



INSTITUTO PARA LA INVESTIGACIÓN Y LA PRESERVACIÓN DEL PATRIMONIO CULTURAL Y NATURAL DEL VALLE DEL CAUCA INCIVA

PROCESO INFORMATICO

PROTOCOLO PARA EL USO ADECUADO DE LOS RECURSOS INFORMATICOS

INDICE

INTRODUCCIÓN	4
OBJETIVOS	5
SEGURIDAD EN LOS RECURSOS INFORMÁTICOS.....	6
POLÍTICAS	7
NORMAS.....	8
LEGALIDAD	8
ADQUISICIÓN.....	8
COMPROMISO.....	8
SANCIONES.....	8
LICENCIAS	9
DERECHO DE PROPIEDAD.....	9
INSTALACIÓN.....	10
CLAVES DE ACCESO.....	11
NO EXPECTATIVA DE PRIVACIDAD	12
CUIDADO DEL EQUIPO.....	13
MANTENIMIENTO.....	14
EQUIPOS PORTÁTILES.....	14
INFORMACIÓN CONFIDENCIAL	14
MEDIDAS PREVENTIVAS	15
SOFTWARE PIRATA.....	15
ORGANIZACIÓN DE LA INFORMACIÓN EN EL EQUIPO.....	15
USO DE LOS PROGRAMAS Y ARCHIVOS.....	15
PROTEGER EL EQUIPO	17
CUIDADO DEL EQUIPO.....	17
VIRUS INFORMÁTICOS.....	19
¿CÓMO EVITAR QUE LA INFORMACIÓN SEA INFECTADA POR UN VIRUS INFORMÁTICO?	19
CORREO ELECTRÓNICO	21
NORMAS DE MANEJO.....	21
PRINCIPALES SERVICIOS DEL CORREO.....	22

PROTOCOLO DE EL USO ADECUADO DE LOS RECURSOS INFORMATICOS

LEGISLACIÓN COLOMBIANA SOBRE DERECHOS DE AUTOR PIRATERÍA DE SOFTWARE.....	24
¿QUÉ DICE LA LEY?	24
¿CUÁLES SON LAS SANCIONES?	24
TENGA EN CUENTA.....	25
MEDIDAS ADMINISTRATIVAS	25

INTRODUCCIÓN

La SEGURIDAD INFORMATICA, consiste en proteger el software, el hardware y los datos de amenazas o peligros tales como:

- Uso y/o copias ilegales de software
- Pérdida de información
- Virus informático
- Fallas técnicas
- Robo
- Vandalismo
- Acceso no autorizado, entre otros.

Para proteger estos recursos informáticos es necesario, no solo el uso de la tecnología, sino también la colaboración de las personas.

Un mecanismo eficaz que contribuye a minimizar la ocurrencia de las amenazas o peligros en la seguridad de la información es la correcta aplicación que le den los funcionarios a las políticas, normas y medidas preventivas contempladas en este manual.

Todos los funcionarios de INCIVA son responsables por los recursos informáticos que manejan (Hardware, Software y datos), teniendo la obligación de cumplir con todos los lineamientos que se dan en el presente manual.

OBJETIVOS

Este protocolo ha sido adoptado por el INCIVA como herramienta de obligatorio cumplimiento y contiene la información necesaria que permita a todos los funcionarios del INCIVA:

- Crear una “Cultura de Seguridad y Control informático” al interior del INCIVA, para que los funcionarios tomen conciencia sobre la necesidad de proteger los equipos, el software y los datos de la entidad.
- Proteger la información contra cualquier forma de acceso no autorizado: utilización indebida, copia, publicación o modificación accidental o intencional del Software adquirido o desarrollado por el INCIVA con el fin de garantizar su confiabilidad, integridad y disponibilidad.
- Dar cumplimiento a las **normas, políticas, procedimientos y medidas preventivas de seguridad** definidas para el manejo de equipos de cómputo e información sistematizada.
- Tener claridad sobre la responsabilidad que cada funcionario tiene en relación con el manejo de información y equipos de cómputo.
- Optimizar el manejo de los recursos informáticos minimizando el riesgo por pérdida de información o deterioro de los equipos.
- Desarrollar la cultura Informática en todos y cada uno de los funcionarios del INCIVA.

