INSTITUTO NACIONAL DE BOSQUES -INAB-
GUATEMALA, 19 DE DICIEMBRE DE 2024
RESOLUCIÓN DE GERENCIA No. 189-2024

APROBACIÓN DE LAS POLÍTICAS DE CONTROL Y SEGURIDAD DE LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN 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 del sector público agrícola en materia forestal.

CONSIDERANDO

Que la Ley Forestal, en el artículo 16 regula las atribuciones del Gerente, que consisten en dirigir, ejecutar y ordenar 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 y procedimientos realizados dentro de la Unidad de Tecnologías de la Información y Comunicación del Instituto Nacional de Bosques -INAB-; en función de incrementar la eficiencia y productividad del desempeño de los objetivos y atribuciones del Instituto Nacional de Bosques -INAB-.

POR TANTO

Esta Gerencia, con base en lo considerado y con fundamento en lo preceptuado en los artículos: 5, 6 y 16 del Decreto Número 101-96 del Congreso de la República, Ley Forestal; y, artículos: 1, 3, 4, 5 y 7 del Reglamento Orgánico Interno del INAB aprobado mediante Resolución Número JD.06.46.2023 de la Junta Directiva del Instituto Nacional de Bosques.

RESUELVE

I. Aprobar la actualización de las Políticas de Control y Seguridad de la Unidad de Tecnologías de la Información y Comunicación del Instituto Nacional de Bosques -INAB-; Versión 3; como instrumento mediante el cual se fomenta el buen uso de la información y acceso a la tecnología como apoyo en los procesos institucionales y a la prestación de servicios de calidad de los usuarios.

INSTITUTO NACIONAL DE BOSQUES. ASUNTOS JURIDICOS -INAB- GUATEMALA, C.A.

II. Es responsabilidad del Jefe (a) de la Unidad de Tecnologías de la Información y Comunicación socializar el contenido de las Políticas de Control y Seguridad de la Unidad de Tecnologías de la Información y Comunicación del Instituto Nacional de Bosques -INAB-; Versión 3; y proponer las actualizaciones al contenido de las mismas.

III. Todo funcionario y empleado del Instituto Nacional de Bosques -INAB-; es responsable de aplicar los requisitos que establecen las Políticas de Control y Seguridad de la Unidad de Tecnologías de la Información y Comunicación del Instituto Nacional de Bosques -INAB-; Versión 3; y ejecutar cualquier otro documento destinado a su implementación.

IV. El Departamento de Gestión de la Calidad de la Dirección de Planificación, Evaluación y Seguimiento Institucional archivará y custodiará en formato físico y digital el original de las Políticas de Control y Seguridad de la Unidad de Tecnologías de la Información y Comunicación del Instituto Nacional de Bosques -INAB-; Versión 3, debidamente aprobadas por el Gerente del Instituto Nacional de Bosques -INAB-.

V. La presente resolución tiene vigencia inmediata y deja sin efecto cualquier otra disposición que contraríe lo aquí establecido.

VI. Notifíquese.

Instituto Nacional de Bosques GERENCIA INAB

Ing. Bruno Enrique Arias Rivas
Gerente

INSTITUTO NACIONAL DE BOSQUES GUATEMALA, C.A. ASUNTOS JURIDICOS -INAB-

¡La calidad la hacemos todos!

Instituto Nacional de Bosques ISO 9001:2015 CERTIFICADO

POLÍTICAS DE CONTROL Y SEGURIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN -INAB-

UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Versión: 3

Número de páginas: 18

Elaboró	Aprobó
Jefe (a) de Unidad de Tecnologías de la Información y Comunicación	Gerente
Mgtr. Aldo Ernesto Ali Barrera Dor[illegible] Jefe de Unidad de Tecnologías de la Información y Comunicación (Firma y sello)	(Firma y sello)

Orientación y acompañamiento: Departamento de Gestión de la Calidad	(Firma y sello)

PRESENTACIÓN

El Instituto Nacional de Bosques -INAB- fue creado mediante el Decreto del Congreso de la República de Guatemala Número 101-96 Ley Forestal, en el año 1996, como el órgano de dirección y autoridad competente del sector público agrícola en materia forestal, teniendo como marco de acción institucional, la administración de los bosques del país fuera de áreas protegidas.

VISIÓN

El Instituto Nacional de Bosques es una institución líder y modelo en la gestión de la política forestal nacional, reconocida nacional e internacionalmente por su contribución al desarrollo sostenible del sector forestal en Guatemala, propiciando mejora en la economía y en la calidad de vida de su población, y la reducción de su vulnerabilidad al cambio climático.

