea enviado por los usuarios del sistema de correo electrónico del Inder, debe contener una firma previamente configurada y automatizada, en la cual se destaquen los datos del remitente, así como una nota de confidencialidad. Tecnologías de la Información deberá suministrar la plantilla con el formato a utilizar en la firma del correo.
- 4.13 El correo electrónico del Inder es de uso personal y para uso estrictamente laboral. Este servicio no puede ni debe ser prestado o facilitado a terceros.
- 4.14 Se prohíbe a todos los usuarios del servicio de correo electrónico utilizar claves de acceso o cuentas de correo de otros usuarios o permitir a otros usuarios utilizar la cuenta de correo institucional.
- 4.15 Ningún usuario puede ver, copiar, alterar o destruir el contenido del correo electrónico o directorio de trabajo de otra persona sin el consentimiento explícito del dueño de la cuenta de correo.
- 4.16 El usuario no debe abrir correos electrónicos de dudosa procedencia, los cuales no han sido solicitados explícitamente, o que provengan de un remitente desconocido. Tampoco aquellos que no tengan un asunto (subject) específico, o que en su interior contengan un archivo adjunto no solicitado con una extensión considerada como peligrosa (por ejemplo: .com, .exe, .src, .bat, .cpl, .hta, .vbs, .cmd, .pif, .bmp, .gif; .scr o .hlp). El correo debe ser eliminado en caso de existir duda, de ser necesario el usuario puede consultar a TI.
- 4.17 Se prohíbe utilizar el correo electrónico para divulgar información propiedad del Inder, y considerada como confidencial, a terceras personas u organizaciones no autorizadas para recibirla, salvo en los casos que así se disponga expresamente.
- 4.18 Se prohíbe el uso del correo electrónico para actividades personales, con fines de lucro, envío de información con contenido pornográfico, música, videos (no relacionados con actividades laborales), cadenas o cualquier otro uso que involucre la masificación de mensajes de correo electrónico (spam), violación explícita de derechos de autor o violación a la privacidad, archivos de gran tamaño, material o contenido ofensivo o en contra de las buenas costumbres, sean morales, religiosas o culturales.
- 4.19 Se prohíbe el envío de cualquier tipo de cadenas de mensajes, así como la distribución de este tipo de información cuando no ha sido solicitada por el receptor del mensaje.
- 4.20 Queda totalmente prohibido el envío de correos masivos para fines no laborales, con excepción de las organizaciones sociales de la Institución, salvo las excepciones autorizadas por la Administración Superior o la normativa que regule dicha materia.
- 4.21 Se prohíbe intentar el envío de mensajes alterando la dirección electrónica del remitente para suplantar a terceros; identificarse como una persona ficticia o simplemente no identificarse. Además, se prohíbe intentar quebrantar las medidas de seguridad que soportan el entorno del servicio de correo electrónico Institucional.



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Uso del Correo Electrónico

Código: PL-TI-008

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

- 4.22 Al establecerse este servicio como un medio oficial de comunicación del Inder, los usuarios deben velar por la eficiencia de su utilización y por el máximo aprovechamiento del mismo en el cumplimiento de sus labores.
- 4.23 Se prohíbe el uso o instalación de cualquier programa o paquete para envío de correo electrónico, que no esté autorizado por Tecnologías de la Información y/o no cuente con las licencias correspondientes, incluyendo los adquiridos o descargados de Internet aún cuando sean gratuitos.
- 4.24 Los usuarios deben reportar inmediatamente, a su jefe inmediato o a Tecnologías de la Información, cualquier situación que pueda comprometer la seguridad y buen funcionamiento del sistema de correo electrónico, ya sea virus, modificación o pérdida de datos, sospecha de robo de claves y otras actividades conexas.
- 4.25 Es responsabilidad del usuario la administración de los mensajes descargados al computador asignado a éste.
- 4.26 El usuario debe revisar su cuenta de correo electrónico en el menor lapso de tiempo posible, de tal forma que descargue todos aquellos mensajes almacenados del servidor a su computador.
- 4.27 La administración de las cuentas del servicio de correo electrónico es competencia de TI.
- 4.28 Tecnologías de la Información dejará de prestar el servicio a aquel usuario que no cumpla con las políticas aquí establecidas, y siguiendo el debido proceso se tomarán las medidas administrativas correspondientes.
- 4.29 Tecnologías de la Información no se responsabiliza por la eliminación o errores en el proceso de almacenamiento o envío de mensajes, que sean causados por el usuario.
- 4.30 Tecnologías de la Información no se responsabiliza por la pérdida de información almacenada en los buzones de correo electrónicos, ya sea por el uso indebido del servicio por parte del usuario, o por daños en los servidores de cómputo.
- 4.31 El administrador del servicio de correo electrónico del Inder no podrá interceptar o editar mensajes de correo de ningún funcionario, salvo solicitud expresa del usuario o por requerimiento expreso de Autoridades Judiciales.
- 4.32 El administrador del servicio de correo electrónico del Inder debe garantizar la confiabilidad, disponibilidad e integridad del mismo, mediante la utilización de tecnologías, sistemas y aplicaciones adecuadas para estos fines.
- 4.33 A cada usuario se le asignará un buzón de correo, el cual tiene un tamaño definido por Tecnologías de la Información. En caso de que un buzón se quede sin espacio, se enviará un mensaje al usuario indicando la necesidad de borrar mensajes almacenados en el servidor de correo.
- 4.34 Tecnologías de la Información, como parte de las actividades rutinarias necesarias para la buena administración del servicio de correo electrónico, realizará al menos una vez al mes, actividades de mantenimiento sobre el servidor de correo electrónico, dentro de las cuales se incluirá la eliminación de correos, como medida de prevención para evitar la saturación de mensajes.



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Uso del Correo Electrónico

Código: PL-TI-008

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

### 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

### 6. Aprobación

#### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

#### 6.2 Aprobación por el Comité de Tecnologías de la Información

##### Acuerdo de aprobación por el Comité de Tecnologías de la Información

Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.

#### 6.3 Aprobación por la Junta Directiva del Inder

##### Acuerdo de aprobación por Junta Directiva

Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.

### 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Uso del internet

Código: PL-TI-009

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

### 1. Objetivo

1.1 Regular el uso del Internet en el Inder, para asegurar que las actividades que se realicen en la Web sean estrictamente relacionadas con las operaciones de la Institución.

### 2. Alcance

2.1 Esta política es aplicable a todos los funcionarios del Inder, terceros y usuarios de los recursos de tecnología de información, incluyendo a todos los niveles de la estructura organizacional del Inder.

### 3. Responsables

3.1 Administración Superior: Apoyar el cumplimiento de lo estipulado en esta política.

3.2 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.

3.3 Tecnologías de la Información: Administrar el servicio de internet.

3.4 Funcionarios, terceros y usuarios: Conocer y aplicar lo estipulado en esta política.

### 4. Pautas

4.1 Todo evento que se dé a través del uso del servicio de Internet, será administrado, monitoreado y regulado por TI, dicha Unidad reportará al Comité de TI cualquier desviación que se presente.

4.2 Los sitios de internet con charlas o redes sociales deben ser utilizados únicamente para fines laborales.

4.3 Las actividades que el usuario realice en internet no debe interferir ni distraerlo de sus funciones normales.

4.4 Al menos una vez al mes, Tecnologías de la Información monitoreará el servicio de internet, generando un reporte con el detalle del uso de este servicio. De existir cualquier anomalía se reportará al Comité de TI.

4.5 Los archivos obtenidos desde Internet deben ser revisados (filtrados) para detección de virus previo a ser descargados en cualquier computador.

4.6 En caso del mal uso comprobado del servicio de internet, las jefaturas inmediatas deben restringir o deshabilitar el uso de dicho servicio. Para esto, se debe enviar una solicitud justificada a Tecnologías de la Información con copia al funcionario involucrado.

4.7 Tecnologías de la Información es responsable de mantener disponibles los recursos tecnológicos que soportan el hospedaje de la página web del Inder.

4.8 La conexión a Internet debe realizarse por los medios autorizados por Tecnologías de la Información.

4.9 Las regulaciones de Internet se establecerán durante las 24 horas del día, los 7 días de la semana, de acuerdo a las funciones del puesto.



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Uso del internet

Código: PL-TI-009

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

- 4.10 Tecnologías de la Información debe asegurar que los usuarios conozcan los riesgos de seguridad asociados con el uso y acceso a Internet.
- 4.11 De suspenderse el servicio de Internet, Tecnologías de la Información debe realizar las acciones necesarias de comunicación con el proveedor de servicios para la habilitación pronta del mismo.
- 4.12 Se prohíbe terminantemente bajar música, películas, programas, juegos o cualquier otra aplicación que no tengan relación con las labores del Inder y que además perjudiquen el funcionamiento de la red y capacidad de almacenamiento de las máquinas.
- 4.13 Es responsabilidad de Tecnologías de la Información proveer herramientas automatizadas que permitan limitar a los usuarios de bajar programas de Internet sin la autorización previa.
- 4.14 Los accesos a Internet que se realicen con recursos informáticos del Inder serán registrados y monitoreados periódicamente. Si existe una duda razonable, respaldada por evidencia, para creer que un funcionario está haciendo mal uso de los recursos electrónicos o ha violado alguna de las políticas, se procederá a revisar el historial de acceso a Internet en el servidor de filtrado de contenido.
- 4.15 Ningún usuario podrá distribuir, acceder, guardar o imprimir materiales, fotografías o mensajes que no tengan relación con sus actividades dentro del Inder.
- 4.16 No se puede usar Internet para realizar actividades comerciales, personales o que violen la ley, tales como invadir la privacidad de terceros, dañar la propiedad intelectual de otro individuo u organización.
- 4.17 Ningún funcionario debe utilizar los recursos de Internet del Inder para propagar intencionalmente algún virus, troyano o aplicación maliciosa.
- 4.18 Está totalmente prohibido el ingreso a páginas de contenido pornográfico, violencia, racismo, descarga de programas que permitan realizar conexiones automáticas o visores de sitios clasificados como pornográficos y la utilización de los recursos para distribución o reproducción de este tipo de material, ya sea vía web o medios magnéticos.
- 4.19 Se prohíbe el uso de servicios de radio y televisión por Internet.
- 4.20 El establecimiento de conexiones directas entre sistemas y computadoras de organizaciones externas, vía Internet o cualquier otra red pública, está prohibido, a menos que esta conexión sea aprobada por Tecnologías de la Información y se instauren los mecanismos de seguridad necesarios para garantizar la seguridad de la información que maneja el Inder.
- 4.21 Los proveedores de servicios de redes y comunicaciones no deben hacer arreglos o actualizaciones completas de medios de transporte de datos, voz u otro sin antes haber obtenido la aprobación y supervisión por parte de personal de TI,

### 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b> <b>Política: Uso del internet</b>	
	Código: PL-TI-009 Versión 2.0	Fecha de vigencia: 02/03/2011 Fecha de última actualización: 30/06/2017

## 6. Aprobación

### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

### 6.2 Aprobación por el Comité de Tecnologías de la Información


<b>Acuerdo de aprobación por el Comité de Tecnologías de la Información</b>	Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.
---	--

### 6.3 Aprobación por la Junta Directiva del Inder

<b>Acuerdo de aprobación por Junta Directiva</b>	Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.
--	--

## 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b> <b>Política: Concienciación y Capacitación</b>	
	Código: PL-TI-010	Fecha de vigencia: 02/03/2011
	Versión 2.0	Fecha de última actualización: 30/06/2017

## 1. Objetivo

1.1 Concientizar y capacitar a los funcionarios del Inder en materia de Seguridad de la Información.

## 1. Alcance

2.1 Esta política es aplicable a todos los funcionarios del Inder, terceros y usuarios de los recursos de tecnologías de información, incluyendo a todos los niveles de la estructura organizacional del Inder.

## 2. Responsables

3.1 Administración Superior: Apoyar la Gestión de Seguridad de la Información por medio de los lineamientos establecidos en esta política.

3.2 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.

3.3 Capital Humano: Ejecutar el plan anual de concienciación y capacitación del Inder, incluyendo los temas mencionados en esta política.

3.4 Comité de TI: Actuar en relación con sus funciones con respecto a productos de esta política.

3.5 Tecnologías de la Información: Definir programas de capacitación y apoyar su implementación.

3.6 Funcionarios, terceros y usuarios: Conocer y aplicar lo estipulado en esta política.

## 3. Pautas

4.1 Tecnologías de la Información debe definir y establecer un programa y procesos de capacitación formal y periódico sobre temas de Seguridad de la Información para todos los usuarios de los sistemas de información y aplicativos del Inder. Este programa debe ser gestionado en conjunto con Capital Humano para que dicha Unidad lo ejecute.

4.2 Todos los funcionarios de la organización y terceros, en caso de ser requerido, deben recibir apropiados entrenamientos de concienciación y actualizaciones regulares en políticas y procedimientos en relación a sus funciones laborales.

4.3 Capital Humano con apoyo del Comité de TI es el encargado de gestionar periódicamente evaluaciones de las debilidades presentadas por los funcionarios de la Institución en temas relacionados con las Políticas de Tecnologías de la Información y Seguridad de la Información. Capital Humano deberá analizar los resultados de las evaluaciones con TI.