SEGURIDAD EN LOS RECURSOS INFORMÁTICOS

Las principales razones que tiene el INCIVA para proteger la información y los equipos informáticos son las siguientes:

- **VALOR DE LA INFORMACIÓN:** La información es un activo importante dentro de una organización. Si se pierde, el costo de recuperarla, puede ser considerable en términos económicos.
- **SERVICIO:** Nuestro Instituto debe proteger la información y equipos informáticos de los riesgos a que están expuestos, para garantizar a los usuarios internos y externos la continuidad en sus operaciones y servicios.
- **LEGAL:** Las copias de Software ilegal instaladas en los equipos de computación violan la Ley 23 de 1982, el decreto 1360 de junio 23 de 1989 y la ley 44 de 1993 sobre Derechos de Autor y exponen al INCIVA a costosas multas y demandas que pueden afectar la imagen institucional, además de las sanciones disciplinarias y administrativas a que se hacen acreedores los empleados que instalen software ilegal.
- **PROTECCIÓN DE LA INFORMACIÓN:** El INCIVA cuenta con información confidencial y estratégica, la cual puede ser utilizada por entes externos con fines fraudulentos y competencia desleal.
- **PRODUCTIVIDAD:** Tiempo muy valioso se puede perder recuperando información de la cual no se tienen copias de respaldo y que se ha borrado o alterado en forma accidental, por ataques de virus informático, como consecuencia de permitir acceso a personas no autorizadas, o por el manejo no adecuado de los recursos computacionales.
- **INCREMENTO EN EL USO DE LOS RECURSOS Y SERVICIOS PRESTADOS A TRAVÉS DE LA RED:** Servicios tales como archivos compartidos, impresoras, correo, Internet y voz, que son un aporte importante para la comunicación entre los usuarios internos del INCIVA.
- **INTERACCIÓN FUNCIONARIOS - COMPUTADOR:** El computador es una herramienta importante utilizada por los funcionarios del INCIVA en el proceso de toma de decisiones y la gestión administrativa.
- **PROTECCIÓN DE LA INVERSIÓN:** El correcto uso y cuidado alarga la vida útil de los sistemas computacionales.

POLÍTICAS

Es responsabilidad de la dirección, coordinadores de área, profesionales universitarios, técnicos operativos, auxiliares administrativos, dar a conocer **éste manual** a todos los usuarios. Además de velar por que la utilización de los equipos de cómputo, software y los periféricos sólo sea por parte de los funcionarios autorizados para desarrollar actividades estrictamente laborales en las horas normales de trabajo a menos que tenga la correspondiente autorización.

- Está totalmente prohibido utilizar los equipos de cómputo, software y/o periféricos, para realizar actividades diferentes a las estrictamente laborales.
- En los equipos del INCIVA sólo podrá instalarse y utilizarse software legal.
- La adquisición de equipos de cómputo, periféricos, y software, además de proyectos de desarrollo de programas, se realizará con la coordinación de la Oficina de Sistemas de Información y Tecnología.
- La utilización de los equipos de cómputo, software y/o periféricos se restringe a las horas normales de trabajo, a menos que exista autorización por parte de dirección y coordinadores de área.
- El software desarrollado con recursos técnicos y humanos del INCIVA es de propiedad del INCIVA
- La instalación y/o uso de juegos para computador en equipos del INCIVA está terminantemente prohibida.
- El INCIVA no se hace responsable de los computadores y accesorios periféricos personales que se encuentren en el Edificio, tanto en lo relacionado con el hardware como el software, ni tampoco asume el mantenimiento de los mismos.