MISIÓN

Ejecutar y promover los instrumentos de política forestal nacional, facilitando el acceso a los servicios forestales que presta la institución a los actores del sector forestal, mediante el diseño e impulso de programas, estrategias y acciones que generen un mayor desarrollo económico, ambiental y social del país.

CONTENIDO

I. INTRODUCCIÓN

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 las presentes políticas a todo el personal del INAB que hace uso del recurso informático.

II. OBJETIVOS

- Garantizar el buen uso de la información y de las tecnologías para ofrecer un servicio de calidad a todos los actores del sector forestal.
- Aprovechar por parte del usuario interno 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.

III. RESPONSABLES

1. El personal de la Unidad de Tecnologías es responsable de regirse en sus acciones en torno a estas políticas para garantizar el buen funcionamiento.
2. Todo usuario debe circunscribir su actuación en los servicios de Informática que presta el INAB a lo establecido en las presentes políticas.
3. 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.
4. 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.
5. 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.
6. La violación de responsabilidades será sancionada de acuerdo a acciones determinadas por la aplicación del Reglamento Interior de trabajo del INAB.

IV. ALCANCE

El alcance aplica para personal interno y externo que haga uso de recursos informáticos, internet y de red del INAB (todo usuario debe respetar y cumplir las presentes políticas).

V. POLÍTICA DE SEGURIDAD INFORMÁTICA

El INAB a través de la Unidad de Tecnologías de la Información y Comunicación establece lineamientos de seguridad para el buen manejo del equipo de tecnología, accesos y usos de sistemas informáticos.

5.1 Usuarios, cuentas de correo y accesos

5.1.1 Creación de usuarios de red interna y correo electrónico

Para la creación de usuarios nuevos para acceso a red y cuenta de correo electrónico es necesario recibir la solicitud vía correo electrónico institucional u oficio por parte del jefe inmediato superior, quien debe adjuntar nombramiento escaneado acompañado de la siguiente información del nuevo usuario.

- Nombre completo.
- Fotocopia de DPI.
- Dirección, Unidad, Departamento, Región o Subregión a la que pertenece.
- Cargo (Para definir el tipo de perfil para uso de la red).

Esta información se cotejará con los datos que actualiza la Dirección de Recursos Humanos, Desarrollo Institucional y Formación de Personal. Para la inactivación de cuentas de correo y accesos a Red se utilizará el mismo procedimiento.

5.1.2 Condiciones sobre 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. Dicha solicitud debe ser por medio de correo electrónico Institucional u oficio.

b) Cada usuario es responsable del uso adecuado del correo electrónico, el cual es para uso exclusivo de las funciones institucionales, no puede utilizarse para fines personales.

c) No puede ceder el uso de la 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 correos con archivos adjuntos superiores a los 5 Mb.

f) No puede utilizar el correo para enviar información a 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 de pago adquirida para uso de la institución, y así evitar comprometer el correo, el dominio o la misma red de INAB.

5.1.3 Creación de usuarios de sistemas oficiales

Toda solicitud de usuario para acceso a los sistemas oficiales de acuerdos 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, adjuntando nombramiento acompañado de la siguiente información del nuevo usuario.

- Nombre completo.
- Fotocopia de DPI.
- Dirección, Unidad, Departamento, Región o Subregión a la que pertenece.
- Cargo (Para definir el tipo de perfil en sistema).

La información anterior se cotejará con los datos que actualiza la Dirección de Recursos Humanos, Desarrollo Institucional y Formación de Personal. Para la inactivación de usuarios se utilizará el mismo procedimiento.

5.1.4 Normas y uso de contraseñas seguras para sistemas

Para garantizar la seguridad en el acceso a los sistemas de información oficiales se establecen los siguientes lineamientos:

- Cada usuario al crear su contraseña debe considerar que la misma tiene que estar constituida por al menos 8 caracteres de los cuales debe contener al menos una letra mayúscula, una letra minúscula, un número y un carácter especial.
- No utilizar nombres, fechas o datos personales que hagan alusión al titular de la credencial.
- El cambio de contraseña se debe realizar al menos 2 veces al año.

- 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 accesos de otro usuario.
- El usuario es responsable de todas las acciones que se realiza con sus credenciales 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 (a) de Sistemas y solicitar los cambios de credenciales.
- Cualquier incumplimiento de los lineamientos descrito anteriormente debe ser sancionado de acuerdo al Reglamento Interior de Trabajo.

5.1.5 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 Recursos Humanos, Desarrollo Institucional y Formación de Personal 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.
- Fotocopia de 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 fin de contrato (para bajas).

