





# POLÍTICAS DE CONTROL Y SEGURIDAD DE LOS RECURSOS INFORMÁTICOS DEL INSTITUTO NACIONAL DE BOSQUES -INAB-

## UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

FEBRERO - 2019  
Versión 1

Documentó:	Revisó:	Aprobó:
Departamento de Desarrollo Institucional	Unidad de Tecnologías de la Información y Comunicación	Gerencia
 Firma y Sello	 Firma y Sello	 Firma y Sello



Instituto Nacional de Bosques  
Más bosques. Más vida

**INSTITUTO NACIONAL DE BOSQUES -INAB-  
GUATEMALA, 14 DE FEBRERO DE 2019  
RESOLUCIÓN DE GERENCIA No. 029-2019**

**APROBACIÓN DE LAS POLÍTICAS DE CONTROL Y SEGURIDAD DE LOS  
RECURSOS INFORMÁTICOS DEL INSTITUTO NACIONAL DE BOSQUES –INAB-**

La Gerencia del Instituto Nacional de Bosques –INAB-

**CONSIDERANDO**

Que el Instituto Nacional de Bosques es una entidad estatal, autónoma, descentralizada, con personalidad jurídica, patrimonio propio e independencia administrativa; es el órgano de dirección y autoridad competente de sector Público Agrícola, en materia forestal.

**CONSIDERANDO**

Que la Ley Forestal, en su Artículo 16 regula las atribuciones del Gerente, que consisten en: dirigir, ejecutar y ordenar todas las actividades técnicas y administrativas del INAB; con base en las políticas, lineamientos y mandatos establecidos por la Junta Directiva, siendo responsable ante ésta por el correcto y eficaz funcionamiento del Instituto.

**CONSIDERANDO**

Que es necesario disponer de instrumentos técnicos actualizados que permitan optimizar las actividades dentro de la institución, en función de incrementar la eficiencia y productividad del desempeño de los objetivos y atribuciones del Instituto Nacional de Bosques.

**POR TANTO**

Esta Gerencia, con base en lo considerado y con fundamento en lo preceptuado en los Artículos: 5, 6 y 16 del Decreto 101-96 del Congreso de la República, Ley Forestal; Artículos: 1, 3, 4, 5, 6, y 18 del Reglamento Orgánico Interno del Instituto Nacional de Bosques aprobado por Resolución de la Junta Directiva del Instituto Nacional de Bosques Número JD.02.47.2018; y en el numeral 2 de las Normas Generales de Control Interno Gubernamental de la Contraloría General de Cuentas.





**RESUELVE**

- I. Aprobar la creación de las Políticas de Control y Seguridad de los Recursos Informáticos del Instituto Nacional de Bosques, de la Unidad de Tecnologías de la Información y Comunicación, integrado de la manera siguiente:

POLITICAS DE CONTROL Y SEGURIDAD DE LOS RECURSOS INFORMÁTICOS DEL INSTITUTO NACIONAL DE BOSQUES –INAB-		
Área	Dirigido a:	Políticas
Unidad de Tecnologías de la Información y Comunicación	Usuarios y accesos	Actualización de altas, bajas y traslados de personal para control de accesos a sistemas oficiales, red interna y correo electrónico
		Cuentas de usuario para acceso a red y correo electrónico
		Condiciones sobre uso de correo electrónico
		Condiciones sobre uso de red
		Usuarios de sistemas oficiales
	Soporte técnico y de sistemas	Soporte técnico
		Soporte de sistemas
	Uso del equipo de computación	Condiciones de confidencialidad
		Respeto de la propiedad intelectual
		Equipo asignado a cada usuario
	Requerimiento de software y hardware	Uso de equipos personales
		Centro de servidores
	Consultores externos	Toda solicitud de hardware o software
	Usos adecuados del recurso informático	Todo desarrollo de nuevos sistemas
		Toda instancia del INAB que contrate a consultores
Se entiende por uso aceptable		
Uso de dispositivos de almacenamiento externo	Se entiende por uso inaceptable	
	Se podrá utilizar dispositivos de almacenamiento externo de propiedad de la institución	
		Queda prohibido el uso de dispositivos de almacenamiento externo que no sean propiedad de la institución