4.4 Se deberán definir o fomentar campañas masivas de concienciación necesarias para divulgar las políticas, utilizando por ejemplo afiches, pancartas, boletines, entre otros.

## 4. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Concienciación y Capacitación

Código: PL-TI-010

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

### 5. Aprobación

#### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

#### 6.2 Aprobación por el Comité de Tecnologías de la Información

##### Acuerdo de aprobación por el Comité de Tecnologías de la Información

Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.


#### 6.3 Aprobación por la Junta Directiva del Inder

##### Acuerdo de aprobación por Junta Directiva

Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.

### 6. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b> <b>Política: Auditoría y Monitoreo</b>	
	Código: PL-TI-011	Fecha de vigencia: 02/03/2011
	Versión 2.0	Fecha de última actualización: 30/06/2017

## 1. Objetivo

1.1 Auditar y monitorear los sistemas, la infraestructura de comunicación y redes en el Inder.

## 2. Alcance

2.1 Esta política es aplicable a todos los funcionarios del Inder, terceros y usuarios de los recursos de tecnología de información, incluyendo a todos los niveles de la estructura organizacional del Inder.

## 3. Responsables

3.1 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.

3.2 Funcionarios, terceros y usuarios: Conocer y aplicar lo estipulado en esta política.

## 4. Pautas

4.1 La planificación de auditorías y monitoreo del Inder, deben enfocarse en la evaluación de los sistemas y la aplicación de los procedimientos para los equipos relacionados con la infraestructura de red, servidores y equipo de cómputo en general.

4.2 Se debe monitorear el acceso a los recursos de cómputo y a la red utilizada por terceras partes, en apego a los acuerdos firmados con los mismos.

4.3 Se debe proveer información sobre protocolos, direccionamiento y conexiones de red al personal autorizado para la realización de las auditorías y monitoreo, de forma que puedan utilizar herramientas o aplicaciones que permitan ejecutar las labores respectivas en forma eficiente.

4.4 Se deben definir pistas de auditoría en los sistemas de software del Inder, de forma que se pueda analizar y dictaminar el estado de las actividades realizadas a través de los mismos.


4.5 Las opciones de bitácoras deben estar activas en la configuración de seguridad de los equipos y aplicativos críticos que lo permitan, siendo las mismas definidas a partir de un análisis que determine su relevancia, consumo de espacio físico e impacto en el rendimiento.

4.6 En caso de detectarse vulnerabilidades o fallos en la seguridad de los sistemas o de la infraestructura tecnológica, las mismas deberán ser reportadas a Tecnologías de la Información, a fin de evaluar el riesgo e impacto de los mismos y prevenir futuros inconvenientes.

4.7 Tecnologías de la Información debe definir e implementar los mecanismos necesarios para monitorear el uso adecuado de los recursos tecnológicos.

4.8 El proceso de auditoría, monitoreo y administración de sistemas informáticos debe respaldar la documentación (física o electrónica) referente a las evaluaciones, hallazgos y muestras realizadas durante el análisis de la información.

4.9 La efectividad del sistema de auditoría y monitoreo debe ser evaluada periódicamente por entes fiscalizadores externos y la Auditoría Interna, de conformidad a las disposiciones legales pertinentes.

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b>	
	<b>Política: Auditoría y Monitoreo</b>	
	Código: PL-TI-011	Fecha de vigencia: 02/03/2011
Versión 2.0	Fecha de última actualización: 30/06/2017	

## 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

## 6. Aprobación

### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

### 6.2 Aprobación por el Comité de Tecnologías de la Información

<b>Acuerdo de aprobación por el Comité de Tecnologías de la Información</b>	Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.
---	--

### 6.3 Aprobación por la Junta Directiva del Inder

<b>Acuerdo de aprobación por Junta Directiva</b>	Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.
--	--

## 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Seguridad Física y Ambiental

Código: PL-TI-012

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

### 1. Objetivo

- 1.1 Mantener la seguridad física y ambiental en las áreas sensibles del Inder, así como la protección de la infraestructura ubicada en estas áreas.

### 2. Alcance


- 2.1 Esta política es aplicable a todos los funcionarios del Inder, terceros y usuarios de los recursos de tecnología de información, incluyendo a todos los niveles de la estructura organizacional del Inder.

### 3. Responsables

- 3.1 Auditoría Interna y Unidades Administrativas: Velar por el cumplimiento de lo estipulado en esta política.
- 3.2 Tecnologías de la Información: Gestionar las medidas de seguridad física y ambiental para la protección de la infraestructura tecnológica.
- 3.3 Funcionarios, terceros y usuarios: Conocer y aplicar lo estipulado en esta política.

### 4. Pautas


- 4.1 Tecnologías de la Información, con apoyo de la Administración Superior, debe adoptar las medidas de seguridad necesarias para la ubicación y protección del equipo tecnológico, la central telefónica, los cuartos de comunicaciones y áreas afines, tomando en cuenta el área física, controles contra fuego, inundaciones, vandalismo, entre otras condiciones ambientales y físicas.
- 4.2 Servicios Generales debe identificar las áreas seguras dentro del Inder, utilizando rótulos, señales y placas, entre otros mecanismos que se consideren apropiados.
- 4.3 Las áreas donde se procesa información del Inder debe ser rotulada, con el fin de evitar el acceso de personas no autorizadas.
- 4.4 Servicios Generales debe desarrollar los controles necesarios para proteger a sus funcionarios contra amenazas naturales o producidas por el hombre.
- 4.5 Los funcionarios deben utilizar las áreas sensibles únicamente para los fines establecidos para las mismas.
- 4.6 Servicios Generales debe brindar la seguridad adecuada para el suministro del servicio eléctrico que evite interrupciones que afecten los equipos tecnológicos del Inder.
- 4.7 Tecnologías de la Información debe brindar la seguridad necesaria para el cableado de telecomunicaciones para evitar interrupciones dentro del Inder.
- 4.8 Se prohíbe el almacenamiento de material inflamable dentro de cualquier zona del Inder que no esté autorizada e identificada para dicho fin.
- 4.9 El Inder debe proteger en forma razonable los recursos tecnológicos de amenazas físicas y/o ambientales que se puedan presentar.

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b> <b>Política: Seguridad Física y Ambiental</b>	
	Código: PL-TI-012	Fecha de vigencia: 02/03/2011
	Versión 2.0	Fecha de última actualización: 30/06/2017

- 4.10 Se deben definir los procedimientos de mantenimiento para el equipo tecnológico del Inder, de manera que se asegure la disponibilidad e integridad de los mismos.
- 4.11 Para ingresar al cuarto de servidores se debe solicitar permiso a Tecnologías de la Información y llenar una bitácora para justificar el ingreso a dicha área.
- 4.12 Las personas ajenas a las áreas sensibles deben ser dirigidas por el personal de la misma área cuando, en forma autorizada, transiten en ella. Esto incluye a empleados de otras dependencias, consultores, familiares, proveedores y otros.
- 4.13 Se deben establecer controles de acceso físico a todas las áreas sensibles del Inder, tomando en cuenta procedimientos de identificación tanto para personal interno como externo.
- 4.14 Tecnologías de la Información en conjunto con las Unidades Administrativas del Inder, deben definir niveles de seguridad física y ambiental según la información administrada en cada área del Inder.
- 4.15 Todo funcionario, personas y empresas que prestan servicios profesionales y técnicos al Inder deben portar el carné asignado en un lugar visible.
- 4.16 Capital Humano es responsable de la creación, asignación y confección del carné de entrada a los funcionarios que lo requieran.
- 4.17 Si un funcionario pierde u olvida su carné, debe coordinar con Capital Humano para la confección de un nuevo carné temporal o permanente.
- 4.18 El ingreso y permanencia de personal externo en las áreas sensibles por efectos de tareas de mantenimiento, aseo o reparación de equipos deberá contar con la supervisión permanente de un funcionario del área autorizado.
- 4.19 Fuera del horario ordinario del Inder, el acceso a las áreas sensibles debe ser debidamente justificado con la Unidad Administrativa responsable de dichas áreas.
- 4.20 Todo equipo de cómputo o de comunicaciones que deba ser trasladado de un edificio a otro u oficina, debe tener la respectiva autorización de Tecnologías de la Información. Si el equipo requiere salir del Instituto, el personal de vigilancia debe solicitar la boleta respectiva y verificar que el equipo corresponda al autorizado en la boleta.
- 4.21 El personal de Seguridad y Vigilancia, debe revisar el contenido de toda maleta, bolsa, caja u otro que presente sospechas para prevenir la sustracción de componentes de equipos de cómputo o de información en medios magnéticos o físicos.
- 4.22 Está prohibido introducir al Inder elementos potencialmente peligrosos para la seguridad de las personas, los equipos de cómputo y de comunicaciones del Inder tales como armas o explosivos.
- 4.23 El personal de Vigilancia debe contar con dispositivos que permitan detectar elementos metálicos.

## 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b> <b>Política: Seguridad Física y Ambiental</b>	
	Código: PL-TI-012 Versión 2.0	Fecha de vigencia: 02/03/2011 Fecha de última actualización: 30/06/2017

## 6. Aprobación

### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

### 6.2 Aprobación por el Comité de Tecnologías de la Información


<b>Acuerdo de aprobación por el Comité de Tecnologías de la Información</b>	Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.
---	--

### 6.3 Aprobación por la Junta Directiva del Inder

<b>Acuerdo de aprobación por Junta Directiva</b>	Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.
--	--

## 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b> <b>Política: Administración de Amenazas y Vulnerabilidades</b>	
	Código: PL-TI-013	Fecha de vigencia: 02/03/2011
	Versión 2.0	Fecha de última actualización: 30/06/2017

## 1. Objetivo

1.1 Reducir los riesgos de explotación de vulnerabilidades técnicas y mitigar el efecto de las amenazas contra los sistemas de información y recursos tecnológicos del Inder.

## 2. Alcance

2.1 Esta política es aplicable para todos los equipos tecnológicos del Inder, así como también para todos los funcionarios Tecnologías de la Información.

## 3. Responsables

3.1 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.

3.2 Tecnologías de la Información: Gestionar las amenazas y vulnerabilidades de la plataforma tecnológica del Inder.

## 4. Pautas

4.1 Se debe llevar un inventario completo de los activos tecnológicos existentes en el Inder como requisito para la efectiva administración de vulnerabilidades técnicas.

4.2 Tecnologías de la Información debe definir y establecer las funciones y responsabilidades asociadas, incluyendo identificación y monitoreo de vulnerabilidades, análisis de riesgos, aplicación de parches y cualquier otra responsabilidad de coordinación requerida.

4.3 Tecnologías de la Información debe analizar la factibilidad y adquisición de herramientas orientadas a la búsqueda de vulnerabilidades técnicas. Dichas herramientas deberán tener la opción de ser actualizadas en forma periódica.

4.4 Cuando una vulnerabilidad ha sido detectada, Tecnologías de la Información debe identificar los riesgos asociados y las acciones a tomar.

4.5 Debe existir un proceso que detalle la administración de las actualizaciones y parches, definiendo los lineamientos a seguir para su prueba y posterior pase a la infraestructura en producción.


4.6 Se debe definir el proceso mediante el cual se monitoreará la efectividad en la administración de vulnerabilidades técnicas.

4.7 Tecnologías de la Información debe realizar revisiones periódicas en búsqueda de posibles amenazas y vulnerabilidades.

4.8 Tecnologías de la Información debe identificar las vulnerabilidades inherentes a sus sistemas de información e identificar las amenazas que podrían materializarlas.

## 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b> <b>Política: Administración de Amenazas y Vulnerabilidades</b>	
	Código: PL-TI-013	Fecha de vigencia: 02/03/2011
	Versión 2.0	Fecha de última actualización: 30/06/2017

## 6. Aprobación

### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

### 6.2 Aprobación por el Comité de Tecnologías de la Información


<b>Acuerdo de aprobación por el Comité de Tecnologías de la Información</b>	Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.
---	--

### 6.3 Aprobación por la Junta Directiva del Inder

<b>Acuerdo de aprobación por Junta Directiva</b>	Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.
--	--

## 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		

	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b> <b>Política: Manipulación y Destrucción de Datos</b>	
	Código: PL-TI-014 Versión 2.0	Fecha de vigencia: 02/03/2011 Fecha de última actualización: 30/06/2017

## 1. Objetivo

1.1 Garantizar el uso apropiado de toda la información clasificada como sensitiva o crítica, incluyendo acceso, transmisión y almacenamiento en todos los tipos de medios.

## 2. Alcance

2.1 Esta política es aplicable a todos los funcionarios del Inder, terceros y usuarios de los recursos de tecnología de información, incluyendo a todos los niveles de la estructura organizacional del Inder.