Con esta información es responsabilidad de la Unidad de Tecnologías de la Información y Comunicación, actualizar los accesos a la 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.

5.1.6 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 explícitamente oír música, radio, streaming de video, compartir internet por medio de equipo personal a teléfonos personales, 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.

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.

f) Todos los equipos que sean donados a INAB deben de ser reportados a la Unidad de Tecnología de la Información y comunicación por el Director (a) Nacional, Regional, Subregional o Jefe de Unidad o por medio de oficio o correo institucional para la configuración del mismo.

5.1.7 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.

5.2 Seguridad del centro de datos

El centro de datos 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, DPI, fecha, hora, firma y motivo del ingreso y salida a los servidores. El acceso está restringido.

5.3 Soporte técnico y de sistemas

5.3.1 Soporte técnico

El soporte técnico se realizará a solicitud del interesado por medio de correo electrónico institucional, 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, configuraciones, reparación de software y/o hardware etc. Este proceso está definido en los manuales de procedimientos de la Unidad de Tecnologías de la Información y Comunicación.

5.3.2 Soporte de sistemas

El soporte de sistemas tiene dos variantes:

5.3.2.1 Soporte de sistemas por actualizaciones en código

Este soporte se recibe solo a solicitud del Administrador (a) 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 o responsable del código.

5.3.2.2 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 resuelto por el Administrador (a) de Sistemas; si la corrección implica cambiar información dentro de la estructura de la base de datos, el Administrador (a) del Sistema deberá trasladarlo a la Unidad de Tecnologías de la Información y Comunicación, toda vez la Unidad posea el control de la base de datos, de lo contrario deberá atenderlo el (la) Desarrollador (a) responsable del Sistema.

VI. POLÍTICA DE ADQUISICIÓN DE SOFTWARE Y HARDWARE

6.1 Requerimientos de software y hardware

6.1.1 Software

a. Toda solicitud de software debe ser canalizada a través de la Unidad de Tecnologías de la Información y Comunicación para su evaluación, la cual consistirá:

   - Compatibilidad con equipos y sistemas operativos.
   - Capacidad del recurso humano para configuración y uso de software.

- Capacidad financiera para licencias de software por pagos únicos, y en otro caso para licencias por suscripción anual.

b. El mantenimiento y configuración del software institucional adquirido está a bajo la responsabilidad del personal que lo tenga en uso.

c. La instalación de software de uso general de todos los equipos institucionales está a cargo de la Unidad de Tecnologías, para software de uso específico está a cargo del responsable del uso de la aplicación.

6.1.2 Hardware

a. Toda solicitud de equipo de escritorio o laptop debe estar dentro de las especificaciones técnicas establecidas por la Unidad de Tecnologías en conjunto con la Subgerencia, la cual se definirá al inicio de cada año de las siguientes características mínimas de:

- Capacidad de memoria RAM.
- Capacidad de disco duro interno.
- Tipo de procesador, generación y velocidad de procesamiento.
- Tipos de puertos de entrada y salida.
- Dispositivos periféricos.
- Sistema operativo adecuado para asociarse al directorio activo institucional.
- Tipo y tamaño de pantalla.
- Marca reconocida, no equipos clonados.
- Soporte local de la marca con atención en sitio.
- Garantía y verificación de garantía desde sitio oficial de la marca.

En el caso de dispositivos para protección de energía, los criterios de la capacidad se definirán de acuerdo al equipo al que estará protegiendo contra altibajos de corriente, además considerar:

- Marca reconocida.
- Soporte local de la marca con atención en sitio.

Para otro tipo de hardware se debe considerar:

- Marca reconocida.
- Soporte local de la marca.

- Costo de consumibles.

La Dirección o Unidad que gestione la adquisición de software o hardware debe solicitar el visto bueno a la Unidad de Tecnologías como garantía de la factibilidad técnica previa realizada para garantizar lo conveniente para la institución.

6.1.3 Respeto 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) Está prohibido instalar en cualquier equipo propiedad del INAB, cualquier programa informático sin licencia legalmente adquirida y/o sin autorización respectiva, toda instalación debe ser autorizada por la Unidad de Tecnologías, para garantizar la seguridad del equipo y el buen funcionamiento.