POLITICAS DE CONTROL Y SEGURIDAD DE LOS RECURSOS INFORMÁTICOS DEL INSTITUTO NACIONAL DE BOSQUES -INAB-		
Área	Dirigido a:	Políticas
Unidad de Tecnologías de la Información y Comunicación	Mantenimiento de equipo de cómputo y redes internas	Mantenimiento de equipo de cómputo
		Mantenimiento de equipo de cómputo y redes internas
	Actualización de la página web	Estructura y funcionamiento del sitio
		Contenido de la pagina
	Protección de redes internas y cableado estructurado	Cableado estructurado
		Dispositivos de red
		Administración de dispositivos de red
	Copias de respaldo (Backup)	Ubicación de dispositivos de red
Backup centro de datos		
	Backup centro de cómputo	

- II. La presente resolución tiene vigencia inmediata y deja sin efecto cualquier otro procedimiento que contrarié los aquí contenidos.
- III. Notifíquese.


Ing. Rony Estuardo Granados Mérida  
Gerente



# CONTENIDO

PRESENTACIÓN.....	1
OBJETIVOS.....	1
RESPONSABILIDADES.....	2
A QUIEN APLICA LA POLÍTICA DEL RECURSO INFORMÁTICO .....	2
USUARIOS Y ACCESOS .....	3
Actualización de Altas, Bajas y Traslados de Personal para Control de Accesos a Sistemas Oficiales, Red Interna y Correo Electrónico .....	3
Cuentas de Usuario para Acceso a Red y Correo Electrónico .....	3
Condiciones sobre uso de Correo electrónico .....	4
Condiciones sobre uso de Red .....	4
Usuarios de sistemas oficiales.....	5
Condiciones de usuarios de sistemas y uso de sistemas .....	5
SOPORTE TECNICO Y DE SISTEMAS .....	5
Soporte técnico .....	5
Soporte de sistemas .....	6
Soporte de Sistemas por errores de código .....	6
Soporte de Sistemas por correcciones de información en Base de Datos.....	6
CONDICIONES DE CONFIDENCIALIDAD .....	6
RESPECTO DE LA PROPIEDAD INTELECTUAL .....	7
USO DEL EQUIPO DE COMPUTACIÓN .....	7
Equipo asignado a cada usuario:.....	7
Uso de equipos personales: .....	7
Centro de Servidores.....	8
REQUERIMIENTOS DE SOFTWARE Y HARDWARE .....	8
CONSULTORES EXTERNOS.....	8
USOS ADECUADOS DEL RECURSO INFORMÁTICO .....	8
Se entiende por uso aceptable: .....	8
Se entiende por uso inaceptable: .....	9
USO DE DISPOSITIVOS DE ALMACENAMIENTO EXTERNO .....	9
MANTENIMIENTO DE EQUIPO DE CÓMPUTO Y REDES INTERNAS .....	10
ACTUALIZACIÓN DE LA PÁGINA WEB.....	10

Estructura y funcionamiento del sitio .....	10
Contenido de la página .....	10
<b>PROTECCIÓN DE REDES INTERNAS Y CABLEADO ESTRUCTURADO.....</b>	<b>11</b>
Cableado Estructurado.....	11
Dispositivos de Red (switches, firewalls, Access point, router y otros relacionados a la red de datos) .....	11
Administración de Dispositivos de Red .....	11
Ubicación de Dispositivos de Red .....	11
<b>COPIAS DE RESPALDO (Backup) .....</b>	<b>12</b>
Backup Centro de datos .....	12
Backup Equipos de Cómputo .....	12


	<b>POLÍTICAS DE CONTROL Y SEGURIDAD DE LOS RECURSOS INFORMÁTICOS -INAB-</b>	Código:	POL-TIC.TIC-01
		Versión:	Versión 01
		Fecha de implementación:	FEBRERO 2019