NORMAS

Las siguientes normas que regulan el uso de los recursos informáticos, son de estricto cumplimiento por todos los funcionarios del INCIVA y es responsabilidad del director, coordinadores de área, profesionales, técnicos operativos y auxiliares administrativos, velar por la aplicación de las mismas.

LEGALIDAD

La Oficina de Sistemas de Información y Tecnología realizará un seguimiento y control del Software residente en los equipos ubicados en todas las áreas y centros del INCIVA, mediante visitas periódicas donde se verificará que la configuración de hardware y software encontrados, corresponda a la que aparece asignada.

ADQUISICIÓN

Teniendo en cuenta que para la compra de equipo de cómputo, software, hardware, etc.; la Oficina de Sistemas de Información y Tecnología realizará el acompañamiento para la adquisición, también se debe tener en cuenta las disposiciones establecidas para la compra de estos elementos; así mismo la contratación de entes externos para el diseño de programas, servicio de asesoría e informática, procesamiento externo de datos y mantenimiento de equipos.

COMPROMISO

El equipo de cómputo, periféricos y software que se entregue a los usuarios, se oficializará a través del **respectivo documento asignado para éste proceso** y el **formato de atención a usuarios proceso informático** (cuando lo a merite), con la cual se reconoce la entrega de estos elementos y se reitera el compromiso del usuario de NO adicionar, copiar y/o modificar el software y de no modificar en ninguna de sus partes el hardware del equipo entregado.

SANCIONES

Cuando sea detectado por la Oficina de Sistemas de Información y Tecnología, software ilegal o no autorizado en los equipos del INCIVA, éste será borrado sin requerir consulta

previa al usuario. Además de reportarse a la **Oficina de Control Interno**.

LICENCIAS

Todo software de libre distribución o gratuito (demos) adquirido a través de Internet o de cualquier otro medio deberá ser autorizado por la Oficina de Sistemas de Información y Tecnología previa evaluación.

Los inconvenientes generados por este software serán responsabilidad del usuario y no se dará cabida a soporte de este software.

DERECHO DE PROPIEDAD

Los programas fuentes y ejecutables desarrollados o adquiridos por el INCIVA, incluyendo su documentación, no deben ser reproducidos, publicados, transmitidos o copiados por los empleados. En caso de ser necesario, podrá realizarse únicamente con autorización de la Oficina de Sistemas de Información y Tecnología.

Para aquellos equipos de cómputo que no dispongan de clave de acceso o bloqueo de teclado, los datos confidenciales no deben ser almacenados en discos duros. Almacene estos datos en dispositivos de almacenamiento secundario (CDs, DVDs, etc.) y guárdelos bajo llaves en un lugar seguro.

Todo empleado que se retire del INCIVA debe presentar paz y salvo de entrega de equipo(s) y de todas las claves de las cuentas que posea para el ingreso a los diferentes ambientes donde esté autorizado. Este **paz y salvo** deberá ser firmado por la Oficina de Sistemas de Información y Tecnología. El paz y salvo es requisito indispensable para la ejecución de la liquidación del empleado.

INSTALACIÓN

Mediante la firma del “documento de entrega del equipo de cómputo” por parte de coordinador de inventarios, e independiente del número de usuarios que lo utilizan, el funcionario se convierte en responsable de:

- No instalar software no autorizado (programas diferentes a lo relacionado en el documento de entrega) en el equipo.
- No retirar, ni movilizar el equipo a otras oficinas del INCIVA sin la debida autorización.
- No intercambiar componentes del hardware con otros equipos.
- No destapar, ni intervenir el hardware por ningún motivo.

Observación: El software comercial (Office, Windows etc.) autorizado para usar en los microcomputadores sólo podrá ser instalado por la Oficina de Sistemas de Información y Tecnología.