## 3. Responsables

3.1 Auditoría Interna: Fiscaliza el cumplimiento de lo estipulado en esta política.

3.2 Funcionarios, terceros y usuarios: Conocer y aplicar lo estipulado en esta política.

## 4. Pautas

4.1 Se considera propiedad del Inder toda aquella información generada por el Inder para uso interno y/o externo, para el conocimiento, uso y ejecución del trabajo diario de los funcionarios, sea generada o se encuentre la misma en cualquier medio, a saber, productos de papel, cintas magnéticas y dispositivos removibles,

4.2 La destrucción de los documentos textuales, electrónicos y digitalizados debe ser realizada en una forma precisa y transformada en material no legible, sea por desmenuzamiento, desmagnetización o incineración, de tal forma que la información no pueda ser obtenida por personal interno o terceras partes.

4.3 Ningún documento institucional debe ser eliminado por medios tradicionales o almacenado para reciclaje.

4.4 Es responsabilidad de Tecnologías de la Información realizar la destrucción de medios magnéticos.


4.5 En caso de desecho de documentos electrónicos y digitalizados que tengan carácter representativo o declarativo para el Inder, los usuarios deben eliminar el documento de su máquina y de la papelería de reciclaje.

4.6 Cuando un usuario cambia de equipo, Tecnologías de la Información debe establecer los lineamientos aplicables para el respaldo de la información almacenada.

4.7 La información generada por el procesamiento de datos de sistemas manuales o automatizados, será propiedad exclusiva del Inder.

4.8 Se prohíbe el uso o distribución de información del Inder para fines ilícitos (propios o para terceros). Es responsabilidad de todos los funcionarios o usuarios de información, utilizarla de manera adecuada y segura.

4.9 La manipulación de la información ya sea almacenamiento, destrucción, transmisión o generación, debe considerar la clasificación asignada para dicha información.

	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b>	
	<b>Política: Manipulación y Destrucción de Datos</b>	
Código: PL-TI-014	Fecha de vigencia: 02/03/2011	
Versión 2.0	Fecha de última actualización: 30/06/2017	

## 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

## 6. Aprobación

### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

### 6.2 Aprobación por el Comité de Tecnologías de la Información

<b>Acuerdo de aprobación por el Comité de Tecnologías de la Información</b>	Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.
---	--

### 6.3 Aprobación por la Junta Directiva del Inder

<b>Acuerdo de aprobación por Junta Directiva</b>	Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.
--	--

## 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		



## TECNOLOGÍAS DE LA INFORMACIÓN

### Política: Privacidad y Protección de la Información

Código: PL-TI-015

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

#### 1. Objetivo

1.1 Garantizar la privacidad y proteger la integridad de la información suministrada, creada, adquirida y almacenada por los funcionarios de Inder y terceros.

#### 2. Alcance

2.1 Esta política es aplicable a todos los funcionarios del Inder, terceros y usuarios de los recursos de tecnología de información, incluyendo a todos los niveles de la estructura organizacional del Inder.

#### 3. Responsables

3.1 Auditoría Interna: Fiscalizar por el cumplimiento de lo estipulado en esta política.

3.2 Funcionarios, terceros y usuarios: Conocer y aplicar lo estipulado en esta política.

#### 4. Pautas

4.1 Toda persona que ingrese a laborar al Instituto, como funcionario de este, debe firmar un acuerdo de confidencialidad que incluya puntos de privacidad y protección de la Información del Inder.

4.2 Para el intercambio de información entre instituciones y accesos a los sistemas del Inder, Tecnologías de la Información debe velar por que se firme un contrato de confidencialidad entre las partes que se vean involucradas.

4.3 Toda la información contenida en las bases de datos del Inder podrá ser accedida de manera restringida de acuerdo a los roles de los usuarios, acuerdos y privilegios establecidos entre las partes.

4.4 Los usuarios que posean acceso a las bases de datos del Inder solo podrán hacer uso de la información para la realización de sus labores y no podrán publicar, reproducir, trasladar ni ceder información sin autorización previa del Inder.

4.5 Toda información que se ingrese o se extraiga de las bases de datos del Inder, por sus usuarios o funcionarios, deberá hacerse a través de los procedimientos instituidos para tal fin, los cuales deben contar con los mecanismos de seguridad adecuados.

4.6 Todo funcionario debe garantizarse que ninguna otra persona haga uso de sus credenciales de acceso a los sistemas y servicios brindados por el Inder.

4.7 Todo usuario con acceso a la información del Inder debe utilizarla de acuerdo con los derechos que se les asignen de conformidad con sus funciones, así como conocer y cumplir las políticas y regulaciones en materia de Seguridad de la Información.

#### 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Privacidad y Protección de la Información

Código: PL-TI-015

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

### 6. Aprobación

#### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

#### 6.2 Aprobación por el Comité de Tecnologías de la Información

##### Acuerdo de aprobación por el Comité de Tecnologías de la Información

Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.

#### 6.3 Aprobación por la Junta Directiva del Inder

##### Acuerdo de aprobación por Junta Directiva

Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.

### 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		



## TECNOLOGÍAS DE LA INFORMACIÓN

### Política: Control de Virus y Software Malicioso

Código: PL-TI-016

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

#### 1. Objetivo

1.1 Asegurar la protección de la información y de la infraestructura tecnológica del Inder.

#### 2. Alcance

2.1 Esta política es aplicable a todos los funcionarios del Inder, terceros y usuarios de los recursos de tecnología de información, incluyendo a todos los niveles de la estructura organizacional del Inder.

#### 3. Responsables

3.1 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.

3.2 Unidades Administrativas: Velar por el cumplimiento de lo estipulado en esta política.

3.3 Tecnologías de la Información: Establecer los mecanismos para el control de virus y software malicioso.

3.4 Funcionario, terceros y usuarios: Velar por el cumplimiento de lo estipulado en esta política.

#### 4. Pautas

4.1 Los funcionarios deben seguir un proceso de verificación de virus antes de proceder a la lectura de la información obtenida de fuentes externas en cualquier medio electrónico de almacenamiento (discos flexibles, CD's, DVD's, cintas magnéticas, memorias extraíbles, discos externos, dispositivos USB) o correo electrónico.

4.2 En caso de funcionarios externos, que por sus labores necesiten hacer uso de la red del Inder con equipos de su propiedad, deberán contar con un software de antivirus debidamente licenciado.

4.3 El software de antivirus no puede ser deshabilitado, y la configuración del mismo no debe de ser alterada. Igualmente, la frecuencia del escaneo automático del software no debe ser modificada.

4.4 Está prohibido el uso de programas para descarga e intercambio de archivos. Asimismo, se prohíbe la descarga y ejecución de otros programas y documentos desde Internet o dispositivos móviles de índole no laboral tales como salvapantallas, música, videos, fotos, juegos, programas de broma y archivos con extensiones ejecutables.

4.5 Los usuarios deberán omitir y cancelar mensajes o solicitudes provenientes desde Internet, que comprometan instalar software en sus equipos.

4.6 No está permitida la conexión a la red de computadoras sin que su configuración sea revisada por Tecnologías de la Información siguiendo los lineamientos de seguridad establecidos.

4.7 Es responsabilidad de los usuarios tomar medidas razonables para prevenir el contagio de virus o la instalación de software malicioso. Las acciones provocadas por software que se encuentre instalado en sus equipos y que no haya sido instalado ni autorizado por Tecnologías de la Información serán responsabilidad del usuario. Cualquier requerimiento adicional por parte de un usuario para la instalación de un aplicativo, debe gestionarlo mediante Tecnologías de la Información, con una solicitud debidamente autorizada y justificada a través de su jefatura inmediata.



## TECNOLOGÍAS DE LA INFORMACIÓN

### Política: Control de Virus y Software Malicioso

Código: PL-TI-016

Fecha de vigencia: 02/03/2011


Versión 2.0

Fecha de última actualización: 30/06/2017

- 4.8 En caso que el usuario detecte una alerta en su antivirus, reciba un correo con un anexo dudoso, sospeche de una infección o note un comportamiento anormal en su computadora (bloqueo, lentitud inusual, reinicio inesperado cada cierto tiempo) deberá avisar inmediatamente a TI.
- 4.9 El usuario no deberá intentar remover un virus o programa malicioso sin la asesoría de TI, ya que esto podría ayudar a la propagación del mismo.
- 4.10 Se debe utilizar un software de antivirus que proteja contra virus, spyware y otros ataques maliciosos a los servidores y demás computadoras del Inder. Dicho software será aprobado por Tecnologías de la Información y será el único permitido.
- 4.11 Se debe definir la periodicidad de descarga de las actualizaciones del antivirus en equipos de cómputo, servidores y demás dispositivos que lo requieran.
- 4.12 Cada sistema de antivirus debe hacer revisiones y actualizaciones automáticas por medio de Internet con el proveedor del software de antivirus.
- 4.13 Los equipos portátiles deben tener la capacidad de actualizar sus firmas de antivirus a través de Internet, considerando la aprobación de TI.
- 4.14 Tecnología de la Información debe ejecutar una revisión continua del debido funcionamiento del software de antivirus, su actualización y configuración.
- 4.15 Tecnologías de la Información debe establecer procedimientos para la instalación y operación del software de antivirus, así como instructivos de tareas técnicas relacionadas al producto y su utilización, orientados al usuario final.
- 4.16 Toda acción relacionada al manejo y configuración de software de antivirus debe estar basada en los procedimientos aprobados por Tecnologías de la Información.
- 4.17 Tecnologías de la Información es el único ente autorizado para habilitar o deshabilitar los servicios relacionados con el software de antivirus o aplicaciones instaladas para combatir el software malicioso, tanto a nivel de servidor como de los demás dispositivos. Los demás usuarios del Inder no podrán deshabilitar dichos servicios por cuenta propia.
- 4.18 Tecnologías de la Información debe velar para que las actualizaciones y parches del software antivirus, así como las actualizaciones del sistema operativo u otras herramientas comerciales proporcionadas por el Inder estén al día.
- 4.19 Tecnologías de la Información deberá alertar e informar de forma periódica a todos los usuarios sobre posibles amenazas de virus, así como los riesgos asociados al uso de software malicioso en sus equipos.
- 4.20 El antivirus instalado en cada computador de escritorio deberá tener la “protección en tiempo real” activada. Éste deberá estar configurado para tratar de limpiar primero, el archivo infectado, y en caso de que no lo logre, deberá enviarlo a cuarentena.

## 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b>	
	<b>Política: Control de Virus y Software Malicioso</b>	
	Código: PL-TI-016	Fecha de vigencia: 02/03/2011
Versión 2.0	Fecha de última actualización: 30/06/2017	

## 6. Aprobación

### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

### 6.2 Aprobación por el Comité de Tecnologías de la Información

<b>Acuerdo de aprobación por el Comité de Tecnologías de la Información</b>	Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.
---	--

### 6.3 Aprobación por la Junta Directiva del Inder

<b>Acuerdo de aprobación por Junta Directiva</b>	Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.
--	--

## 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		



## TECNOLOGIAS DE INFORMACIÓN Política: Fin de la Relación Laboral

Código: PL-TI-017

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

### 1. Objetivo

- 1.1 Asegurar la continuidad de las operaciones y la seguridad de la información cuando un funcionario termina su relación laboral o un tercero termina un contrato, considerando despidos, renuncia, muerte o pensión.

### 2. Alcance

- 2.1 Esta política es aplicable a todas las Direcciones y Jefaturas de las Unidades Administrativas del Inder.

### 3. Responsables

- 3.1 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.
- 3.2 Direcciones y Jefaturas: Conocer y aplicar lo estipulado en esta política.

### 4. Pautas

- 4.1 Capital Humano debe informar a TI y a las Unidades Administrativas responsables de los Sistemas de Información, por medio de un correo electrónico y ratificado por medio de un oficio, acerca de cualquier cambio en la relación laboral o contractual de un funcionario o tercero con el Inder, de manera que el área encargada, proceda a la modificación, eliminación o suspensión de los privilegios a los sistemas y red.
- 4.2 En caso de contrataciones administrativas o convenios, es responsabilidad del jefe inmediato de cada Dirección o Unidad Administrativa informar a TI y a las Unidades Administrativas responsables de los Sistemas de Información para proceder a la modificación, eliminación o suspensión de los privilegios de los sistemas y red.
- 4.3 Los funcionarios o terceros deben devolver todos los activos de la organización que estén en su posesión, cuando finalicen sus labores dentro del Inder o cuando ya no requieran de su uso.
- 4.4 Los funcionarios o terceros deben devolver las tarjetas de identificación al jefe inmediato, cuando finalicen sus labores dentro del Inder. El jefe inmediato debe realizar la devolución de dichas tarjetas al Capital Humano.
- 4.5 Para los funcionarios o terceros con el rol de administración sobre los sistemas de información o equipos tecnológicos, la contraseña debe cambiarse inmediatamente, cuando dicho funcionario o tercero finaliza sus labores dentro del Inder.
- 4.6 Si el funcionario que se va a retirar del Inder tiene conocimiento importante que afecte la continuidad de las operaciones dentro del Inder, se debe seguir un procedimiento de documentación o transferencia de conocimiento.
- 4.7 Capital Humano debe difundir cada seis meses a toda la Institución, un padrón visual del personal que ya no labora en el Inder.

