



# **INSTRUCTIVO**

## **USO Y MANEJO**

### **DE LOS RECURSOS**

### **INFORMATICOS**

---

**GERENCIA DE**  
**SISTEMAS**

Actualización:  
FEBRERO DE 2010

## TABLA DE CONTENIDOS

1.	NORMAS GENERALES.....	1
2.	ESPECIFICACIONES DE LA RED DE DATOS .....	2
3.	CUENTAS DE USUARIO.....	3
4.	USO DE CORREO.....	4
5.	USO DE INTERNET .....	5
6.	MANTENIMIENTO PREVENTIVO .....	6
7.	MANTENIMIENTO CORRECTIVO.....	8
8.	ADQUISICION Y ELIMINACION DE LOS EQUIPOS.....	8
9.	UBICACIÓN Y RESPONSABILIDAD SOBRE LOS EQUIPOS .....	9
10.	PROTECCION CONTRA VIRUS .....	10
11.	SEGURIDAD .....	10
12.	DATOS.....	11
13.	RECURSOS DE LA INSTITUCION.....	11
14.	RESPONSABILIDADES.....	12
15.	FALTAS.....	13
16.	SANCIONES .....	14
17.	SOBRE LO NO PREVISTO .....	14
18.	VIGENCIA .....	14

## **1. NORMAS GENERALES**

- a) Queda terminantemente prohibido utilizar el equipo informático del Instituto Nacional de los Deportes para realizar trabajos de beneficio personal o que no estén relacionados al desempeño de sus labores.
- b) Queda terminantemente prohibido modificar cualquier tipo de configuración en los equipos de cómputo, así como instalar o ejecutar cualquier tipo de software sin su respectiva licencia de uso y con fines no laborales y sin conocimiento del Jefe Inmediato.
- c) No esta permitido el uso de ningún tipo de juegos, así como utilidades de red cuyo uso no sea de beneficio para la institución y que no sea registrado por la Gerencia de Sistemas, incluyendo cualquier tipo de Chat como por ejemplo el Yahoo Messenger, AOL Messenger , ICQ, así como portales web de intercambio de fotografías personales, hacer amigos, etc. El uso del MSN Messenger (Hotmail) será autorizado para los casos particulares en que por las propias funciones laborales, este sea necesario.
- d) En caso de una revisión técnica del equipo, en la cual se encontrase software que no hubiera sido instalado o registrado por la Gerencia de Sistemas y la institución se haga acreedora de alguna observación en dicha revisión, el usuario responsable deberá someterse a lo establecido en el apartado “Faltas y Sanciones” de esta normativa.
- e) Si una unidad o gerencia necesita un software específico, para el cual se necesita licencia y la misma no se ha adquirido, debe gestionar su compra con la respectiva justificación, es decir, especificar las labores en las cuales el software beneficiará su desempeño laboral y el consiguiente apoyo al cumplimiento de metas de la unidad , gerencia o institución.
- f) Debe moderarse el volumen de los parlantes de la computadora, a fin de no intervenir en el trabajo de los compañeros de área, además de velar por la imagen institucional; además, está prohibido reproducir sonidos que atenten contra las normas morales, que puedan ser ofensivos para las personas, que generen sonidos molestos al oído y/o promover racismo, discriminación y vulgaridad.
- g) Existe un formulario de control, denominado: Formulario de Acceso de Usuarios, el cual se menciona en este instructivo, el cual se adjunta como ANEXO y el puede solicitarse en su versión electrónica a cualquier miembro de la Gerencia de Sistemas.

## **2. ESPECIFICACIONES DE LA RED DE DATOS**

- a) En el tendido de cableado se deberá de utilizar cable UTP categoría 5e o 6, según el sitio, bajo la norma EIA/TIA 568A, con soporte para transmisión de datos a 10, 100 y 1000 mbps, donde sea requerido.
- b) La distancia máxima para cada punto de red no deberá exceder de 90 mts. a partir del patch panel hasta el toma respectivo.
- c) La longitud máxima de cada patch cord (extensión), desde el toma al equipo no deberá exceder de 3 mts., excepto en los casos en que por problemas de espacio se necesite mayor a 3 mts., para lo cual se deberá solicitar al personal de informática su conformidad.
- d) Los cables de red (UTP 5e o 6), no deberán pasar a una distancia menor a 15cms de fuentes generadoras de ruido, lámparas fluorescentes, líneas de alta tensión, aires acondicionados y la misma distancia aplica para la canalización del cable de datos el cual no debe mezclarse con cables de potencia.
- e) La trayectoria del cable no deberá presentar quiebres bruscos a 90 grados.
- f) Cualquier modificación o ampliación en la red de datos, necesaria para utilizar equipo de cómputo, debe contar con el visto bueno del encargado de la infraestructura del edificio y en el caso de incurrir en costos, éstos serán financiados con el presupuesto del área que lo solicite.