CLAVES DE ACCESO

Para los equipos donde se utilizan claves de acceso (password) para el ingreso del usuario a diferentes ambientes de trabajo tenga en cuenta:

- Que el manejo del la(s) clave(s) implica responsabilidades sobre su uso.
- Siempre que ingrese o digite la clave de acceso en el sistema tenga especial cuidado de que no haya sido observada por otra(s) persona(s), si tiene dudas proceda a su cambio.
- La clave es personal e intransferible, manténgala siempre en secreto y no la dé a conocer a otros funcionarios.
- No utilice claves prestadas o de personas ya retiradas del INCIVA.
- Cambie la(s) clave(s) periódicamente.
- La clave del personal retirado del INCIVA debe eliminarse y no reasignarse a otro empleado.
- Cierre la sesión de trabajo de la terminal u ordenador cuando:
 - Se vaya a almorzar.
 - Se retire temporalmente de su sitio de trabajo.
 - Se retire al finalizar su trabajo.
- Al instalar software ilegal que controle el ingreso de los usuarios al equipo de cómputo (password) corre el riesgo de perder la información, debido a que si se le llega a olvidar o perder la clave, es difícil y en la mayoría de los casos imposible recuperar. Si esto sucede seguramente se deberá formatear el disco duro, con el consecuente borrado de todos los datos.
- Si usa claves de acceso en el computador, NO utilice claves fáciles de identificar o débiles, tales como: Nombres, apellidos, sobrenombres, códigos de terminal o

PROTOCOLO DE EL USO ADECUADO DE LOS RECURSOS INFORMATICOS

estación, iniciales de nombres y apellidos, fechas, nombres de archivos.

- Si posee claves de acceso o diferentes sistemas, no utilice la misma para todos, use una diferente para cada aplicativo.
- Si suspende temporalmente el trabajo, sale a almorzar o a finalizar el día y deja activa la clave de acceso en su estación de trabajo u ordenador personal, facilita que toda persona la pueda utilizar inadecuadamente, quedando la operación registrada como si hubiera sido realizada por usted.
- El acceso a los equipos debe ser solo permitido a personal autorizado

Observaciones:

- Al finalizar las labores diarias, guarde los reportes y documentos confidenciales en un lugar seguro.
- Destruya o elimine los reportes, documentos, cartas y memorandos confidenciales cuando dejen de ser útiles.

NO EXPECTATIVA DE PRIVACIDAD

Los computadores y las cuentas de computador (Correo Electrónico, e-mail e Internet) asignadas a los usuarios son para que mejoren su desempeño en sus puestos de trabajo.

La existencia de claves de acceso (passwords) es simplemente un mecanismo para garantizar la individualidad pero no es una aceptación de la privacidad. Los usuarios no deben de tener expectativas sobre la privacidad de nada de lo que creen, almacenen, envíen o reciban en el sistema de cómputo que se les ha asignado y que es de propiedad del INCIVA.

CUIDADO DEL EQUIPO

No fume, ni consuma alimentos y/o bebidas cerca de los equipos de cómputo, y periféricos.

Vacune previamente los disquetes o memorias USB que vaya a utilizar en los equipos del INCIVA.

Asegure la información del disco duro. Es necesario efectuar copias de seguridad (backup) de todos los datos que por su confiabilidad y/o importancia valga la pena guardar. La toma de copias de seguridad es de carácter obligatorio y de responsabilidad de cada usuario.

Por lo anterior es necesario:

- Identificar la información del área.
- Que el coordinador de área seleccione los archivos a los cuales hay que hacer copia de respaldo.
- Hacer como mínimo dos copias respaldo de los datos, para que sean almacenadas en un lugar seguro dentro de la organización y si la información es muy valiosa envíe una copia a una entidad externa para su custodia.
- Identificar las copias de respaldo mediante un rótulo al cd o dvd, o llevar un registro independiente en el cual se anote el número del cd o dvd, así como su contenido.
- Identificar la información correspondiente a los archivos de trabajo de cada usuario, la cual debe ser respaldada con copias de seguridad que debe tomar cada usuario, quedando bajo su responsabilidad la recuperación de la información en caso de pérdida de ésta.