### 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.



## TECNOLOGÍAS DE INFORMACIÓN Política: Fin de la Relación Laboral

Código: PL-TI-017

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

### 6. Aprobación

#### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

#### 6.2 Aprobación por el Comité de Tecnologías de la Información

##### Acuerdo de aprobación por el Comité de Tecnologías de la Información

Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.

#### 6.3 Aprobación por la Junta Directiva del Inder

##### Acuerdo de aprobación por Junta Directiva

Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.

### 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba			



## TECNOLOGÍAS DE LA INFORMACIÓN

### Política: Administración de la Infraestructura de Software

Código: PL-TI-018

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

#### 1. Objetivo

1.1 Garantizar el uso y funcionamiento adecuado y correcto de la infraestructura de software del Inder.

#### 2. Alcance

2.1 Esta política es aplicable a todos los funcionarios del Inder, terceros y usuarios de los recursos de Tecnologías de la Información, incluyendo a todos los niveles de la estructura organizacional del Inder.

#### 3. Responsables

3.1 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.

3.2 Funcionarios, terceros y usuarios: Conocer y aplicar lo estipulado en esta política.

3.3 Comité de TI: Actuar en relación con sus funciones con respecto a productos de esta política.

3.4 Tecnologías de la Información: Administrar la infraestructura de software del Inder.

3.1 Funcionarios, terceros y usuarios: Conocer y aplicar lo estipulado en esta política.

#### 4. Pautas

4.1 Tecnologías de la Información debe asegurar el funcionamiento correcto y adecuado de la infraestructura de software del Inder.

4.2 Tecnologías de la Información debe procurar mantener software actualizado, con su respectiva instalación de parches y actualizaciones de versiones.

4.3 El Inder proveerá el software necesario para que los funcionarios puedan realizar sus labores, bajo los lineamientos establecidos para la adquisición de software. Todas las copias de software que se instalen en las computadoras del Inder tendrán una licencia vigente.

4.4 La infraestructura de software del Inder, incluyendo aplicaciones, sistemas de Información y los datos que éstos generen son propiedad del Inder y sólo pueden utilizarse para fines estrictamente oficiales y legales.

4.5 Está prohibido el uso de la infraestructura de software del Inder para fines ajenos a las actividades de la Institución.

4.6 En caso de que el usuario descubra software sin licencia en su computadora del Inder, deberá tomar medidas inmediatas para rectificar la situación, ya sea borrándolo de la computadora o reportándolo a TI.

4.7 En caso de que un usuario necesite instalar un software especial en su computadora, deberá entregar una solicitud a TI, con el visto bueno de la jefatura inmediata. Todas las solicitudes para instalar software deben incluir los detalles del uso que se planea darle al software, justificaciones para la instalación, detalles acerca de la duración del uso, el número de licencias a instalar e información relevante respecto a la licencia.



## **TECNOLOGÍAS DE LA INFORMACIÓN**

### **Política: Administración de la Infraestructura de Software**

Código: PL-TI-018

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

- 4.8 Se debe contar con un registro detallado de las licencias de software adquiridas, con sus respectivas fechas de compra, vigencia y ubicación de la licencia. Este registro debe de ser consistente para facilitar la auditoría y creación de reportes.
- 4.9 Se debe mantener un respaldo de todos los programas de software antes de que éstos sean utilizados. Se deben guardar en un lugar seguro todas las copias originales, licencias y manuales de los programas adquiridos, y se deben utilizar las copias para instalar el software en los equipos.
- 4.10 Para que un proceso de adquisición sea válido deberá cumplir con los requerimientos internos definidos por Tecnologías de la Información y la Proveduría Institucional.
- 4.11 Para la elaboración de un sistema de información se deben seguir los lineamientos definidos por TI.
- 4.12 Tecnologías de la Información debe contar con un documento de requerimientos y controles de seguridad que debe ser considerado para la implementación y mantenimiento del software para el Inder.
- 4.13 Se debe establecer y aplicar un procedimiento formal para la solicitud de cambios y nuevos requerimientos hacia la infraestructura de software del Inder.
- 4.14 Se debe establecer un procedimiento para el control de versiones y cambios en la infraestructura de software del Inder.
- 4.15 Se debe mantener un acceso restringido y los controles necesarios sobre los ambientes de desarrollo, pruebas y producción.
- 4.16 Se debe contar con los procedimientos y controles para garantizar que los datos utilizados en el ambiente de pruebas sean representativos de los datos que se utilizarán eventualmente en el ambiente de producción, proporcionando medidas adecuadas para prevenir la divulgación de datos sensibles. La documentación de los resultados de las pruebas se debe archivar y los datos de prueba se deben salvar para propósitos de las pistas de auditoría y para pruebas futuras.
- 4.17 Se deben definir y aplicar procedimientos para controlar la transferencia de sistemas desde y hacia los ambientes de desarrollo, pruebas y producción. Asimismo, procedimientos para la migración de datos.
- 4.18 Todo proceso de implementación de sistemas de información o adquisición de software debe considerar la capacitación o transferencia del conocimiento requerido para todos sus usuarios.
- 4.19 El acceso a archivos ejecutables, código fuente, librerías y otra documentación o recursos asociados al diseño de una aplicación, debe ser estrictamente controlado y manejado por Tecnologías de la Información.
- 4.20 Los roles de usuario asociados a los sistemas de información y/o aplicativos del Inder serán definidos, otorgados y documentados por el administrador asignado en cada Unidad Administrativa para tal fin.
- 4.21 La infraestructura de software del Inder y herramientas asociadas, como el correo electrónico e internet, sólo podrán ser utilizados por el personal debidamente autorizado. El uso de tales recursos constituye un privilegio otorgado con el propósito de agilizar los trabajos del Inder y no es un derecho.



## TECNOLOGÍAS DE LA INFORMACIÓN

### Política: Administración de la Infraestructura de Software

Código: PL-TI-018

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

- 4.22 Es responsabilidad de las Unidades Administrativas tomar las medidas necesarias para salvaguardar la confidencialidad de los datos personales de los empleados o de los ciudadanos contenidos en los sistemas de información que administra, conforme a la legislación aplicable.
- 4.23 Los documentos generados o contenidos en los sistemas de información serán parte de los expedientes oficiales del Inder.
- 4.24 Los usuarios de la infraestructura de software del Inder deben respetar los derechos de propiedad intelectual de los autores de las obras, programas y aplicaciones, manejadas o accedidas a través de dichos sistemas.
- 4.25 Los programas o recursos utilizados en los sistemas de información del Inder deben tener su correspondiente licencia vigente o autorización de uso para poder ser utilizadas. Dichos programas solo podrán ser instalados por el personal autorizado para tales efectos. Además, no podrán instalarse programas sin la previa autorización de Tecnologías de la Información, aunque sean programas libres de costo.
- 4.26 Los programas y aplicaciones contenidos en los sistemas de información no podrán reproducirse sin autorización de la Unidad Administrativa responsable o ser utilizados para fines ajenos a las funciones o poderes del Inder.
- 4.27 El acceso a información o a una cuenta ajena sin autorización, obtenido mediante la modificación de privilegios de acceso o la interceptación de información en cualquier otra manera está prohibido, por lo que tal conducta se castigará conforme a la legislación local y vigente y a las normas aplicables que rigen la conducta de los empleados.
- 4.28 Los relojes de todos los sistemas y terminales deberán ser sincronizados para corregir cualquier diferencia entre los mismos.
- 4.29 Tecnologías de la Información debe utilizar técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.
- 4.30 Las transacciones de datos sensibles se deben intercambiar sólo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen.

## 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

## 6. Aprobación

6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	



## TECNOLOGÍAS DE LA INFORMACIÓN

### Política: Administración de la Infraestructura de Software

Código: PL-TI-018

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

#### 6.2 Aprobación por el Comité de Tecnologías de la Información

##### Acuerdo de aprobación por el Comité de Tecnologías de la Información

Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.


#### 6.3 Aprobación por la Junta Directiva del Inder

##### Acuerdo de aprobación por Junta Directiva

Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.

### 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b> <b>Política: Administración de la Infraestructura de Hardware</b>	
	Código: PL-TI-019	Fecha de vigencia: 02/03/2011
	Versión 2.0	Fecha de última actualización: 30/06/2017

## 1. Objetivo

1.1 Mantener una adecuada administración de la infraestructura de hardware del Inder

## 2. Alcance

2.1 Esta política es aplicable a todos los funcionarios del Inder, terceros y usuarios de los recursos de tecnología de información, incluyendo a todos los niveles de la estructura organizacional del Inder.

## 3. Responsables

3.2 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.

3.3 Tecnologías de la Información: Administrar la infraestructura de hardware del Inder.

3.4 Funcionarios, terceros y usuarios: Conocer y aplicar lo estipulado en esta política.

## 4. Pautas

4.1 Ningún usuario debe realizar reparaciones o hacer alteraciones al equipo de hardware. Únicamente el personal autorizado por TI puede realizar éstas acciones.

4.2 Los usuarios son responsables de informar a TI de cualquier daño, anomalía o pérdida de los componentes de hardware del Inder de los cuales sean responsables.

4.3 Los usuarios que dispongan de computadoras portátiles deben tomar todas las medidas adecuadas para la protección de éstas, así como sacar el equipo del Inder sólo cuando sea necesario y con previa autorización de la jefatura inmediata.

4.4 Cuando una computadora portátil es colocada en un escritorio, el funcionario debe asegurarse de que esté físicamente segura con dispositivos como candados.

4.5 Si un activo es robado, se ha dañado o se extravió, debe ser reportado al Departamento Administrativo y Control de Activos inmediatamente.

4.6 Tecnologías de la Información debe asegurar el funcionamiento correcto y adecuado de la infraestructura de hardware.

4.7 Tecnologías de la Información y Control de Activos deben crear y mantener un inventario actualizado de todos los componentes de hardware que posea el Inder.

4.8 El inventario debe contener información del tipo de activo, vendedor, localización física, persona o área responsable, garantía, fecha de adquisición y número de activo.

4.9 El Sistema de Registro de Proveedores debe contar con una lista actualizada de los proveedores de hardware, sus teléfonos, direcciones y contacto.

4.10 Tecnologías de la Información es responsable de almacenar en un lugar seguro las garantías, acuerdos de servicio y copias de las facturas de todos los componentes de hardware adquiridos.



## TECNOLOGÍAS DE LA INFORMACIÓN

### Política: Administración de la Infraestructura de Hardware

Código: PL-TI-019

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

- 4.11 Tecnologías de la Información debe dar mantenimiento preventivo al equipo de hardware para maximizar su desempeño y vida del mismo. Se debe inspeccionar y dar mantenimiento al equipo según las especificaciones de fábrica.
- 4.12 Tecnologías de la Información debe realizar un respaldo de la información laboral almacenada antes de cualquier reparación sobre el equipo.
- 4.13 Se mantendrá un registro de las reparaciones y servicios prestados a cada componente de hardware, a través de reportes automatizados o de TI.
- 4.14 Los componentes de hardware deberán permanecer en temperaturas adecuadas. Se instalarán sistemas de ventilación o aire acondicionado cuando sea necesario.
- 4.15 Los equipos deberán limpiarse periódicamente según las especificaciones de los fabricantes de la empresa. Se deberá instruir a los encargados de limpieza acerca de la vulnerabilidad de los equipos, y de los materiales adecuados para el aseo de éstos. En esta pauta se incluye la limpieza del centro de datos.
- 4.16 Se deben utilizar dispositivos de respaldo eléctrico en todo el equipo que realice operaciones críticas del Inder.
- 4.17 Los dispositivos de respaldo eléctrico deben ser revisados periódicamente para cerciorarse de que pueda proveer suficiente tiempo de respaldo. También se deben realizar las pruebas que recomiendan sus fabricantes.
- 4.18 Cuando una Unidad Administrativa presente la necesidad de adquirir nuevos componentes de hardware, ésta deberá presentar la justificación escrita a la Proveduría Institucional y solicitar a Tecnologías de la Información los requerimientos técnicos del equipo.
- 4.19 Tecnologías de la Información debe presentar anualmente al Comité de TI el plan de renovación de hardware institucional con el respectivo presupuesto.
- 4.20 Los nuevos activos deben rotularse con la respectiva placa y número de activo, esto es responsabilidad de Control de Activos. Además, se deberá llenar la boleta de asignación de activos.

## 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

## 6. Aprobación

6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

6.2 Aprobación por el Comité de Tecnologías de la Información



## TECNOLOGIAS DE LA INFORMACIÓN

### Política: Administración de la Infraestructura de Hardware

Código: PL-TI-019

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

#### Acuerdo de aprobación por el Comité de Tecnologías de la Información

Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.

#### 6.3 Aprobación por la Junta Directiva del Inder

#### Acuerdo de aprobación por Junta Directiva

Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.

### 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Continuidad de TI

Código: PL-TI-020

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

### 1. Objetivo

1.1 Garantizar una adecuada continuidad de los servicios brindados por Tecnologías de la Información al Inder

### 2. Alcance

2.1 Esta política resulta aplicable para todos los funcionarios de TI, así como a los encargados de los procesos del Inder.

### 3. Responsables

3.1 Administración Superior: Proveer el entorno necesario para elaborar, ejecutar y mantener el Plan de Continuidad de los servicios de TI.