### **3. CUENTAS DE USUARIO**

- a) Para tener acceso a cuentas del dominio institucional, la unidad interesada deberá presentar el formulario de Acceso a Usuarios (altas, bajas y cambios) para la creación de las cuentas de sus empleados, este formulario deberá firmarlo el empleado, su jefe inmediato y el gerente del área, y deberá remitirse a la Gerencia de Sistemas.
- b) El usuario debe cambiar la clave que se le asigne inicialmente por otra suficientemente segura y deberá modificar esta clave con la mayor frecuencia posible para salvaguardar la seguridad de la misma (máximo 2 meses), considerando las políticas de nomenclatura definidas por la Gerencia de Sistemas.
- c) No compartir bajo ningún concepto la clave o cuenta de usuario a terceras personas, ya que estas son personales. El propietario de la cuenta se responsabiliza de cualquier utilización inadecuada de la misma. (mientras no se compruebe lo contrario).
- d) Solicitar el cierre de la cuenta cuando no se vaya a utilizar durante un período prolongado.
- e) La cuenta de usuario sólo se utilizará para actividades laborales que competan al cargo, lo que excluye cualquier uso comercial así como las prácticas desleales que puedan suponer delito o entorpecer voluntariamente el trabajo de otros usuarios o sistemas tanto del INDES como de otras instituciones accesibles a través de la red, afectando su funcionamiento o la privacidad de su información.
- f) Notificar inmediatamente al Área de Informática cualquier sospecha de intervención ajena o cambio en su cuenta de usuario.
- g) Es responsabilidad del Jefe Inmediato, solicitar la eliminación de la cuenta de un usuario que haya renunciado o haya sido despedido de la institución, lo cual deberá hacerse el mismo día que suceda.
- h) Es responsabilidad del Jefe Inmediato, solicitar la eliminación de permisos a ciertos recursos compartidos o aplicaciones, cuando el usuario ya no los utilice.
- i) El jefe inmediato debe solicitar por medio de el Formulario de Acceso a Usuarios la creación de cuentas para el personal de nuevo ingreso o para el personal que de acuerdo a sus funciones lo necesite, especificando en el mismo, la justificación correspondiente que la ampare. El formulario puede obtenerse descargándose la intranet institucional, en la sección de formularios, o solicitándolo directamente a la Gerencia de Sistemas.

## **4. USO DE CORREO**

- a) Para que un usuario tenga acceso a una cuenta de correo institucional (ALTA), deberá completar el Formulario de Acceso a usuarios, el cual será firmado por el usuario, su jefe inmediato y del gerente del área. Este formulario deberá remitirse a la Gerencia de Sistemas.
- b) Cuando un usuario se retira de la institución, es responsabilidad del jefe inmediato remitir el formulario de Acceso a usuarios (BAJA), a efectos de dar de baja la cuenta de correo electrónico institucional. Este formulario deberá remitirse a la Gerencia de Sistemas.
- c) No está autorizado que dos usuarios compartan una misma cuenta de correo institucional a nombre personal de un empleado. Esto solamente será posible en los casos de las cuentas de correo electrónico institucional genéricos, es decir los que no están directamente relacionados al nombre de una persona, por ejemplo: [información@indes.gob.sv](mailto:información@indes.gob.sv), [contabilidad@indes.gob.sv](mailto:contabilidad@indes.gob.sv) y similares.
- d) Debe evitarse adjuntar archivos de gran tamaño a los mensajes de correo electrónico, (Consulte con el personal de la Gerencia de Sistemas, las capacidades de envío asignada o la forma de comprimir los archivos grandes).
- e) No está autorizado el hacer propaganda política, religiosa o comercial.
- f) En la redacción de mensajes debe ser cortés y honesto, evitando el lenguaje vulgar u obsceno.
- g) Debe seguir la cadena de mando establecida para la comunicación con sus superiores.
- h) No debe enviar mensajes que contengan cualquier forma de discriminación racial, de género o de acoso sexual.
- i) No utilizar el correo electrónico de la institución para suscripciones de envío de información si ésta no es de carácter laboral.