6.2 Uso del equipo informático

6.2.1 Equipo asignado a cada usuario

a. El usuario es responsable del estado y bueno uso del equipo asignado para elaborar su trabajo.

b. 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.

c. El usuario debe de buscar un lugar adecuado para colocar el equipo de cómputo, para el caso de equipos de escritorio, estos no deben colocarse en el suelo, por lo que debe instalarse en un ambiente adecuado, de preferencia 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, para evitar cualquier tipo de descarga a tierra por estar en el suelo.

d. Los equipos UPS se deben utilizar únicamente como respaldo por energía eléctrica a equipos de cómputo. Al UPS estos NO se debe conectar fotocopiadoras, escáner, ni impresoras, los cuales deben protegerse por medio de reguladores de voltaje NO por UPS.

6.2.2 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, correo u oficio considerando que el mismo debe ser sometido a una revisión exhaustiva sobre

tipos de programas instalados, virus y otro que ponga en riesgo la seguridad de la red del INAB, o comprometa la estabilidad de la conexión y ancho de banda, por lo que el acceso se dará de forma temporal.

6.2.3 Consultores Externos

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

6.3 Usos adecuados del recurso informático

6.3.1 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:

- Guardar toda la información institucional únicamente en la carpeta de mis documentos.
- Clasificar la información con un máximo de cuatro subniveles de carpetas.
- Utilizar nombres cortos para los nombres de archivos y/o carpetas.
- No guardar en los equipos información personal tales como video, imágenes u otros que no sean de uso para el desarrollo de las funciones institucionales.

6.3.2 Se entiende por uso inaceptable

- La instalación de software sin la autorización de la Unidad de Tecnologías.
- 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.
- Utilizar los diferentes dispositivos de almacenamiento externo propiedad del INAB para almacenar música, videos, imágenes y/o cualquier tipo de archivo ajeno a actividades laborales.
- El uso de los equipos y la red con fines privados, personales o comerciales.
- Intentar conectarse a un sitio Internet sin ser autorizado por cualquiera de estas vías ftp, telnet, ssh u otro con algún puerto determinado sin permiso.

- Cualquier intento de usurpar otra identidad o de interceptar comunicaciones entre terceras personas.
- Conexión de equipos no autorizados por parte de la Unidad de Tecnologías, router, switch, acces point y otros relacionados.

6.4 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).
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 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.

6.5 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 y si no contara con personal será 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 una vez al año, de los cuales la Unidad de Tecnologías de la Información y Comunicación anualmente establecerá planificación para su ejecución.

6.5.1 Actualización de la página web

6.5.1.1 Estructura y funcionamiento del sitio

La Unidad de Tecnologías de la Información y Comunicación, es la encargada de mantener en línea y en funcionamiento 24 x 7 el sitio web institucional, así como el desarrollo de la maqueta del sitio y su estructura para la administración del contenido.

6.5.1.2 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 constantemente, en el momento de cualquier actualización debe trasladarse a la Unidad de Comunicación Social para su validación y publicación.

El acceso a la información pública es a través de la Dirección de Asuntos Jurídicos quien debe actualizar la información según la ley, solicitando a los encargados de los temas la información que corresponda, para ser validados y enviados a la Unidad de Tecnologías para su publicación.

6.6 Protección de redes internas y cableado estructurado

6.6.1 Cableado estructurado

El cableado de comunicación de voz (IP) y datos está 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 de Tecnologías. De acuerdo a la factibilidad y/o emergencia, la Unidad de Tecnologías 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.

6.6.2 Dispositivos de red (switches, firewalls, access point, router y otros relacionados a la red de datos)

6.6.2.1 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.

6.6.2.2 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.

VII. POLÍTICA DE RESPALDO (BACKUP)

7.1 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 centro de datos, así como de los sistemas (código fuente y versión publicada) de forma quincenal (dos veces al mes), para ello se realizará un plan anual de backup para su cumplimiento.

7.1.1 Características del Backup y prueba de restauración

El backup está bajo la responsabilidad del Profesional de Desarrollo de Sistemas y Bases de Datos asignado para realizarlo, por lo que debe considerar:

a. Las copias de respaldo se obtienen desde cada servidor a un servidor de consolidación de backups.

b. Se realiza restauración de backup dentro de otro servidor (servidor SIFGUA) para garantizar la integridad de la copia de respaldo.

c. Las copias se extraen a un sitio fuera del espacio físico de servidores con factor de autenticación para su seguridad, puede ser por medio de almacenamiento físico o en la nube que garantice su alta disponibilidad.

d. Se hará un informe sobre el desarrollo de los backups institucionales realizados el cual debe ser entregado al Jefe (a) de la Unidad de Tecnologías.

7.2 Backup equipos de cómputo

Actualmente la información institucional se centraliza a través de los sistemas informáticos, por lo que los expedientes son totalmente electrónicos, esta información ya se encuentra considerada en los respaldos que se realizan al Centro de Datos.