3.2 Auditoría Interna: Fiscaliza el cumplimiento de lo estipulado en esta política.

3.3 Encargados de los procesos del Inder: Conocer el plan y los procedimientos que les compete, de manera de puedan aplicarlos adecuadamente cuando se requiera.

3.4 Tecnologías de la Información: Administrar el Plan de Continuidad de los servicios de TI.

### 4. Pautas

4.1 Se deben realizar periódicamente análisis de riesgos e impacto en el negocio, para los procesos que son soportados por los servicios de TI.

4.2 Se debe identificar, cuantificar y priorizar los riesgos de acuerdo a los criterios y objetivos relevantes del Inder, contemplando recursos críticos, impactos por interrupción, tiempos permitidos de interrupción y prioridades de recuperación. Esto debe estar alineado con la metodología de evaluación de riesgos del Inder.

4.3 El plan de continuidad de los servicios de TI debe ser gestionado para asegurar una reanudación oportuna de las operaciones de los servicios de TI.

4.4 Tecnologías de la Información debe asignar un responsable para la administración del Plan de Continuidad de los servicios de TI.

4.5 El Plan de Continuidad de los servicios de TI debe ser revisado periódicamente, para asegurar que la estrategia sigue siendo aplicable. Tecnologías de la Información debe definir la periodicidad para las revisiones y la vigencia del Plan de Continuidad de los servicios de TI.

4.6 Tecnologías de la Información debe definir el calendario y guiones para las pruebas periódicas que certifiquen la debida ejecución del plan.

4.7 La infraestructura y los procesos que soportan la estrategia de continuidad de los servicios de TI deben ser integrados con los requerimientos de seguridad de la información.

4.8 El Plan de Continuidad de los servicios de TI debe integrar los procedimientos de recuperación y restauración en caso de desastre.



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Continuidad de TI

Código: PL-TI-020

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

- 4.9 Los procedimientos de recuperación y restauración deben incluir todos los aspectos necesarios para garantizar la seguridad de la información.
- 4.10 Se debe determinar una estrategia de distribución de los planes y procedimientos, para asegurar que se distribuyan de manera apropiada y que estén disponibles a todas las partes involucradas y autorizadas, cuando y donde se requiera.
- 4.11 Tecnologías de la Información debe asegurar que todas las partes involucradas reciban sesiones de capacitación periódicamente, respecto a los procesos, roles y responsabilidades en caso de incidente o desastre.
- 4.12 El responsable de administrar el Plan de Continuidad de los servicios de TI debe tener una lista de los contactos en caso de emergencia. Se tendrán los números de teléfono y direcciones primarias de cada persona crítica a quien contactar en caso de que ocurra una eventualidad.
- 4.13 Se deben definir líderes responsables de velar por el seguimiento del plan y los procedimientos, en caso de una interrupción del Inder, esto para aspectos operacionales, disponibilidad de recursos e instalaciones.

### 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

### 6. Aprobación

#### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

#### 6.2 Aprobación por el Comité de Tecnologías de la Información

##### Acuerdo de aprobación por el Comité de Tecnologías de la Información

Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.

#### 6.3 Aprobación por la Junta Directiva del Inder

##### Acuerdo de aprobación por Junta Directiva

Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.



**TECNOLOGIAS DE LA INFORMACIÓN**  
**Política: Continuidad de TI**

Código: PL-TI-020


Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

**7. Historial de revisiones**

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		

	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b> <b>Política: Respaldos y Recuperación</b>	
	Código: PL-TI-021 Versión 2.0	Fecha de vigencia: 02/03/2011 Fecha de última actualización: 30/06/2017

## 1. Objetivo

- 1.1. Asegurar el respaldo y la recuperación de los datos propios de la organización asegurando su confidencialidad, integridad y disponibilidad en el almacenamiento tanto en el sitio como fuera de él.

## 2. Alcance


- 2.1. Esta política es aplicable a todos los funcionarios de TI y las Unidades Administrativas que administren bases de datos locales de sus sistemas de información.

## 3. Responsables

- 3.1 Auditoría Interna: Fiscalizar por el cumplimiento de lo estipulado en esta política.
- 3.2 Tecnologías de la Información: Realizar los respaldos de los datos e información que custodia y garantizar la adecuada recuperación de los mismos.
- 3.3 Unidades Administrativas: Realizar respaldos de los datos e información custodiada por cada oficina.
- 3.4 Funcionarios, terceros y usuarios: Conocer y aplicar lo estipulado en esta política.

## 4. Pautas

- 4.1 Tecnologías de la Información debe tener claramente definido el personal que tendrá la responsabilidad de realizar los distintos tipos de respaldos. El personal no sólo debe ser capaz de generar el respaldo, sino estar capacitado para la recuperación de la información en caso de ser necesario, a partir de los distintos tipos de respaldo.
- 4.2 El respaldo de los datos ejecutado por Tecnologías de la Información, debe considerar tanto los datos de sistemas de información (archivos, bases de datos) como los demás elementos necesarios para asegurar la prestación de servicios, el software de la aplicación (código fuente) y operación, documentación complementaria al software de ambiente.
- 4.3 Debe crearse una programación formal de respaldo. Además, se debe contar con procedimientos de verificación y supervisión de los procesos y del contenido de los respaldos.
- 4.4 Todos los procesos de respaldo y recuperación deben proveer los elementos que evidencien la ejecución del proceso, detalle el contenido de los mismos, así como errores o inconsistencias en caso de existir.
- 4.5 Los medios de respaldo deben ser protegidos de borrados accidentales a través del uso de medios físicos y lógicos de carácter preventivo.
- 4.6 Los medios de respaldo deben disponer de etiquetas internas y externas, así como una identificación permanente, que permita determinar fácil y confiablemente su contenido.
- 4.7 Los respaldos de datos y demás elementos complementarios, deben estar resguardados en sitios que dispongan de condiciones de acceso restringido y de medio ambiente y físicos apropiados que los protejan de cualquier contingencia.

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b>	
	<b>Política: Respaldos y Recuperación</b>	
	Código: PL-TI-021	Fecha de vigencia: 02/03/2011
	Versión 2.0	Fecha de última actualización: 30/06/2017

- 4.8 Antes de proceder a la restauración de datos sensitivos o críticos a partir de un respaldo se debe realizar una copia de los mismos para minimizar efectos de corrupción o daños de los datos originalmente respaldados.
- 4.9 Los respaldos mensualmente se envían a una bóveda de seguridad, que cumpla con las características de protección física y ambiental apropiadas para resguardo de las cintas.
- 4.10 Se debe tomar las medidas de seguridad necesarias para el traslado de los medios de respaldo a la bóveda de seguridad.
- 4.11 Los equipos y medios de respaldo de las distintas plataformas de información y tecnología deben ser estandarizada para que faciliten el intercambio de datos, control y maniobrabilidad de operación por parte del personal de Tecnologías de la Información.
- 4.12 Los equipos y medios usados para el respaldo deben ser sometidos a un mantenimiento preventivo de acuerdo a las recomendaciones del fabricante que asegure las condiciones adecuadas de su funcionamiento y fiabilidad.
- 4.13 Cada Unidad Administrativa deberá tener un encargado de realizar los respectivos respaldos de la información primordial de cada oficina.
- 4.14 Los procedimientos adoptados para respaldar y recuperar la información deben de ser revisados periódicamente.
- 4.15 Los respaldos deben ubicarse en un lugar restringido, de manera que personas no autorizadas no logren manipularlos. El lugar donde se almacenan debe poseer condiciones ambientales que aseguren la confiabilidad de la información.

## 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

## 6. Aprobación

6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

6.2 Aprobación por el Comité de Tecnologías de la Información

<b>Acuerdo de aprobación por el Comité de Tecnologías de la Información</b>	Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.
---	--

6.3 Aprobación por la Junta Directiva del Inder

<b>Acuerdo de aprobación por Junta</b>	Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del
--	--



## TECNOLOGIAS DE LA INFORMACIÓN Política: Respaldos y Recuperación

Código: PL-TI-021

Fecha de vigencia: 02/03/2011

Versión 2.0


Fecha de última actualización: 30/06/2017

### Directiva

Inder del 19/03/2018.

### 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		

	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b> <b>Política: Administración de Proyectos de TI</b>	
	Código: PL-TI-022 Versión 2.0	Fecha de vigencia: 02/03/2011 Fecha de última actualización: 30/06/2017

## 1. Objetivo

- 1.1 Asegurar la entrega de los resultados de los proyectos de TI en el tiempo, con el presupuesto y la calidad acordados y considerando también el adecuado alineamiento con los planes estratégicos corporativos y de TI.

## 2. Alcance


- 2.1 Esta política es aplicable a todos los funcionarios de TI y terceros que apoyan el proceso de Administración de Proyectos de TI del Inder.

## 3. Responsables

- 3.1 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.
- 3.2 Comité de TI: Aprobar los proyectos y priorizar la ejecución de los mismos, con base a la propuesta generada por TI.
- 3.3 Funcionarios de TI y terceros: Conocer y aplicar lo estipulado en esta política.

## 4. Pautas

- 4.1 Según el portafolio de proyecto del PETI, Tecnologías de la Información debe realizar un análisis de factibilidad para la ejecución de los proyectos, considerando la posibilidad técnica, operativa, recursos y económica de ejecutarlo.
- 4.2 Según los resultados del análisis de factibilidad, el Comité de Tecnologías de la Información será el responsable de aprobar o denegar el proyecto.
- 4.3 Todo proyecto en Tecnologías de la Información deberá cumplir con las siguientes etapas: iniciación, planificación, ejecución, monitoreo y cierre, de acuerdo a lo establecido en el marco de referencia PMBOK del Project Management Institute.
- 4.4 La metodología de Administración de Proyectos y todo cambio que se realice a la misma, debe ser aprobado formalmente por el Comité de TI.
- 4.5 Deben aplicarse todas las etapas de la metodología de Administración de Proyectos a todos los proyectos de Tecnologías de la Información. En caso que alguna de las etapas no aplique para algún proyecto específico, esto debe ser documentado y aprobado formalmente por la jefatura de TI.
- 4.6 Se asignará un equipo de trabajo para administrar cada proyecto de acuerdo a la metodología definida por el Inder. El número de miembros en el equipo dependerá del tamaño, complejidad y duración del proyecto. Este equipo se asegurará de establecer un plan del proyecto y que éste sea completado de manera coordinada.
- 4.7 Los miembros del equipo de trabajo serán seleccionados tomando en cuenta su experiencia en proyectos similares, conocimientos, familiaridad con proyectos relacionados y disponibilidad. Se elegirá a un miembro del proyecto como Director de Proyecto, que se encargará de coordinar las labores del proyecto.

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b>	
	<b>Política: Administración de Proyectos de TI</b>	
	Código: PL-TI-022	Fecha de vigencia: 02/03/2011
	Versión 2.0	Fecha de última actualización: 30/06/2017

- 4.8 Una vez elegidos los miembros del equipo de trabajo, se procederá a asignar los roles, responsabilidades y autoridad de cada persona. Éstos deberán ser claramente entendidos antes de iniciar el proyecto para evitar conflictos durante la realización del mismo.
- 4.9 El equipo de proyecto se reunirá cuantas veces lo considere necesario. Sin embargo, se deberá preparar una reunión al inicio del proyecto para aclarar los roles, responsabilidades y plan a seguir y se deberán programar reuniones periódicas para supervisar el avance del proyecto.
- 4.10 Al final del proyecto, el Director del Proyecto se reunirá con las áreas involucradas para discutir los resultados del proyecto, problemas que surgieron y hacer recomendaciones para futuros trabajos similares.
- 4.11 Se documentarán minutas detalladas de todas las reuniones que se realicen durante el proyecto.
- 4.12 Cualquier duda, recomendación, observación que se considere pertinente durante la ejecución del proyecto deberá tratarse directamente con el Director del Proyecto.
- 4.13 Previo al inicio del proyecto, deben establecerse y documentarse los criterios de aceptación para cada uno de los entregables del proyecto. Dichos criterios deben incluir el tiempo de entrega y requisitos de funcionalidad y calidad del mismo.
- 4.14 Se deberá desarrollar un Plan de Calidad que identifique los estándares y lineamientos que se utilizarán al planear, administrar, controlar e implementar un proyecto efectivamente.
- 4.15 Se deberán tomar medidas correctivas para lidiar con el incumplimiento de los requisitos del Plan de Calidad.
- 4.16 Los entregables producidos en cada fase del proyecto deben ser aprobados formalmente por el Director del Proyecto.
- 4.17 Todo cambio en el proyecto debe quedar debidamente documentado y aprobado.
- 4.18 Para el cierre del proyecto, el Director del Proyecto deben aprobar formalmente el proyecto.
- 4.19 Toda la información relativa al control en la ejecución de los proyectos de Tecnologías de la Información deberá ser documentada y almacenada en un lugar seguro.