MANTENIMIENTO

El mantenimiento, modificación o cualquier tipo de arreglo o traslado de equipos de cómputo, periféricos, etc., debe ser realizado únicamente por personal autorizado por la Oficina de Sistemas de Información y Tecnología e informado al coordinador de inventarios.

No se debe permitir que personas sin la debida identificación, inspeccionen o hagan “arreglos” a su equipo.

EQUIPOS PORTÁTILES

Los funcionarios que tengan a su cargo un equipo de cómputo portátil: Deberán hacerse responsables del cuidado y protección del equipo. Asimismo, se compromete a no sacar copias para uso personal, del software que el equipo tenga instalado, ni copias para personas ajenas al INCIVA.

INFORMACIÓN CONFIDENCIAL

Los listados o reportes con información del INCIVA Se deben destruir cuando hayan cumplido su tiempo de conservación, por tanto, queda terminantemente prohibido que se obsequien, vendan o donen a menos que previamente se hayan destruido.

El acceso a la información del INCIVA y de sus clientes en medios magnéticos e impresos, se restringe únicamente a las personas que por sus funciones deban utilizarla.

Apague el computador (CPU y Monitor) cuando finalice su horario de trabajo.

Evite consumos innecesarios de energía.

MEDIDAS PREVENTIVAS

A continuación se describen las principales MEDIDAS PREVENTIVAS que ayudan a proteger la información contra modificación, revelación y/o pérdida. Y como una forma de advertir a los funcionarios del INCIVA sobre las consecuencias de utilizar software ilegal:

SOFTWARE PIRATA

El uso de software pirata o no adquirido legalmente puede causarle a usted o al INCIVA serios problemas:

- Sanciones.
- Demandas civiles o penales.
- Multas o arrestos.
- Pérdida o daño de información por infección de Virus Informático.

Evite que en el equipo de cómputo a su cargo experimenten personas ajenas “sabelotodos”, el acceso a los equipos debe ser solo permitido a personal autorizado y calificado.

ORGANIZACIÓN DE LA INFORMACIÓN EN EL EQUIPO

Mantenga organizando la información en el disco duro y conserve los archivos que verdaderamente utiliza. Utilice la información de las tablas de retención documental, especialmente las referentes al área para la organización de ésta.

NOTA: No utilice su equipo de trabajo como repisa para colocar objetos de decoración.

USO DE LOS PROGRAMAS Y ARCHIVOS

Utilice los programas o comandos del sistema operativo cuando tenga un buen

PROTOCOLO DE EL USO ADECUADO DE LOS RECURSOS INFORMATICOS

conocimiento de ellos, de lo contrario, es posible que dañe su información y/o la de los demás.

Si no está seguro del origen o funcionamiento de un archivo evite borrarlo.

Cuando esté utilizando el computador, salve periódicamente la información. Evite que un corte de energía le haga perder el trabajo.

Si se retira temporalmente del computador, salve la información. Otra persona puede utilizar el equipo sin guardar o salvar los datos.

PROTEGER EL EQUIPO

Para prevenir que se presenten fallas técnicas o fallas en su equipo, prenda su computador en el siguiente orden: Primero el monitor, luego los periféricos (impresora) y por último la CPU. Para apagarlo haga la inversa, primero la CPU luego los periféricos y por último el monitor.