## PRESENTACIÓN

*En virtud de que la estructura del Instituto Nacional de Bosques coloca a la Unidad de Tecnologías de la Información y Comunicación, como unidad de apoyo fundamental para el desarrollo de la institución en el uso tecnológico de sistemas y aplicaciones, esta Unidad con la intención de optimizar los recursos con que cuenta la institución aplica la presente política de uso a todo el personal del INAB que hace uso del recurso informático.*

## OBJETIVOS

- *Garantizar el buen uso de la información y de las tecnologías para ofrecer un buen servicio a todos los actores del Sector Forestal.*
- *Aprovechar por parte del usuario todo el Recurso Informático para el desarrollo de sus funciones.*
- *Utilizar por parte del usuario los recursos disponibles con cortesía y responsabilidad, respetando el derecho de otros usuarios.*

	<b>POLÍTICAS DE CONTROL Y SEGURIDAD DE LOS RECURSOS INFORMÁTICOS -INAB-</b>	Código:	POL-TIC.TIC-01
		Versión:	Versión 01
		Fecha de implementación:	FEBRERO 2019


## RESPONSABILIDADES

- *Todo usuario debe circunscribir su actuación en los servicios de Informática que presta el INAB a lo establecido en la presente política.*
- *Es responsabilidad de cada usuario adoptar las medidas necesarias que garanticen el cumplimiento de la Normativa para el uso de los equipos, software y licencias propiedad del INAB.*
- *Con el objeto de delimitar responsabilidades, es obligatorio que cada Director(a) y/o Jefe(a) de Oficina informe adecuadamente a todos sus miembros del alcance de sus responsabilidades en la utilización de nuestros equipos y de sus facilidades.*
- *Cada Director(a) Nacional, Regional, Subregional o Jefe(a) de Unidad es responsable de supervisar el uso adecuado de los recursos informáticos, cualquier anomalía deberá hacer uso de las herramientas proporcionadas por el Reglamento Interior de Trabajo.*
- *El usuario que haya instalado software ilegal en su equipo, se hace responsable de las consecuencias establecidas de la ley de propiedad intelectual.*
- *La violación de responsabilidades será sancionada de acuerdo a acciones determinadas por la aplicación del Reglamento Interior de trabajo del INAB.*

## A QUIEN APLICA LA POLÍTICA DEL RECURSO INFORMÁTICO

*Esta política se aplica a todo usuario de recursos informáticos, internet y de red del INAB tanto para personal Interno como externo. (Todo usuario debe respetar y cumplir la presente política)*



	<p style="text-align: center;"><b>POLÍTICAS DE CONTROL Y SEGURIDAD DE LOS RECURSOS INFORMÁTICOS -INAB-</b></p>	Código:	POL-TIC.TIC-01
		Versión:	Versión 01
		Fecha de implementación:	FEBRERO 2019

## USUARIOS Y ACCESOS

### Actualización de Altas, Bajas y Traslados de Personal para Control de Accesos a Sistemas Oficiales, Red Interna y Correo Electrónico

*Por tratarse de un tema de control de personal, la Dirección de Desarrollo Institucional y Recursos Humanos debe de enviar de forma electrónica a la Unidad de Tecnologías de la Información y Comunicación, así como a los Administradores de los Sistemas Oficiales la actualización de las Altas, Bajas y Traslados de personal en el momento que estos se generen, con la información siguiente:*


- *Nombre completo*
- *DPI*
- *Dirección, Unidad, Departamento, Región o Subregión a la que pertenece.*
- *Cargo (Para definir el tipo de perfil para uso de la red)*
- *Fecha en la cual entra en vigencia.*
- *Fecha Final de contrato (para bajas)*
- *Para el caso de Altas y Traslados, adjuntar nombramiento de forma escaneada.*