## 5. Sanciones


El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

## 6. Aprobación

6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

6.2 Aprobación por el Comité de Tecnologías de la Información

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b> <b>Política: Administración de Proyectos de TI</b>	
	Código: PL-TI-022 Versión 2.0	Fecha de vigencia: 02/03/2011 Fecha de última actualización: 30/06/2017


<b>Acuerdo de aprobación por el Comité de Tecnologías de la Información</b>	Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.
---	--

### 6.3 Aprobación por la Junta Directiva del Inder

<b>Acuerdo de aprobación por Junta Directiva</b>	Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.
--	--

## 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b> <b>Política: Administración de la Capacidad</b>	
	Código: PL-TI-023 Versión 2.0	Fecha de vigencia: 02/03/2011 Fecha de última actualización: 30/06/2017

## 1) Objetivo

1.1 Determinar y monitorear la capacidad y el desempeño de los recursos que dan soporte a la plataforma tecnológica del Instituto.

## 2) Alcance

2.1 Esta política es aplicable para los funcionarios de TI.

## 3) Responsables

3.1 Funcionarios de Tecnologías de la Información: Conocer y aplicar lo estipulado en esta política.

## 4) Pautas

4.1 El monitoreo de los recursos tecnológicos se realizará siguiendo una guía de monitoreo de la capacidad y desempeño, en la cual se indicarán los parámetros, límites de tolerancia y frecuencias de cada recurso, con base en los cuáles se estarán realizando las mediciones de capacidad y desempeño.

4.2 Esta guía de monitoreo debe ser desarrollada por TI y deberá ser evaluada, al menos una vez al año, para asegurar su aplicabilidad a las necesidades cambiantes del Inder.

4.3 Los datos recolectados con respecto a la capacidad y desempeño de los recursos tecnológicos deberán ser almacenados y analizados considerando:

4.3.1 Información histórica del desempeño y capacidad

4.3.2 Cargas de trabajo a las que está sometido el recurso tecnológico.

4.3.3 Tendencias en los niveles de desempeño y capacidad

4.4 Los informes y estudios de capacidad y desempeño deberán de ser utilizados como parte del proceso del desarrollo de la planeación estratégica y operativa de TI, con el fin de tomar las medidas relacionadas con los aspectos tecnológicos.


4.5 Toda adquisición y actualización de equipo tecnológico debe estar fundamentada con base en los informes y estudios de capacidad y desempeño.

4.6 Los informes y estudios de capacidad y desempeño se custodiarán por un espacio de aproximadamente dos años, luego del cual se trasladará al Archivo Institucional para que proceda según la normativa vigente.

4.7 Todo desarrollo de un nuevo sistema, o cambio a los sistemas actuales o plataforma tecnológica deberá ser evaluado en términos del impacto a nivel de la capacidad y desempeño de los recursos tecnológicos requeridos para su funcionamiento.

## 5) Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b>	
	<b>Política: Administración de la Capacidad</b>	
	Código: PL-TI-023	Fecha de vigencia: 02/03/2011
	Versión 2.0	Fecha de última actualización: 30/06/2017

## 6) Aprobación

### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

### 6.2 Aprobación por el Comité de Tecnologías de la Información

<b>Acuerdo de aprobación por el Comité de Tecnologías de la Información</b>	Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.
---	--

### 6.3 Aprobación por la Junta Directiva del Inder

<b>Acuerdo de aprobación por Junta Directiva</b>	Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.
--	--

## 7) Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		



## **TECNOLOGÍAS DE LA INFORMACIÓN**

### **Política: Segregación de Funciones y Responsabilidades**

Código: PL-TI-024

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

#### **1. Objetivo**

1.1 Definir las responsabilidades que le competen a cada uno de los funcionarios del Inder y asegurar la adecuada segregación de funciones para garantizar la protección adecuada de la información.

#### **2. Alcance**

2.1 Esta política es aplicable a todos los funcionarios del Inder, incluyendo a todos los niveles de la estructura organizacional del Inder.

#### **3. Responsables**

3.1 Administración Superior: Velar por el cumplimiento de esta política y ejecutar medidas correctivas.

3.2 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.

3.3 Funcionarios: Conocer y aplicar lo estipulado en esta política.

#### **4. Pautas**

4.1 Los directores, jefes o encargados de cada Unidad Administrativa del Inder deben desarrollar una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte un proceso crítico dentro del Inder, considerando la legislación aplicable.

4.2 Es responsabilidad de los directores, jefes o encargados de cada Unidad Administrativa del Inder documentar las responsabilidades de cada uno de los funcionarios que están bajo su supervisión y facilitar dicha documentación a Capital Humano.

4.3 Los jefes inmediatos deben velar que los funcionarios realicen solo las tareas autorizadas, relevantes a su puesto y responsabilidades.

4.4 Tecnologías de la Información debe aplicar controles como las pistas de auditoría en los sistemas y el monitoreo de los equipos tecnológicos de Inder con el fin de detectar cualquier anomalía.

4.5 Auditoría Interna debe definir procesos adecuados para la supervisión de los servicios de TI, esos procesos deben estar orientados a garantizar una adecuada ejecución de las responsabilidades, adicionalmente deben evaluar si el personal dispone de la autoridad y recursos suficientes para cumplir satisfactoriamente con los roles y responsabilidades que le fueron asignados.

4.6 Para la definición y administración de una adecuada segregación de funciones y responsabilidades, las Unidades Administrativas deberán realizar revisiones periódicas de manera oportuna para determinar los cambios en los accesos a los sistemas de información y otros cambios en las funciones generales de los funcionarios, con el objetivo de realizar las actualizaciones pertinentes.

4.7 Deben llevarse a cabo de forma periódica evaluaciones de las necesidades de TI para garantizar que la función de servicios de TI cuente con el personal suficiente y competente para realizar las labores necesarias. Esa evaluación debe realizarse al menos anualmente o en su defecto cuando se presente un cambio significativo en el Inder en las operaciones o en el ambiente operativo de TI.



## TECNOLOGÍAS DE LA INFORMACIÓN

### Política: Segregación de Funciones y Responsabilidades

Código: PL-TI-024

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

#### 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

#### 6. Aprobación

##### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

##### 6.2 Aprobación por el Comité de Tecnologías de la Información

###### Acuerdo de aprobación por el Comité de Tecnologías de la Información

Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.

##### 6.3 Aprobación por la Junta Directiva del Inder

###### Acuerdo de aprobación por Junta Directiva

Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.

#### 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		



## TECNOLOGÍAS DE LA INFORMACIÓN

### Política: Administración de Niveles de Servicio

Código: PL-TI-025

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

#### 1. Objetivo

- 1.1 Lograr una comunicación efectiva entre Tecnologías de la Información y los proveedores de servicios respecto de los servicios requeridos.

#### 2. Alcance

- 2.1 Esta política es aplicable a todos los funcionarios de TI del Inder y terceros que brindan servicios que apoyan la Función de TI

#### 3. Responsables


- 3.1 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política y monitorear y reportar desvíos en los SLA definidos y aprobados
- 3.2 Tecnologías de la Información: Definir y negociar con los proveedores de servicios los niveles aceptables para dichos servicios.
- 3.3 Funcionarios de TI y Terceros: Conocer y aplicar lo estipulado en esta política.

#### 4. Pautas

- 4.1 Tecnologías de la Información debe definir los acuerdos de nivel de servicio (SLA) para los servicios críticos del negocio apoyados por la Función de TI, de manera que dichos acuerdos se negocien, acuerden y aprueben con los terceros involucrados.
- 4.2 Realizar revisiones periódicas de los objetivos de cada SLA acordado, la eficacia y eficiencia, e informar a los responsables e interesados según cada SLA.
- 4.3 Mejorar o ajustar cada SLA basado en la retroalimentación sobre su desempeño y ajustarlos según los requisitos del Inder.
- 4.4 Definir un proceso para monitorear continuamente todos los SLA's definidos y aprobados
- 4.5 Definir y revisar periódicamente los criterios para identificar y clasificar todas las relaciones con los proveedores según el tipo de proveedor, la importancia y la criticidad del servicio que este presta.
- 4.6 Tecnologías de la Información debe mantener una lista con la categorización de los proveedores según el desempeño en los servicios que presta.
- 4.7 La Proveeduría Institucional debe establecer y mantener un registro detallado de los proveedores, incluyendo el nombre, el alcance de su servicio, la finalidad del mismo y detalles de contacto clave.

#### 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b>	
	<b>Política: Administración de Niveles de Servicio</b>	
	Código: PL-TI-025	Fecha de vigencia: 02/03/2011
Versión 2.0	Fecha de última actualización: 30/06/2017	

## 6. Aprobación

### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

### 6.2 Aprobación por el Comité de Tecnologías de la Información

<b>Acuerdo de aprobación por el Comité de Tecnologías de la Información</b>	Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.
---	--

### 6.3 Aprobación por la Junta Directiva del Inder

<b>Acuerdo de aprobación por Junta Directiva</b>	Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.
--	--

## 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		



## TECNOLOGÍAS DE LA INFORMACIÓN

### Política: Administración de Cambios y Liberaciones

Código: PL-TI-026

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

#### 1. Objetivo

1.1 Garantizar que los cambios implementados sean beneficios para el Inder y que haya la mínima interrupción posible de los servicios ofrecidos, asegurando la integridad del ambiente de producción cuando se liberan cambios.

#### 2. Alcance

2.1 Esta política es del alcance de todos los funcionarios responsables por la ejecución, implementación y aprobación de cambios a la infraestructura de TI del Inder.

2.2 Esta política debe aplicarse para todos los cambios que se deban ejecutar, para cualquiera de los componentes de Tecnología de la Información del Inder, ya sean estos cambios de adición, modificación o eliminación. La política aplica al menos cuando se requiera ejecutar cambios en:

- **Hardware:** cambios, adiciones, eliminación, reconfiguración, reubicación, mantenimiento preventivo o de emergencia.
- **Software:** nuevas versiones del producto, tuning, arreglos temporales, alteraciones a las librerías de producción, configuración de “jobs”, actualización de sistemas operativos, instalación de parches, modificación de estructuras de datos.
- **Ambiental:** fuentes de poder, sistemas de UPS, generadores de electricidad, aire acondicionado, trabajo eléctrico, mantenimiento del lugar, sistemas de seguridad, sistemas contra incendio.
- **Sistemas de red:** adiciones, modificaciones o eliminaciones de líneas de comunicación, módems, enrutadores, conmutadores, muros de fuego, firewalls, sistemas de detección de intrusos, servidores, direcciones IP.
- **Sistemas de información y aplicaciones:** implementación de aplicaciones nuevas, actualizaciones masivas de datos, versiones nuevas de las aplicaciones, modificaciones, migración del ambiente de pruebas al de producción, cambios al código fuente, creación o modificación de documentación.

#### 3. Responsables

3.1 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política garantizando que cualquier cambio sigue el proceso aprobado

3.2 Tecnologías de la Información: Administrar los cambios que se requieran para la plataforma tecnológica y gestionar la adecuada liberación de los mismos al ambiente de producción.

3.3 Funcionarios, terceros y usuarios: Conocer y aplicar lo estipulado en esta política

#### 4. Pautas

4.1 Todo cambio debe ser gestionado con Tecnologías de la Información por medio de una solicitud formal de cambio, la cual incluye el detalle del cambio requerido y las firmas de las autorizaciones respectivas.

4.2 Para todos los cambios propuestos, Tecnologías de la Información debe realizar un análisis de riesgo que considere al menos los siguientes aspectos:

- El número de usuarios que se verán afectados por el cambio.
- El impacto en otros servicios que corren en la misma infraestructura.



## **TECNOLOGÍAS DE LA INFORMACIÓN**

### **Política: Administración de Cambios y Liberaciones**

Código: PL-TI-026

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

- El efecto que traerá para el negocio no implementar el cambio.
- Los recursos necesarios para implementar el cambio.

- 4.3 Tecnologías de la Información debe asignar a cada cambio una categoría y una prioridad que permita decidir cuáles cambios deben ser discutidos e implementados primero. En las prioridades se deben considerar los cambios de emergencia.
- 4.4 Los cambios de emergencia deben seguir un proceso abreviado de Administración de Cambios, el cual permita la rápida implementación de los mismos. La documentación de los cambios de emergencia puede realizarse posterior a su implementación en el mínimo tiempo posible después de que el cambio fue implementado.
- 4.5 Los cambios frecuentes deben ser formalmente documentados y aprobados por la jefatura de Tecnologías de la Información. Esta lista debe ser revisada periódicamente para asegurar su actualización, completitud y alineación con las necesidades de Tecnologías de Información del Inder.
- 4.6 Los cambios frecuentes han sido pre-aprobados por la jefatura de TI y por lo tanto no necesitan pasar por nuevas aprobaciones durante el proceso de Administración de Cambios.
- 4.7 Tecnologías de la Información debe establecer un plan de liberación del cambio, considerando la construcción del cambio, la documentación de las pruebas, la implementación, fechas y horas para la liberación, situaciones de aceptación y no aceptación.
- 4.8 Debe existir un ambiente separado para realizar las pruebas de los cambios, previo a la ejecución en el ambiente de producción.
- 4.9 Antes de realizar el pase del cambio al ambiente de producción, se debe desarrollar y documentar un plan de retorno que especifique los pasos a seguir para poder restaurar el ambiente de producción del Inder a su estado original en caso de ser necesario.
- 4.10 Los cambios deben ser aprobados previo a su pase al ambiente de producción. Las aprobaciones deben realizarse dependiendo de las categorías de los cambios.
- 4.11 En caso de que la liberación sea considerada de emergencia, la misma puede pasar por un proceso abreviado que permita una rápida implementación en el ambiente de producción. En estos casos, la documentación puede realizarse posterior a su implementación, en el mínimo tiempo posible después de que el cambio fue implementado en el ambiente de producción.