En otro caso:

- Cada usuario es responsable del manejo de la información Institucional que no posea un sistema informático que lo administre, por lo que debe realizar de forma planificada copias de respaldo (Backups) mensual de la información que no cuente con sistema informático que lo administre.

- 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 que no cuente con sistema informático que lo administre.

- No se deben incluir en las copias de respaldo música, películas, videos, imágenes u otro material ajeno a la institución.

VIII. POLÍTICA PARA EL DESARROLLO DE SOFTWARE

8.1 Creación de aplicaciones

La creación de nuevos sistemas a desarrollar, así como el desarrollo de nuevos módulos debe cumplir con las siguientes etapas:

1. Solicitud por parte de la dirección o unidad interesada.
2. Aprobación por la Subgerencia para ser incluido dentro del Plan Anual Operativo de la Unidad de Tecnologías de la Información y Comunicación.
3. Elaboración del documento de requerimientos el cual debe contener:
    a. Flujo de los procesos.
    b. Formatos de formularios de ingreso y de documentos a generar.
    c. Formato de reportes u otros. Este documento se realizará en conjunto entre el personal de la Unidad TIC y de la dependencia del requerimiento.
4. Análisis por parte del programador y el profesional de desarrollo para realizar cronograma de trabajo el cual debe contemplar los productos por módulos para las diferentes entregas.
5. Desarrollo de cada módulo por el profesional de desarrollo.
6. Creación de entorno de pruebas para sistema en desarrollo.
7. Validación de cada módulo en torno de pruebas, por parte del encargado temático, usuarios operativos y personal de la Unidad TIC.
8. Elaboración de documento con solicitud de correcciones y mejoras a cada módulo validado.
9. Desarrollo de mejoras de cada módulo.
10. Validación final de cada módulo.
11. Pruebas de procesamiento, cálculo, generación de documentos. Se incluye prueba de estrés del sistema, y control de calidad por parte del encargado temático.
12. Creación de entorno de producción.
13. Configuración de servidor de producción, configuración publicada.
14. Asignación de certificado SSL, DNS y publicación oficial del sitio.
15. Entrega de sistema oficialmente al administrador temático del mismo.
16. Las capacitaciones de los sistemas quedan a cargo del administrador del sistema.
17. Los instructivos de los sistemas deben ser elaborados y actualizados por el administrador de cada sistema.

8.2 Versionamiento de código

El código fuente de cada proyecto se encuentra a cargo de cada Profesional de Desarrollo de Sistemas y Bases de Datos, quien a su vez es el responsable de guardar una vez al mes la última versión del código de los proyectos a su cargo en el File Server establecido para resguardar los mismos. El File Server del versionamiento de código debe tener almacenado un histórico de un año.

8.3 Actualización de Sistemas

1. Toda actualización de los sistemas que se encuentran en funcionamiento y sobre todo de uso oficial debe realizarse de acuerdo a los siguientes lineamientos:
2. Debe ser validado en el entorno de prueba por los responsables del proceso para garantizar su correcto funcionamiento.
3. Antes de ser aplicado al sistema debe ser socializado previamente para conocimiento del personal que hace uso del mismo.
4. Si la actualización modifica procedimientos estructurales del sistema, debe acompañarse de un instructivo por parte de los administradores, lo más ilustrativo para orientar a los usuarios, también debe acompañarse de una inducción para evitar cualquier confusión en las buenas prácticas de uso del sistema.
5. Las actualizaciones de los sistemas en los servidores oficiales para que sea puestas en funcionamiento, se deben realizar en horario de menor carga de trabajo del sistema, se exceptúan las que se deben de aplicar de emergencia, de la cual deben ser notificadas todas las oficinas regionales y subregionales para no hacer uso del sistema durante el período de actualización de los servidores.

8.4 Software desarrollado por externos

Todo desarrollo de nuevos sistemas por consultoría externa deberá ser avalado por la Unidad de Tecnologías de la Información y Comunicación, para establecer los lineamientos de desarrollo, tipo de tecnología, lenguaje de programación y metodología, por lo que los términos de referencia deben estar establecidos por dichos lineamientos.

IX. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS		
Versión actualizada	**Descripción del cambio**	**Fecha de aprobación del cambio**
2	Se incluyen modificaciones e incorporaciones al contenido de los apartados 5.1 Usuarios, cuentas de correo y accesos. 5.2 Seguridad del centro de datos 6.2.2 Uso de equipos personales 6.3.2 Se entiende por uso inaceptable	Diciembre 2024