*Con esta información es responsabilidad de la Unidad de Tecnologías de la Información y Comunicación, actualizar los accesos a Red Interna y Correo Institucional, y para el caso de los Administradores de los Sistemas Oficiales la actualización de los accesos a los usuarios de dichos sistemas.*

### Cuentas de Usuario para Acceso a Red y Correo Electrónico

*Toda solicitud de usuario para la red interna con sus accesos de acuerdo a las funciones dentro del INAB se debe realizar a la Unidad de Tecnologías el cual debe ser solicitado por el (la) Director(a) Nacional, Regional, Subregional o Jefe(a) de Unidad, por medio de Oficio o desde Correo Institucional. Esta información se cotejará con la data que actualiza la Dirección de Desarrollo Institucional y Recursos Humanos.*

*Para la eliminación de cuentas se utilizará el mismo procedimiento.*

	<b>POLÍTICAS DE CONTROL Y SEGURIDAD DE LOS RECURSOS INFORMÁTICOS -INAB-</b>	Código:	POL-TIC.TIC-01
		Versión:	Versión 01
		Fecha de implementación:	ENERO 2019


### **Condiciones sobre uso de Correo electrónico**

- a) *La Unidad de Tecnologías de la Información y Comunicación utilizará la siguiente nomenclatura para la cuenta de correo electrónico institucional para su creación: <primer\_nombre>.<primer\_apellido>@inab.gob.gt, si en dado caso existiera un homónimo, se considerará utilizar segundo nombre, o segundo apellido, cualquier otra variante debe ser solicitada por el (la) Director(a) Nacional, Regional, Subregional o Jefe(a) de Unidad con la justificación.*
- b) *Cada usuario es responsable del uso adecuado del correo electrónico, el cual es para uso exclusivo de las funciones institucionales, no puede utilizarlo para fines personales.*
- c) *No puede ceder el uso de cuenta de correo por tratarse de un nombre que identifica la cuenta de correo.*
- d) *El usuario es responsable de suscripciones ajenas a la institución que provoquen el ingreso de correo no deseado o con contenido malicioso.*
- e) *Únicamente está permitido el envío de documentos oficiales y además no debe exceder en enviar correo con adjuntos superiores a los 5mb.*
- f) *No puede utilizar el correo para enviar información más de 30 destinatarios, para ello debe requerir la asistencia de la Unidad de Tecnologías de la Información y Comunicación, para el envío de correo masivo el cual se hace por medio de una plataforma comprada para uso de la institución, y así evitar comprometer el correo, el dominio o la misma red de INAB.*

### **Condiciones sobre uso de Red**

*El acceso a la red permite el uso de recursos como impresoras y escáner de red, uso de internet, actualización y protección de información desde conexiones externas de la red pública de internet.*

- a) *El acceso a la red Interna es para uso exclusivo para aprovechar los recursos que se proporcionan para el desarrollo de las funciones de los usuarios.*
- b) *Utilizar el internet únicamente para uso del desarrollo de funciones de los usuarios.*
- c) *No se permite el uso indebido de la red para oír música, Radio, Streaming de Video, películas, redes sociales, descarga de contenido de dudosa procedencia que pueda comprometer la seguridad de la información y la estabilidad de la conexión del internet.*
- d) *Es responsabilidad del Usuario el buen uso del internet.*

	<p style="text-align: center;"><b>POLÍTICAS DE CONTROL Y SEGURIDAD DE LOS RECURSOS INFORMÁTICOS -INAB-</b></p>	Código:	POL-TIC.TIC-01
		Versión:	Versión 01
		Fecha de implementación:	ENERO 2019

e) *El acceso a páginas de dudosa reputación, donde se comparten variedad de archivos, los cuales son focos de contaminación de virus, spyware, malware y otros tipos de infección de los cuales es responsabilidad del usuario el acceso a los mismos, a los cuales está prohibido.*