## **5. Sanciones**

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

## **6. Aprobación**

### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	



## **TECNOLOGÍAS DE LA INFORMACIÓN**

### **Política: Administración de Cambios y Liberaciones**

Código: PL-TI-026

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

#### 6.2 Aprobación por el Comité de Tecnologías de la Información

##### **Acuerdo de aprobación por el Comité de Tecnologías de la Información**

Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.

#### 6.3 Aprobación por la Junta Directiva del Inder

##### **Acuerdo de aprobación por Junta Directiva**

Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.

### 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Atención de Usuarios

Código: PL-TI-027

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

### 1. Objetivo

1.1 Regular la implementación y ejecución de la función de la Mesa de Ayuda que funge como único punto de contacto para las solicitudes de usuario relacionadas con servicios de TI.

### 2. Alcance

2.1 Esta política es aplicable a todos los funcionarios del Inder, terceros y usuarios de los recursos de tecnología de información, incluyendo a todos los niveles de la estructura organizacional del Inder.

### 3. Responsables

3.1 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.

3.2 Tecnologías de la Información: Administrar y asegurar el uso adecuado de la Mesa de Ayuda.

3.3 Funcionarios, terceros y usuarios: Conocer y aplicar lo estipulado en esta política.

### 4. Pautas

4.1 Toda solicitud de servicio emitida por un usuario debe ser procesada únicamente por la Mesa de Ayuda con el fin de realizar una gestión adecuada.

4.2 Toda solicitud de servicio debe ser debidamente registrada y categorizada de acuerdo a su tipo, prioridad, impacto y urgencia.

4.3 Se deben definir y asignar roles y responsabilidades para cada nivel de soporte dentro de la Mesa de Ayuda.

4.4 Se debe definir e implementar un sistema de escalamiento de incidentes entre los niveles de soporte internos del proceso, como para la transferencia a otros procesos.

4.5 Para cada solicitud de servicio debe existir una encuesta de satisfacción, la cual busca identificar el nivel de satisfacción de los usuarios con el servicio brindado por la Mesa de Ayuda.

4.6 Se debe realizar una inducción de la Mesa de Ayuda al personal de nuevo ingreso y definir planes de capacitación del personal en general.

4.7 Todo el conocimiento generado en el proceso debe ser debidamente documentado.

### 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Atención de Usuarios

Código: PL-TI-027

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

### 6. Aprobación

#### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

#### 6.2 Aprobación por el Comité de Tecnologías de la Información

##### Acuerdo de aprobación por el Comité de Tecnologías de la Información

Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.

#### 6.3 Aprobación por la Junta Directiva del Inder

##### Acuerdo de aprobación por Junta Directiva

Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.

### 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		



## **TECNOLOGÍAS DE LA INFORMACIÓN**

### **Política: Administración de Incidentes y Problemas**

Código: PL-TI-028

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

#### **1. Objetivo**

1.1 Asegurar que los problemas e incidentes presentados en sistemas de información y plataforma tecnológica sean resueltos y que sus causas sean investigadas para mitigar su recurrencia.

#### **2. Alcance**

2.1 Esta política es aplicable a todos los funcionarios del Inder, terceros y usuarios de los recursos tecnológicos, incluyendo a todos los niveles de la estructura organizacional del Inder.

#### **3. Responsables**

3.1 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.

3.2 Tecnologías de la Información: Administrar los incidentes y problemas en relación con las tecnologías de información del Inder.

3.3 Funcionarios, terceros y usuarios: Conocer y aplicar lo estipulado en esta política.

#### **4. Pautas**

4.1 Todos los funcionarios del Inder son responsables de notificar, en el menor tiempo posible a su jefatura inmediata y/o a TI, cualquier anomalía en torno a los sistemas informáticos o plataforma tecnológica para iniciar la respectiva investigación y tomar las medidas correctivas pertinentes.

4.2 Se deben establecer los parámetros y lineamientos que rijan el proceso de administración de incidentes y problemas, donde se definan los procedimientos necesarios para el reporte de incidentes y problemas, identificación y respuesta, el escalamiento en los casos más críticos y el seguimiento necesario para la adecuada solución, considerando niveles de servicio establecidos.

4.3 Se debe crear un procedimiento que indique la secuencia de pasos a seguir para registrar, investigar, solucionar y documentar todos los incidentes y problemas identificados. Este procedimiento debe incluir los niveles de prioridad y la categorización para abordar la situación en un tiempo adecuado.

4.4 Se deben asignar los roles y funciones al personal, cuya participación sea requerida en la atención de los incidentes. Estos deben conocer y entender cuáles son las prioridades del Inder en caso de que se presentes varios eventos simultáneamente.

4.5 Deben existir métodos de concienciación hacia los funcionarios y terceros con el fin de que puedan ejecutar un debido proceso ante un eventual incidente.

4.6 Para todo problema presentado se debe identificar los componentes específicos de la infraestructura de TI que se vean afectados, así como las áreas o dependencias afectadas fuera de TI y comunicar formalmente la situación dada, con el fin de aplicar las medidas preventivas y correctivas del caso.

4.7 Se deben emitir reportes de incidentes y problemas para todos los casos que se presenten. Éstos deben ser generados por los funcionarios que atendieron y dieron respuesta a dichos incidentes o problemas.

4.8 Los incidentes y problemas deben ser registrados en un sistema de gestión que permita establecer registros de auditoría y dar el seguimiento apropiado a los casos abiertos, reabiertos, en curso y cerrados.



## TECNOLOGÍAS DE LA INFORMACIÓN

### Política: Administración de Incidentes y Problemas

Código: PL-TI-028

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

- 4.9 Tecnologías de la Información debe comunicar los avances en la solución de problemas y controlar continuamente el impacto de los problemas no resueltos.
- 4.10 Se deben tener activas las herramientas de auditoría en sistemas operativos, gestores de bases de datos, equipos de comunicación, equipos de seguridad y demás equipos críticos, las cuales deben ser revisadas periódicamente para la atención y respuesta de incidencias y/o problemas. Estas herramientas deben proporcionar adecuadas pistas de auditoría que permitan el seguimiento de un incidente o problema a partir de sus causas.
- 4.11 Tecnologías de la Información debe establecer, documentar y aprobar la prioridad de los procesos involucrados en una emergencia, cuando los mismos requieran del uso de servicios tecnológicos y de su personal para atender una situación y cuya solución no sea tratable a través de los procesos normales del Inder.

## 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

## 6. Aprobación

### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

### 6.2 Aprobación por el Comité de Tecnologías de la Información

<b>Acuerdo de aprobación por el Comité de Tecnologías de la Información</b>	Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.
---	--

### 6.3 Aprobación por la Junta Directiva del Inder

<b>Acuerdo de aprobación por Junta Directiva</b>	Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.
--	--



**TECNOLOGIAS DE LA INFORMACIÓN**  
**Política: Administración de Incidentes y Problemas**

Código: PL-TI-028

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

## 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Administración de Terceros

Código: PL-TI-029

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

### 1. Objetivo

- 1.1 Asegurar la adecuada evaluación y contratación de terceros que provean bienes o servicios relacionados con tecnologías de la información.

### 2. Alcance


- 2.1 Esta política es aplicable a todos los funcionarios del Inder, terceros y usuarios de los recursos de tecnología de información, incluyendo a todos los niveles de la estructura organizacional del Inder.

### 3. Responsables

- 3.1 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.
- 3.2 Tecnologías de la Información en conjunto con las Unidades Administrativas responsables: Aplicar las pautas y procedimientos definidos en relación con esta política.
- 3.3 Proveeduría Institucional: Administrar la información que establezca las responsabilidades de las partes.
- 3.4 Funcionarios y terceros: Conocer y aplicar lo estipulado en esta política.

### 4. Pautas

- 4.1 La Unidad Administrativa responsable es la encargada de fiscalizar el desempeño de la contratación de un tercero.
- 4.2 Asuntos Jurídicos es responsable de la revisión en términos legales de todos los puntos del contrato concernientes a las responsabilidades de ambas partes.
- 4.3 Toda documentación que establezca las responsabilidades de las partes debe ser almacenada en un lugar que garantice su integridad y disponibilidad. Esta información será administrada por la Proveeduría Institucional, facilitando una copia de dicha información a la Unidad Administrativa responsable.
- 4.4 En toda contratación se deben considerar los requisitos técnicos, aspectos de seguridad y pautas requeridas por el Inder que deben cumplirse, así como las acciones a tomar en caso de violaciones a las cláusulas definidas.
- 4.5 Para la implementación de cualquier servicio contratado, TI brindará acceso supervisado a los recursos tecnológicos estrictamente necesarios, de acuerdo a los lineamientos definidos.
- 4.6 En caso de ser necesario, según el tipo de servicio contratado, se podrán establecer limitaciones y restricciones referentes al acceso a los recursos involucrados en el servicio.
- 4.7 Todo contrato donde la empresa externa deba interactuar con información perteneciente al Inder, debe incluir el respectivo acuerdo de confidencialidad y no divulgación de la información. Se debe definir un responsable por parte del personal externo para las acciones realizadas por los terceros.
- 4.8 Si el contrato está sujeto a un Acuerdo de Nivel de Servicio, se debe incluir una cláusula en la cual se especifique que el bien o servicio proporcionado por la contraparte podría ser sujeta a una revisión por parte del Inder.

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGÍAS DE LA INFORMACIÓN</b>	
	<b>Política: Administración de Terceros</b>	
	Código: PL-TI-029	Fecha de vigencia: 02/03/2011
	Versión 2.0	Fecha de última actualización: 30/06/2017

4.9 En toda contratación se debe respetar y acatar los lineamientos y políticas establecidos por TI.

## 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

## 6. Aprobación

6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

6.2 Aprobación por el Comité de Tecnologías de la Información

<b>Acuerdo de aprobación por el Comité de Tecnologías de la Información</b>	Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.
---	--

6.3 Aprobación por la Junta Directiva del Inder

<b>Acuerdo de aprobación por Junta Directiva</b>	Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.
--	--

## 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Monitoreo del desempeño de TI

Código: PL-TI-030

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

### 1. Objetivo

1.1 Garantizar el logro de los objetivos de desempeño establecidos para los procesos de gestión de la función de TI del Inder.

### 2. Alcance

2.1 Esta política es aplicable a todos los funcionarios de TI del Inder.

### 3. Responsables

3.1 Auditoría Interna: Fiscalizar el cumplimiento de lo estipulado en esta política.

3.2 Funcionarios de TI: Conocer y aplicar lo estipulado en esta política.

### 4. Pautas

4.1. Auditoría Interna es el encargado de velar y responder por la ejecución de las actividades y el logro de los objetivos del proceso de monitoreo y evaluación del desempeño de los procesos de TI.

4.2. Los involucrados en el proceso de Monitoreo y evaluación del desempeño de los procesos de TI que sean convocados como delegados principales a reuniones o sesiones de trabajo, cuando se les imposibilite asistir, deben de asignar un representante con las facultades técnicas y administrativas necesarias para suplir su labor en la reunión o sesión correspondiente, o bien, solicitar la reprogramación de la reunión o sesión.

4.3. Los administradores de los procesos de TI, en conjunto con Auditoría Interna son responsables por la evaluación continua de los procesos, así como la ejecución de las acciones preventivas o correctivas necesarias para su mejora.

4.4. Auditoría Interna es el responsable por la creación y actualización del modelo de monitoreo.

4.5. El Comité de TI es el encargado del análisis y evaluación del modelo de monitoreo, los resultados de la evaluación del desempeño y de todos los planes o acciones de mejora.

4.6. Los procesos de TI deben ser evaluados en forma continua según las frecuencias definidas en el modelo de monitoreo, considerando que todos los indicadores claves de desempeño (KPI) de los procesos deben ser analizados en el periodo.

4.7. Los KPI a monitorear deben ser aquellos que han sido definidos como parte del modelo vigente de procesos de gestión de TI.

4.8. La definición del modelo de monitoreo debe considerar los lineamientos y las herramientas existentes definidas en la versión vigente del plan de calidad de TI.

4.9. Para toda evaluación del desempeño, el modelo de monitoreo definirá un alcance, el cual puede corresponder a todos los procesos en ejecución o ser restringida a procesos específicos que requieran un análisis particular acorde con necesidades particulares

4.10. Como resultado de la evaluación del desempeño de los procesos de TI, en los casos que amerite, se deben plantear planes de mejora que consideren:

- la capacidad actual operativa y de gestión en la función de TI,



## TECNOLOGÍAS DE LA INFORMACIÓN Política: Monitoreo del desempeño de TI

Código: PL-TI-030

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

- disponibilidad y competencia de los recursos, y
- avance en el desarrollo de la cultura de calidad organizacional en la función de TI.