## **5. USO DE INTERNET**

- a) Para que un usuario tenga acceso a internet (ALTA), deberá completar el Formulario de Acceso a usuarios, el cual será firmado por el usuario, su jefe inmediato y gerente del área, incluyendo la justificación clara de la necesidad de este servicio para el desempeño de las labores del empleado. Este formulario deberá remitirse a la Gerencia de Sistemas.
- b) Cuando un usuario se retira de la institución, es responsabilidad del jefe inmediato remitir el formulario de Acceso a usuarios (BAJA), a efectos de dar de baja la cuenta del usuario. Este formulario deberá remitirse a la Gerencia de Sistemas.
- c) Debe usar los servicios de Internet únicamente para asuntos laborales.
- d) No está autorizado el acceder o visitar salas de Chat, amigos en línea, sitios pornográficos, sitios de juegos en línea, sitios relacionados con drogas y/o terrorismo.
- e) Si un usuario necesita hacer uso de elementos web como facebook, twitter, foros de terceros y otros similares para efectos de tener presencia e imagen institucional en estas formas de expresión ciudadana, debe ser justificado y autorizado por su jefe inmediato y gestionado a través de la Gerencia de Sistemas de INDES.
- f) Cuando un Comité Organizador de Eventos solicite el acceso a internet deberá solicitarlo por escrito a la Presidencia de INDES, especificando claramente el tipo de acceso que necesitan, las fechas y horarios, la cantidad aproximada de usuarios a utilizar el servicio y el lugar en que se pretende acceder a la red.

## **6. MANTENIMIENTO PREVENTIVO**

- a) Es responsabilidad de la Gerencia de Sistemas o de los proveedores contratados para tal fin, la ejecución del mantenimiento preventivo a los equipos informáticos de la institución.
- b) La Gerencia de Sistemas podrá hacer uso de recurso humano calificado en servicio social o voluntariado para realizar estas labores.

### **Computadoras personales y portátiles**

- a) Los usuarios no deberán comer, beber, fumar o mantener productos alimenticios especialmente líquidos cerca de los equipos informáticos, ya que representan un riesgo para los mismos, adicionalmente, deben tener cuidado en el manejo de clips, grapas y otros materiales metálicos, para que no se introduzcan en el teclado, monitor e impresores.
- b) Al finalizar la jornada laboral, los usuarios deben verificar que todo el equipo incluyendo el UPS quede completamente apagado y adicionalmente, éste último desconectado del suministro eléctrico comercial, excepto en los casos que el equipo deba permanecer encendido por funciones específicas.
- c) El usuario debe asegurarse que el equipo informático que tenga asignado esté colocado en superficies planas, con la suficiente rigidez para evitar vibración, la cual podría dañar el disco duro o cualquier otro dispositivo.
- d) No se deben presionar fuertemente las teclas del teclado para que funcione correctamente.
- e) No deben dejar disquetes o cds, dentro de las respectivas unidades después de haber sido utilizados.
- f) Los usuarios no deben forzar un reinicio para cancelar cualquier proceso si su equipo experimenta congelamientos, comuníquese con el personal de la Gerencia de Sistemas para asesorarlo y si es requerido deberá complementar el formulario que corresponda.

### **Computadoras portátiles**

- a) Debe almacenar los accesorios de su equipo en su respectivo maletín de viaje.
- b) No debe exponer la computadora a un detector de metales, los datos de su disco duro, disquetes o cd's pueden perderse.



## **Impresores**

- a) No debe presionar fuertemente los botones del panel de control del impresor.
- b) No debe imprimir en papel copia, ya que éste es muy delgado, se recomienda utilizar papel base 20.
- c) No debe apagar el impresor para mover el rodillo o los cabezales de impresión en forma manual.
- d) No debe conectar los impresores láser directamente al UPS, ya que la demanda eléctrica de estos es superior a los otros tipos de impresor, excepto si tiene garantizado que la capacidad del UPS es adecuada para soportar éste tipo de impresores.
- e) No deben halarse las hojas para “agilizar” la impresión, ya que estaría forzando algunas piezas del mecanismo del impresor que podrían dañarse y luego presentar problemas en la tracción del papel.

## **Sistemas de protección (UPS y reguladores de voltaje)**

- a) No debe sobrepasar el límite de capacidad permitida de voltaje.
- b) No deben conectarse a éstos ningún otro tipo de dispositivo (sacapuntas, contómetros, radios, parlantes, etc.)
- c) En caso de falta de energía, debe guardar sus archivos y apagar todo el equipo inmediatamente.
- d) No debe apoyar objetos sobre estos equipos.
- e) Si tiene dudas sobre cómo conectar la computadora al equipo de protección (ups), consulte con un técnico de la Gerencia de Sistemas.