CUIDADO DEL EQUIPO

- Proteja el equipo de cómputo. Evite instalarlo cerca de las ventanas, en sitios húmedos, poco ventilados y/o expuestos a los rayos del sol.
- El ruido que producen algunos aparatos eléctricos distorsionan la información. Evite instalar estos equipos cerca del computador.
- La electricidad estática puede ocasionar daños a los componentes electrónicos de los equipos; para ello es aconsejable que antes de iniciar sus labores en el computador toque cualquier elemento metálico para descargar dicha electricidad.
- Si el equipo de cómputo no está conectado a un estabilizador de voltaje y hay tormenta, apague y desconecte el equipo.
- Cuando el equipo se moje no lo encienda, si está encendido apague y desconéctelo inmediatamente.
- Si traslada o mueve un equipo de cómputo que se encuentre enchufado y encendido, se puede dañar físicamente. Antes de hacerlo apáguelo y desconéctelo.
- Cuide el teclado del equipo de Cómputo. Es un dispositivo que se puede dañar fácilmente, si es golpeado, maltratado o rayado.
- Si el equipo está encendido, conectar o desconectar la impresora, módem y/o mouse, puede ocasionar cortos circuitos en los componentes electrónicos internos del equipo. Apáguelo mientras hace conexiones o desconexiones.

PROTOCOLO DE EL USO ADECUADO DE LOS RECURSOS INFORMATICOS

- Cuando se coloca la impresora demasiado cerca al computador, puede afectar el funcionamiento del equipo.
- Mantenga las rejillas del computador destapadas cuando este encendido. El equipo debe tener una adecuada ventilación para su correcto funcionamiento.
- Si su computador es portátil la falta de uso de la batería por períodos superiores a un mes le genera deterioros irremediables al equipo.
- Cuide su computador portátil y/o mouse, éstos tienen mucho “amigos” dado su tamaño pueden ser hurtados fácilmente de las áreas del INCIVA; por esto es necesario, que una vez termine su uso, lo guarde en un lugar seguro, preferiblemente con llave.
- Mantener su equipo limpio y aseado en sus partes exteriores, no use líquidos o elementos extraños para limpiar su monitor.

VIRUS INFORMÁTICOS

Los virus informáticos son programas que tienen la capacidad de multiplicarse y propagarse rápidamente en su computador. Existen varios tipos de virus o malware pero los más conocidos son aquellos que afectan el funcionamiento normal de los programas del computador, estos son llamados malignos y pueden destruir parcialmente y totalmente los programas de la información almacenada.

Los síntomas que puede presentar el computador cuando está siendo afectado por el virus informático son:

- El computador empieza a funcionar anormalmente (lento en el proceso, pérdida de fragmentos de información, mensajes extraños etc.).
- Aparecen archivos que usted no ha creado o con tamaño inusual (muy grandes o de tamaño "0").
- No puede ingresar a programas o aplicaciones a las que normalmente ha tenido acceso.
- Disco duro o disquetes aparentemente llenos sin justificación alguna.

¿CÓMO EVITAR QUE LA INFORMACIÓN SEA INFECTADA POR UN VIRUS INFORMÁTICO?

La mejor forma de evitar que un virus informático dañe la información es no utilizar o permitir que se utilicen disquetes o memorias USB que no hayan sido vacunados o en lo posible evite usar disquetes o memorias USB con datos que hayan sido grabados en ordenadores que no sean del INCIVA.

EL INCIVA cuenta con programas antivirus que detectan y pueden eliminar los virus informáticos más conocidos. Los programas de detección de virus alertan con un sonido (pito) o mensajes, la presencia de un virus conocido (indican el nombre del virus) o

PROTOCOLO DE EL USO ADECUADO DE LOS RECURSOS INFORMATICOS

desconocido (indica la existencia de un virus pero que no ha sido identificado por el software antivirus), si esto se presenta, comuníquese con la Oficina de Sistemas de Información y Tecnología.

Asimismo, para que la vacuna pueda cumplir con su objetivo se debe tener en cuenta:

- No cancelar la vacuna automática que se hace a los archivos cuando usted prende el computador.
- No suprima las instrucciones de limpieza que se encuentra en los archivos del sistema.
- Antes de utilizar un disquete o memoria USB vacúnelo(a) previamente.
- Si el computador no posee el programa antivirus solicite inmediatamente la instalación a la Oficina de Sistemas de Información y Tecnología.

CORREO ELECTRÓNICO

NORMAS DE MANEJO

Correo Electrónico

Hace referencia a los mensajes de correo intercambiados entre los usuarios del INCIVA y/o con usuarios externos a través de la herramienta Outlook.