## **Usuarios de sistemas oficiales**

*Toda solicitud de usuario para acceso a los sistemas oficiales de acuerdo a las funciones dentro de los procesos de los mismos se debe realizar al Administrador del Sistema, el cual debe ser solicitado por el (la) Director(a) Nacional, Regional, Subregional o Jefe(a) de Unidad, por medio de Oficio o desde Correo Institucional esta información se cotejará con la información que actualiza la Dirección de Desarrollo Institucional y Recursos Humanos.*


## **Condiciones de usuarios de sistemas y uso de sistemas**

- *Cada usuario es responsable del uso adecuado de sus accesos a los Sistemas oficiales, el cual es para uso exclusivo de las funciones institucionales.*
- *No puede ceder el uso de su usuario dentro ni fuera de la institución.*
- *No puede utilizar cuentas de otro usuario.*
- *Es responsable de todas las acciones que se realiza con su usuario en los Sistemas Oficiales.*
- *La información de los sistemas es de uso exclusivo de la institución no se puede extraer parcial, ni totalmente información para propósitos personales y/o ajenos a la institución.*
- *Cualquier situación anómala en su acceso debe de informarlo de forma inmediata al Administrador de Sistemas y solicitar los cambios de credenciales.*

## **SOPORTE TECNICO Y DE SISTEMAS**

### **Soporte técnico**

*El soporte técnico se realizará a solicitud del interesado por medio de correo electrónico, llamada u oficio. El soporte entrará a la Unidad de Tecnologías de la Información y Comunicación, para la asignación del técnico que atenderá. El soporte puede ser remoto o en sitio según sea el caso, atendiendo problemas de conectividad, impresión, correo electrónico,*

	<p style="text-align: center;"><b>POLÍTICAS DE CONTROL Y SEGURIDAD DE LOS RECURSOS INFORMÁTICOS -INAB-</b></p>	Código:	POL-TIC.TIC-01
		Versión:	Versión 01
		Fecha de implementación:	ENERO 2019

*configuraciones, reparación de software y/o hardware etc. Este proceso esta definido en los manuales de procedimientos de la Unidad de Tecnologías de la Información y Comunicación.*

## **Soporte de sistemas**

*La Unidad de Tecnologías de la Información y Comunicación, tiene la responsabilidad de mantener los sistemas en línea 24x7, aplicar actualizaciones y copias de respaldo de información de sus bases de datos, de forma semanal.*

*El soporte de sistemas tiene dos variantes:*

### **Soporte de Sistemas por errores de código**


*Este soporte se recibe solo a solicitud del Administrador de Sistemas para corrección de errores propios de funcionamiento del sistema, el cual debe ser solicitado por medio de correo electrónico u oficio a la Unidad de Tecnologías de la Información y Comunicación, toda vez la Unidad posea el control del código fuente, de lo contrario deberá atenderlo el Desarrollador a responsable del código.*

### **Soporte de Sistemas por correcciones de información en Base de Datos**

*Este tipo de soporte debe ser solicitado por medio de Oficio o Correo Electrónico por el Director(a) Regional o Subregional quien previamente analizó las implicaciones de los cambios en la información almacenada, y es resuelta por el Administrador(a) de Sistemas, si la corrección implica cambiar estructura de información de base de datos deberá hacerlo a la Unidad de Tecnologías de la Información y Comunicación, toda vez la Unidad posea el control del código fuente, de lo contrario deberá atenderlo el Desarrollador a responsable del código.*

## **CONDICIONES DE CONFIDENCIALIDAD**

*Está prohibido acceder a la información propiedad de otros usuarios, aun cuando estos últimos no las hayan protegido explícitamente. Esta regla también se aplica a las conversaciones privadas, de tipo correo electrónico, sin haber sido el destinatario directo o puesto en copia de dichas conversaciones.*

	<b>POLÍTICAS DE CONTROL Y SEGURIDAD DE LOS RECURSOS INFORMÁTICOS -INAB-</b>	Código:	POL-TIC.TIC-01
		Versión:	Versión 01
		Fecha de implementación:	ENERO 2019