- 4.11. Las acciones de mejora inmediata que buscan normalizar el desempeño de uno o más procesos serán implementadas y oficializadas por el Comité de TI.
- 4.12. Las responsabilidades por la implementación de las acciones correctivas/preventivas, se definen como parte del respectivo plan de mejora asociado; estableciendo los plazos de ejecución y puntos de control para realizar su seguimiento.
- 4.13. Como resultado de cada evaluación del desempeño de los procesos se debe generar un informe consolidado de la gestión de TI, que indique en qué medida se lograron los objetivos planteados y se cumplieron las metas del desempeño, así como las estrategias de mejora a implementar para el mejoramiento continuo de los procesos de TI. Dicho informe es responsabilidad de Auditoría Interna y debe ser presentado a todos los interesados para su información y apoyo en la toma de decisiones.
- 4.14. Se debe registrar en una bitácora toda revisión y actualización al modelo de procesos de TI, indicando la fecha de la revisión, alcance, procesos modificados (de ser necesario) y responsables por la revisión y/o actualización.

### 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

### 6. Aprobación

#### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

#### 6.2 Aprobación por el Comité de Tecnologías de la Información

##### Acuerdo de aprobación por el Comité de Tecnologías de la Información

Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.

#### 6.3 Aprobación por la Junta Directiva del Inder

##### Acuerdo de aprobación por Junta Directiva

Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.

### 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
---------	-------	-------	-------	-----------------



**TECNOLOGIAS DE LA INFORMACIÓN**  
**Política: Monitoreo del desempeño de TI**

Código: PL-TI-030

Fecha de vigencia: 02/03/2011

Versión 2.0

Fecha de última actualización: 30/06/2017

2.0	Carmen Zuñiga Córdoba	Contraparte Técnica		
-----	-----------------------	------------------------	--	--



## TECNOLOGÍAS DE LA INFORMACIÓN

### Política: Restringir el acceso a los servidores del Centro de Datos

Código: PL-TI-031

Fecha de vigencia: 19/03/2018

Versión 3.0

Fecha de última actualización: 30/04/2017

#### 1. Objetivo

1.1 Prevenir el acceso físico no autorizado, daños a los activos e interrupciones a las actividades del Inder.

#### 2. Alcance

2.1 Esta política se aplica al acceso restringido al Centro de Datos de la institución, incluye a todos los funcionarios del Inder, terceros y usuarios de los recursos de Tecnología de Información, así como a todos los niveles de la estructura organizacional del Inder.

#### 3. Responsables

3.1 Administración Superior: Apoyar la Gestión de Seguridad de la Información, representada por esta política.

3.2 Auditoría Interna: Fiscalizar el cumplimiento de la política.

3.3 Tecnología de Información. Velar por el cumplimiento de lo estipulado en esta política

3.4 Funcionarios, terceros y usuarios: Conocer y aplicar lo estipulado en esta política.

#### 4. Pautas

4.1 El acceso físico al Centro de Datos será restringido o regulado por la jefatura a personas no autorizadas, debiéndose gestionar y documentar.

4.2 El Centro de Datos debe estar debidamente rotulado con la advertencia de acceso restringido en un lugar visible (puerta de ingreso).

4.3 El ingreso a esta área debe hacerse con autorización de la Encargada de Tecnología de Información, en caso de requerirse el ingreso de terceros, debe hacerse bajo la supervisión de un funcionario autorizado.

4.4 Para ingresar al Centro de Datos se debe portar tarjeta de acceso magnética personal con su respectivo código.

4.5 Las tarjetas de acceso magnético solamente las portará la Encargada de Tecnología de Información, así como el encargado de Redes y Telecomunicaciones, únicos autorizados a ingresar o autorizar ingreso de terceros.

4.6 Las tarjetas de acceso magnético son de índole personal No deben ser compartidas.

4.7 Los registros de accesos de las tarjetas magnéticas se deben conservar para mantener una revisión de los accesos y rutinas realizadas.

4.8 La Encargada de Tecnología de Información o quien se designe, se encargará de revisar al menos dos veces al año, los privilegios y derechos de las tarjetas de acceso para eliminar las que ya no lo requieren o bien otorgar nuevos privilegios y derechos.



## TECNOLOGÍAS DE LA INFORMACIÓN

### Política: Restringir el acceso a los servidores del Centro de Datos

Código: PL-TI-031

Fecha de vigencia: 19/03/2018

Versión 3.0

Fecha de última actualización: 30/04/2017

- 4.9 El ingreso y permanencia de personal externo al Centro de Datos por efectos de tareas de mantenimiento, aseo o reparación de equipos deberá contar con la supervisión permanente de un funcionario del área autorizado.
- 4.10 Si existiera alguna situación donde los autorizados para ingresar al Centro de Datos estén fuera de las instalaciones del Instituto, la Encargada de Tecnología de Información debe autorizar a otro funcionario de Tecnología de Información para el ingreso en el Centro de Datos.
- 4.11 El acceso al Centro de Datos fuera del horario ordinario del Inder, debe ser debidamente justificado con la Encargada de Tecnología de Información.
- 4.12 Todo acceso al Centro de Datos se concederá únicamente al personal designado por la Encargada de Tecnología de Información, cuyas responsabilidades de trabajo requieran el acceso a dicha instalación.
- 4.13 La pérdida o robo de las tarjetas de acceso magnéticas o claves deberán ser reportados a la jefatura de Tecnología de Información a los correos, [ivargas@inder.go.cr](mailto:ivargas@inder.go.cr), [xcastillo@inder.go.cr](mailto:xcastillo@inder.go.cr), incluyendo: nombre completo del funcionario, dependencia y circunstancias en las cuales sucedió el robo o pérdida.
- 4.14 Personal autorizado: Los accesos al Centro de Datos del Inder estarán restringidos sólo a encargados (a) de Tecnología de Información., y Telecomunicaciones. Los otros accesos a personal de servicio, oficiales de seguridad y otros actores estarán restringidos y según sea necesario se solicitará a la jefatura correspondiente para gestionar dichos privilegios. Cualquier otro tipo de personal deberá ingresar acompañado a las instalaciones.

## 5. Sanciones

El incumplimiento de esta política estará sujeto a una eventual sanción, previo debido proceso por parte de la Unidad de Relaciones Laborales.

## 6. Aprobación

### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

### 6.2 Aprobación por el Comité de Tecnologías de la Información

#### Acuerdo de aprobación por el Comité de Tecnologías de la Información

Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.

### 6.3 Aprobación por la Junta Directiva del Inder

#### Acuerdo de aprobación por Junta Directiva

Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.



**TECNOLOGÍAS DE LA INFORMACIÓN**  
**Política: Restringir el acceso a los servidores del Centro de Datos**

Código: PL-TI-031


Fecha de vigencia: 19/03/2018

Versión 3.0

Fecha de última actualización: 30/04/2017

**7. Historial de revisiones**

Versión	Autor	Cargo	Fecha	Cambio/Revisión
1.0	Comité de Tecnologías	Comité	28 enero 2015	Se incluye la pauta 4.10, la cual es una excepción en la política
2.0	Dixon Alvarez Valverde	TI- Gerencia General	5 abril 2016	Se solicita revisión según nota A-GG-029-2016 y remisión de documentos GG-430-2016, para ajustar la política acorde al lineamiento emitido en la circular N° 017-2015
3.0	Manuel Montero Ureña	Revisión y Ajustes.	29 agosto 2016	Se modifica la pauta 4.1  Se incluye la pauta 4.12, 4.13 y 5 para mejorar y validar el acceso al Centro de Datos, se ajusta la política acorde al lineamiento emitido en la circular N° 017-2015.

	<b>TECNOLOGIAS DE INFORMACIÓN</b>	
	<b>Política: Cambio de equipo de cómputo</b>	
	Código: PL-TI-032	Fecha de vigencia: 19/03/2018
Versión 2.0	Fecha de última actualización: 30/08/2016	

## 1. Objetivo

1.1 Proponer al Inder herramientas Tecnológicas acorde con las funciones, para adquirir o renovar equipo de Hardware o Software conforme a las necesidades de inversión a mediano y largo plazo de 1 a 5 años, permitiendo a los funcionarios del Inder tener mejor equipo para poder desarrollar sus funciones, garantizando la operatividad, la confiabilidad y la oportunidad de la información, base gerencial para la toma de decisiones.

## 2. Alcance

2.1 Esta política se aplica al Equipo de Cómputo de la institución, incluye a todos los funcionarios del Inder, terceros y usuarios de los recursos de Tecnología de Información, así como a todos los niveles de la estructura organizacional del Inder.

## 3. Responsables

3.1 Administración Superior: Apoyar la Gestión de Seguridad de la Información, representada por esta política.

3.2 Auditoría Interna: Fiscalizar el cumplimiento de la política.

3.3 Tecnología de Información. Velar por el cumplimiento de lo estipulado en esta política

3.4 Funcionarios de Activos, terceros y usuarios: Conocer y aplicar lo estipulado en esta política.

3.5 Área de Contratación administrativa

3.6 Unidad de Activos

3.7 Unidad de Relaciones Laborales, Para el manejo de discrepancias en la política


## 4. Pautas

4.1 **Estudio de necesidades:** Los recursos Informáticos a adquirirse deben considerar la arquitectura tecnológica del Inder que está en el plan de cambio de equipo de cómputo del Inder y su visión a futuro.

4.2 **Cambio de equipos por obsolescencia:** Tecnología de Información será la encargada de brindar la descripción de todos aquellos equipos informáticos de usuario final que a su criterio se encuentren obsoletos, con el fin de que sean sustituidos por equipo de punta, conforme con la disponibilidad presupuestaria existente, y de acuerdo a las necesidades de los usuarios. Todo equipo que sea desechado, se entregará a la Unidad de Activos, mediante la boleta respectiva de traslado, Tecnología de Información, no recibirá activos a su cargo, excepto aquellos que sean de su uso normal.

4.3 **Sondeo de Equipo:** Tecnología de Información realizara estudios respectivos a fin de conocer cuál es el equipo que más requiere en Inder para la función y satisfacción de las diferentes unidades administrativas, por lo menos 1 vez al año.

4.4 **Especificaciones Técnicas:** Tecnología de Información deberá mantener actualizada una lista de todos aquellos equipos que el Inder utiliza, con el propósito de que sea consultada como punto de referencia al momento de definir especificaciones técnicas que luego serán

 <b>Inder</b> <small>INSTITUTO DE DESARROLLO RURAL</small>	<b>TECNOLOGIAS DE INFORMACIÓN</b>	
	<b>Política: Cambio de equipo de cómputo</b>	
	Código: PL-TI-032	Fecha de vigencia: 19/03/2018
Versión 2.0	Fecha de última actualización: 30/08/2016	

incorporados a los carteles para la adquisición, dicho listado debe ser actualizado semestralmente por parte de los funcionarios de soporte técnico, esto con el propósito de incorporar nuevas tecnologías sobre Hardware acorde a la evolución del mercado.

**4.5 Recepción y revisión técnica de los equipos:** La Unidad de Activos, en coordinación con el Área de Contratación y Suministros, recibirá todos los equipos de cómputo que adquiera el Inder. Dichos equipos serán revisados por el área de soporte técnico, antes de ser recibidos a satisfacción. Los equipos que van a ser substituidos por obsolescencia deberán ser devueltos por los usuarios a la Unidad de Activos, para que ésta Unidad pueda entregar los nuevos activos a los usuarios correspondiente en las diferentes dependencias del Inder.

## 5. Sanciones

El incumplimiento de esta política estará sujeto al debido proceso por parte de la Unidad de Relaciones Laborales.

## 6. Aprobación

### 6.1 Aprobación y dictamen de conformidad técnica de Tecnologías de la Información

Nombre	Puesto	Firma
Ingrid Vargas González	Coordinadora a.i. Tecnologías de la Información	

### 6.2 Aprobación por el Comité de Tecnologías de la Información

<b>Acuerdo de aprobación por el Comité de Tecnologías de la Información</b>	Acuerdo #2 de la Sesión Ordinaria 004-2017 del Comité de Tecnologías de la Información del 27/07/2017.
---	--

### 6.3 Aprobación por la Junta Directiva del Inder

<b>Acuerdo de aprobación por Junta Directiva</b>	Acuerdo #8 de la Sesión Ordinaria 011-2018 de la Junta Directiva del Inder del 19/03/2018.
--	--

## 7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión
1.0	Dixon Alvarez Valverde	TI- Gerencia General	5 abril 2016	Se solicita revisión según nota A-GG-029-2016 y remisión de documentos GG-430-2016, para ajustar la política acorde al lineamiento emitido en la circular N° 017-2015
2.0	Manuel Montero Ureña	Revisión y Ajustes.	30 agosto 2016	Se modifica la pauta 4.5, readecuando la política acorde al lineamiento emitido en la circular N° 017-2015.



**TECNOLOGIAS DE INFORMACIÓN**  
**Política: Cambio de equipo de cómputo**

Código: PL-TI-032

Fecha de vigencia: 19/03/2018

Versión 2.0

Fecha de última actualización: 30/08/2016