Usuarios Autorizados

Están autorizados para intercambiar mensajes de correo electrónico los funcionarios y trabajadores vigentes del INCIVA que por razones propias de su trabajo requieren de esta herramienta y que se encuentren legalmente definidos.

Deberes

- Todos los mensajes que se envían a través de correo electrónico deben estar enmarcados en normas mínimas de respeto.
- El sistema de correo electrónico debe ser utilizado únicamente para la transmisión de información relacionada con asuntos laborales del usuario y/o asuntos de interés común que inciden en la buena marcha y en el mejoramiento de la armonía laboral del INCIVA.
- Es responsabilidad de los usuarios de correo electrónico mantener o archivar los mensajes enviados y/o recibidos para efectos de soportar ante terceros (internos o externos) la ejecución de operaciones o acciones.

Prohibiciones:

El incumplimiento de las normas establecidas acarreará sanciones disciplinarias.

Como uso inapropiado del correo electrónico se considera:

- Envío de mensajes desde el correo de un usuario con firma de otro.
- Intentos de acceso y/o accesos no autorizados a otra cuenta de correo.
- Transmisión de mensajes de correo con información sensible o confidencial a personas u organizaciones externas sin autorización.
- Cadenas de mensajes que congestionen la red.
- Transmisión de mensajes obscenos.
- Cualquier actividad no ética que afecte al INCIVA.

PRINCIPALES SERVICIOS DEL CORREO

Listas de distribución:

Hace referencia a la agrupación de varios buzones de usuarios de correo electrónico, permitiendo que el envío de mensajes sea únicamente a la lista de distribución y no independiente a cada uno de los buzones de usuarios. Un mensaje enviado a una lista de distribución será entregado a cada buzón de usuario que pertenezca a la lista.

Carpetas:

Es un conjunto de directorios creados en el correo, que permiten almacenar y/o organizar los mensajes de correo enviados y recibidos. Existen tres tipos de carpetas.

Carpetas del Sistema: Son creadas por la herramienta Outlook durante la configuración a cada usuario de correo. No pueden ser eliminadas y son utilizadas por Outlook para controlar el ingreso y salida de mensajes de correo. También permiten controlar otras funcionalidades de Outlook como el calendario, contacto, las notas y tareas entre otros.

Carpetas Personales: Son creadas, modificadas y eliminadas por el usuario del correo. Permiten el almacenamiento y organización de mensajes de correo, de mensajes de citas, contactos, notas etc. Son uso exclusivo del propietario y quedan almacenadas en el disco duro de su estación de trabajo.

PROTOCOLO DE EL USO ADECUADO DE LOS RECURSOS INFORMATICOS

Procedimiento de Seguridad: Todos los mensajes enviados a través del correo electrónico serán almacenados por el usuario, reservándose el derecho a los mismos con fines de supervisión, así como la eliminación de correos de acuerdo con los estándares de almacenamiento.

Los computadores no deben dejarse desatendidos estando en una sesión abierta a menos que estén bloqueados de pantalla con contraseña.

Restricciones y Recomendaciones:

Acerca del espacio en disco:

Uno de los recursos más difíciles de controlar es el consumo de espacio en el disco duro. De acuerdo con la experiencia y características de los servidores, se ha optado por limitar el espacio del buzón de 100 MB a 1000 MB en el servidor respectivo por usuario.

Teniendo en cuenta esta restricción, se recomienda hacer un muy buen uso del correo para garantizar el mejor aprovechamiento posible de esta capacidad. Las siguientes son algunas recomendaciones para disminuir la cantidad de espacio que gastan los mensajes.

No abusar del servicio:

No utilice el servicio de correo para cadenas, juegos, anuncios, etc. Este tipo de utilización hace que se pierdan recursos valiosos para usted, para otros funcionarios y para del INCIVA.

Eliminar elementos antiguos y que ya no se necesiten.