## **RESPECTO DE LA PROPIEDAD INTELECTUAL**

*El uso de los programas informáticos y de los datos debe realizarse en el respeto de la propiedad intelectual. Muy en especial:*

- a) Las licencias de software adquiridas por INAB son de uso exclusivo para la institución no pueden ser utilizadas en otros equipos que no sean propiedad de INAB.*
- b) Esta igualmente prohibido instalar, sobre cualquier equipo propiedad del INAB, cualquier programa informático sin licencia legalmente adquirida y/o sin autorización respectiva, toda instalación debe ser realizada por la Unidad de Tecnologías, para garantizar la seguridad del equipo y el buen funcionamiento.*

## **USO DEL EQUIPO DE COMPUTACIÓN**


*Las siguientes Normas han sido diseñadas para ser observadas por todo el personal dentro del INAB.*

### **Equipo asignado a cada usuario:**

- ✓ *El usuario es responsable del equipo asignado para elaborar su trabajo.*
- ✓ *Si el equipo es utilizado fuera de las oficinas, deberá tomar las respectivas precauciones, y sujetarse a las condiciones sobre reposición de bienes inventariables en caso de robo o extravío.*
- ✓ *El usuario debe de buscar un lugar adecuado para colocar el equipo de cómputo para el caso de equipos de escritorio, el cual no debe colocar en el suelo, debe estar en ambiente adecuado, sobre el escritorio, si por espacio es necesario poner el CPU en el suelo, debe estar sobre una superficie aislante entre el suelo y el equipo.*
- ✓ *Los equipos UPS se deben utilizar solo para respaldar por energía únicamente a equipos de cómputo, a estos no se debe conectar fotocopiadoras, escáner, ni impresoras láser los cuales por respaldo de altibajos de corriente únicamente se les debe conectar a reguladores de voltaje según capacidad de los mismos.*

### **Uso de equipos personales:**

- ✓ *Si por casos fortuitos se requiere el uso de equipo personal, el Director(a) Nacional, Regional, Subregional o Jefe(a) de Unidad debe solicitar el acceso a la red de INAB de dicho equipo,*

	<p style="text-align: center;"><b>POLÍTICAS DE CONTROL Y SEGURIDAD DE LOS RECURSOS INFORMÁTICOS -INAB-</b></p>	Código:	POL-TIC.TIC-01
		Versión:	Versión 01
		Fecha de implementación:	ENERO 2019

*considerando que el mismo debe ser sometido a una revisión exhaustiva sobre tipos de programas instalados, Virus etc., que ponga en riesgo la seguridad de la red del INAB, o comprometa la estabilidad de la conexión y ancho de banda.*

## **Centro de Servidores**

- ✓ *El centro de servidores debe permanecer cerrado, el cual está bajo custodia de la Unidad de Tecnologías de la Información y Comunicación, no se permite el ingreso de personal no autorizado a dicha instalación, el ingreso al mismo deberá registrarse con una bitácora donde se indicará, nombre, fecha, hora y motivo del ingreso a los servidores.*

## **REQUERIMIENTOS DE SOFTWARE Y HARDWARE**

- ✓ *Toda solicitud de hardware o software debe ser canalizada a través de la Unidad de Tecnologías de la Información y Comunicación, tanto para su cotización, compra y recepción.*
- ✓ *Todo desarrollo de nuevos sistemas por consultoría externa deberá ser avalado por la Unidad de Tecnologías de la Información y Comunicación, para delimitar los lineamientos de desarrollo tipo de tecnología, lenguaje de programación y metodología.*

## **CONSULTORES EXTERNOS**

*Toda instancia del INAB que contrate a consultores externos que necesiten hacer uso de los recursos de internet del INAB, debe solicitar a la Unidad de Tecnologías de la Información y Comunicación, por correo u oficio un permiso temporal para consultor, el cual consiste en un acceso con tiempo limitado.*


## **USOS ADECUADOS DEL RECURSO INFORMATICO**

### **Se entiende por uso aceptable:**

*El intercambio de información, cuyo contenido sea académico, educacional o de investigación. La utilización eficiente de la red, con el fin de evitar en la medida de lo posible la congestión de la misma.*

*Esto se logra con:*

- a) *Guardar toda la información Institucional únicamente en la carpeta de Mis Documentos.*

	<p style="text-align: center;"><b>POLÍTICAS DE CONTROL Y SEGURIDAD DE LOS RECURSOS INFORMÁTICOS -INAB-</b></p>	Código:	POL-TIC.TIC-01
		Versión:	Versión 01
		Fecha de implementación:	ENERO 2019

- b) *Clasificar la información con un máximo de cuatro sub-niveles de carpetas*
- c) *Utilizar nombres cortos para los nombres de archivos y/o Carpetas*
- d) *Hacer uso de nombres cortos para carpetas y/o archivos.*

### **Se entiende por uso inaceptable:**

- a) *La instalación de software sin la autorización del administrador de la red.*
- b) *Utilizar los recursos de la red para descargas de archivos no autorizados. Archivos ejecutables de dudosa procedencia, música, videos u otros considerados perjudiciales al rendimiento del ancho de banda en la red.*
- c) *Utilizar los diferentes dispositivos de almacenamiento (CD, DVD, USB, discos duros internos y externos, etc.) propiedad del INAB para almacenar música, videos, fotos y/o cualquier tipo de archivo ajeno a actividades laborales.*
- d) *El uso de los equipos y la red con fines privados, personales o comerciales.*
- e) *Intentar conectarse a un sitio Internet sin ser autorizado por cualquiera de estas vía ftp, telnet, ssh u otro con algún puerto determinado sin permiso.*
- f) *Cualquier intento de usurpar otra identidad o de interceptar comunicaciones entre terceras personas.*


### **USO DE DISPOSITIVOS DE ALMACENAMIENTO EXTERNO**

*Se entiende por almacenamiento externo a dispositivos tales como discos duros externos, Memorias USB o micro USB, CD o DVD Regrabables, o cualquier otro con fines de almacenamiento externo.*

*Se podrá utilizar dispositivos de almacenamiento externo de propiedad de la Institución, para usos exclusivos de procesos controlados:*

1. *Para copia de respaldo interno (Backup) o*
2. *Traslado y/o Recuperación de información de un equipo institucional a otro el cual debe estar autorizado por el Director(a) y/o Jefe(a) a cargo de la oficina.*

*Queda prohibido el uso de dispositivos de almacenamiento externo que no sean propiedad de la institución, quedando bajo responsabilidad del Director(a) o Jefe(a) de oficina autorizar en casos de emergencia el uso de los mismos quedando bajo su responsabilidad el control y*

	<p style="text-align: center;"><b>POLÍTICAS DE CONTROL Y SEGURIDAD DE LOS RECURSOS INFORMÁTICOS -INAB-</b></p>	Código:	POL-TIC.TIC-01
		Versión:	Versión 01
		Fecha de implementación:	ENERO 2019

*monitoreo del uso de los mismos, con el fin de garantizar la confidencialidad de la información institucional.*

*Cualquier extracción de información institucional con fines personales será sancionada de acuerdo al reglamento interior de trabajo de INAB.*

## **MANTENIMIENTO DE EQUIPO DE CÓMPUTO Y REDES INTERNAS**

*El mantenimiento del equipo de cómputo se realizará a través de la Unidad de tecnologías, de acuerdo a la factibilidad lo realizará por medio del personal de la Unidad o por a través de contratación de terceros en coordinación con los Delegados(as) administrativos(as) para las oficinas Regionales y Subregionales.*

*El mantenimiento de los Equipos de cómputo y Redes Internas, se deben realizar al menos 2 veces al año, de los cuales la Unidad de Tecnologías de la Información y Comunicación anualmente enviará planificación para su ejecución.*