Trate de organizar los mensajes recibidos de tal manera que solo conserve la información que le interesa y que está vigente. No deje congestionar su “Bandeja de Entrada”, ya que mientras más mensajes tenga, más difícil identificar lo útil de lo inservible. Trate de deshacerse de lo inservible tan pronto como pierda vigencia, no deje esta tarea pendiente en ninguna de las carpetas que hacen parte del buzón como: Bandeja de Entrada, Calendario, Contactos, Diario, Tareas, Bandeja de Salida, Elementos Eliminados, Elementos Enviados y Notas. Si necesita mantener algunos mensajes utilice las “Carpetas Personales”, que tampoco hacen parte de los buzones asignados en el servidor, pero hacen parte del espacio en el disco duro de su microcomputador, y evite así que su buzón se llene.

LEGISLACIÓN COLOMBIANA SOBRE DERECHOS DE AUTOR PIRATERÍA DE SOFTWARE

¿QUÉ DICE LA LEY?

La legislación de derechos de autor en Colombia se fundamenta en la Ley 23 de 1982. Esta fue modificada por la Ley 44 de 1993, la cual otorga una nueva e importante protección a los programas de Software, al señalar que una copia de programas de software se considera ilícita cuando se produce sin el consentimiento de los propietarios de los derechos de autor, con excepción de la copia de seguridad. Así mismo, y reforzando aún más su compromiso con estos principios, Colombia es miembro tanto de la convención Universal de los Derechos de Autor como de la convención de Berna para la protección de Obras Literarias y Artísticas.

¿CUÁLES SON LAS SANCIONES?

Si usted y/o su empresa copian ilegalmente un programa de computador, podrán ser demandados tanto individual como conjuntamente, civil o penalmente. El propietario de los derechos de autor podrá solicitar medidas cautelativas consistentes en impedirle a usted y a su empresa el uso de los programas de computador y exige la destrucción de todas las copias piratas. Adicionalmente, usted o su empresa pueden ser obligados a pagar, por concepto de daños o perjuicios, el costo de venta de todas las copias ilegales realizadas. Aún cuando sólo exista sospecha de actividad ilícita, un juez puede ordenar que se lleve a cabo una visita prejudicial a su empresa.

La ley 44 de 1993, impone multas considerables al que intencionalmente realice copias ilegales de programas de computador. Las sanciones por el uso ilegal del software varían según se trate de aprobación o uso indebido de los programas y quien lo haga se hará acreedor a penas de prisión y multas; existiendo además, por parte de la Policía Judicial, la facultad de incautar y destruir los ejemplares obtenidos de manera irregular. La ley

PROTOCOLO DE EL USO ADECUADO DE LOS RECURSOS INFORMATICOS

castiga con prisión de dos (2) a cinco (5) años y multas que van de cinco (5) a veinte (20) salarios mínimos en algunos casos, y prisión de uno (1) a cuatro (4) años y multas de diez (10) salarios mínimos legales en otros.

Independientemente o de manera conjunta con acción penal correspondiente, se puede adelantar la acción civil que buscará obtener la indemnización por los daños y perjuicios materiales ocasionados por la conducta.

TENGA EN CUENTA

Es ilegal comprar un solo programa de software para instalar en más de un computador y copiar o distribuir tanto el software como los manuales de uso (con excepción de la copia de seguridad) sin el consentimiento por escrito del propietario de los derechos de autor.

La utilización de programas piratas coloca a la empresa en un alto riesgo, al igual que a la información, los sistemas financieros y otras funciones vitales del negocio, lo que le ocasiona: Pérdida de tiempo, dinero, credibilidad y negocio.

Cuando se utilizan copias piratas estas carecen de documentación, soporte técnico, actualizaciones y calidad en los programas.

MEDIDAS ADMINISTRATIVAS

El incumplimiento de las políticas generales anteriormente definidas en el presente manual, constituye falta grave.

PROTOCOLO DE EL USO ADECUADO DE LOS RECURSOS INFORMATICOS