## **ACTUALIZACIÓN DE LA PÁGINA WEB**

### **Estructura y funcionamiento del sitio**


*La Unidad de Tecnologías de la Información y Comunicación, es la encargada de mantener en línea y en funcionamiento 24x7 el sitio Web Institucional, así como el desarrollo de la maqueta del sitio y su estructura para la administración del contenido.*

### **Contenido de la página**

*Es responsabilidad de la Unidad de Comunicación Social la actualización del contenido dinámico de notas, anuncios, videos y otros.*

*De la misma manera es responsabilidad de las Direcciones Sustantivas y de apoyo actualizar la información del sitio de INAB mensualmente, la cual debe trasladarse a la Unidad de Comunicación Social para su validación y publicación.*



	<b>POLÍTICAS DE CONTROL Y SEGURIDAD DE LOS RECURSOS INFORMÁTICOS -INAB-</b>	Código:	POL-TIC.TIC-01
		Versión:	Versión 01
		Fecha de implementación:	ENERO 2019

*El Acceso a la Información Pública a través de la Unidad de Asuntos Jurídicos, debe actualizar información según la ley, solicitando a los encargados de los temas la información que corresponda, para ser validados y publicados.*

## **PROTECCIÓN DE REDES INTERNAS Y CABLEADO ESTRUCTURADO**

### **Cableado Estructurado**

*El cableado de comunicación de voz (IP) y datos esta a cargo de la Unidad de Tecnologías de la Información y Comunicación, este cableado no puede ser instalado por otro personal que no esté autorizado por la Unidad TIC's, de acuerdo a la factibilidad y emergencia, la Unidad TIC's puede delegar a través de contratación de terceros la instalación de la red de datos siguiendo los estándares y lineamientos de seguridad para la instalación, y así garantizar la efectiva comunicación de la red Interna.*


### **Dispositivos de Red (switches, firewalls, Access point, router y otros relacionados a la red de datos)**

#### **Administración de Dispositivos de Red**

*El personal de la Unidad de Tecnologías de la Información y Comunicación, es la única autorizada para administrar los dispositivos de Red, a excepción en casos de emergencia para oficinas remotas (fuera del perímetro de la capital) se solicitará apoyo al personal local para la manipulación de los mismos, para lo cual solamente será posible en coordinación con el Director(a) o Jefe(a) de la Oficina quien autorizará al personal de apoyo.*

#### **Ubicación de Dispositivos de Red**

*Los dispositivos de Red, deben estar resguardados dentro de un gabinete, o bien en un Rack de pared en un punto medio de la oficina para garantizar óptimo rendimiento por la distancia a los puntos de acceso, deben estar independientes de contacto con cualquier otro dispositivo que no tenga relación con la Red de datos y/o Internet.*

	<p style="text-align: center;"><b>POLÍTICAS DE CONTROL Y SEGURIDAD DE LOS RECURSOS INFORMÁTICOS -INAB-</b></p>	Código:	POL-TIC.TIC-01
		Versión:	Versión 01
		Fecha de implementación:	ENERO 2019

## **COPIAS DE RESPALDO (Backup)**

### **Backup Centro de datos**

*La Unidad de Tecnologías de la Información y Comunicación es la responsable de realizar backup de todas las Bases de datos Institucionales que se encuentran en el Data Center, así como de los sistemas (código fuente y versión publicada) de forma semanal.*

### **Backup Equipos de Cómputo**

- *Cada usuario es responsable del manejo de la información de la Institución a su cargo y de realizar de forma planificada copias de respaldo (Backup`s) del equipo a cargo haciendo uso de unidades de almacenamiento externo (Discos Duros externos), propiedad de INAB de forma mensual.*
- *Cada Director(a) Nacional, Regional, Subregional o Jefe(a) de Unidad es responsable de supervisar que todo el personal a su cargo cumpla con el proceso de respaldar (backup) cada mes de la información institucional.*
- *Las copias de respaldo solo se harán a los archivos institucionales de acuerdo a las funciones de cada empleado.*
- *No se deben incluir en las copias de respaldo Música, Películas, Videos, imágenes u otro material ajeno a la institución.*