## **7. MANTENIMIENTO CORRECTIVO**

Todos los requerimientos por fallas y asistencias de problemas de hardware y software de la institución, deberán ser enviados por los usuarios afectados a la Gerencia de Sistemas,

### **Respaldos de Información**

Cada usuario es responsable de almacenar y actualizar la información a ser respaldada de sus equipos, para tal efecto, en la raíz de sus discos duros deberá existir una carpeta denominada “Backup INDES” y estrictamente, deberán almacenar en dicha carpeta únicamente la información laboral, es decir, no deberá almacenar en dicha carpeta, archivos de música, video o información personal. Es responsabilidad de la Gerencia de Sistemas realizar el respaldo de ésta carpeta de todos los equipos, lo cual se realizará en el tiempo estipulado por Gerencia de Sistemas.

Se recomienda a los usuarios realizar copias de seguridad de sus archivos de trabajo en cualquier momento, a fin de protegerse de pérdidas de información por fallas en el equipo, dichas copias de seguridad pueden almacenarse en CD's, memorias, discos duros externos, etc.

## **8. ADQUISICION Y ELIMINACION DE LOS EQUIPOS**

- a) Es responsabilidad total del área solicitante, gestionar las autorizaciones necesarias para sustituir el equipo extraviado o deteriorado en forma parcial o total dentro o fuera del período de garantía, dicha adquisición deberá contar con el Visto Bueno de la Gerencia de Sistemas y deberá ser autorizada por el Gerente de Área correspondiente.
- b) La responsabilidad de la Gerencia de Sistemas sobre el equipo informático asignado a esta Gerencia finalizará hasta que dicho equipo haya sido debidamente entregado a la Gerencia de Operaciones de Activo Fijo por las siguientes causas: a) equipo resultante del programa anual de sustitución, b) equipo dañado e irreparable y c) Equipo extraviado.

## **9. UBICACIÓN Y RESPONSABILIDAD SOBRE LOS EQUIPOS**

- a) Es responsabilidad del Jefe inmediato, garantizar que los usuarios de su área verifiquen y firmen debidamente el listado de asignación de equipo informático emitida por Activo Fijo, cada vez que se actualice, el cual deberá contar con su firma.
- b) Cada usuario será responsable por la seguridad total del equipo instalado y asignado a su persona, de acuerdo a lo detallado en el reporte de equipo firmado al Área de Activo Fijo.
- c) Todo cambio de ubicación física de cualquier equipo de cómputo, debe previamente notificarse al Área de Activo Fijo con el documento establecido para esto, remitiendo copia al Área de Informática.
- d) En caso de no notificar el cambio de ubicación, y el equipo se extravía o sufre algún desperfecto, el empleado que tiene asignado este equipo dentro del inventario será el único responsable de su equipo asignado.
- e) El equipo informático deberá ubicarse en un local limpio, con suficiente ventilación natural o artificial, evitando exposición directa a la luz solar y mantener las áreas de ventilación de los equipos sin obstrucción.
- f) El espacio y mobiliario destinado para el equipo informático deberá ser fijo, procurando evitar vibraciones o golpes a los equipos y a los muebles.
- g) La responsabilidad de la Gerencia de Sistemas sobre los equipos informáticos, se limita al mantenimiento preventivo y correctivo de los mismos, así como de emitir las recomendaciones sobre el uso adecuado de los mismos.
- h) Cuando un empleado, unidad o gerencia institucional necesiten mantenimiento correctivo, el cual involucre el movilizar el equipo al área de la Gerencia de Sistemas, es responsabilidad del solicitante la elaboración y autorización del movimiento de ese equipo utilizando para ello el procedimiento definido por la unidad de Activos Fijos de INDES.

## **10. PROTECCION CONTRA VIRUS**

- a) Todos los usuarios deben asegurarse que el programa antivirus se cargue automáticamente cada vez que su computadora sea encendida, de lo contrario, notifique al personal de Informática. Haciendo uso de requerimiento.
- b) Todos los usuarios deben revisar todos los disquetes que vaya a utilizar en su computadora con el programa antivirus para prevenir que ésta sea infectada, si es que estos son de procedencia externa a la institución.
- c) Todos los usuarios deben ejecutar al menos una revisión semanal de todos los archivos de su disco duro.
- d) Si su computadora es infectada por algún virus, no continúe compartiendo información e informe inmediatamente al Área de informática, para que le ayuden a eliminarlo, Por medio de Requerimiento.
- e) Después de alguna infección, y posterior a su limpieza, debe asegurarse de revisar los disquetes con los que haya estado trabajando, para evitar que su equipo se contamine nuevamente.

## **11. SEGURIDAD**

- a) Todos los usuarios están obligados a colaborar en una investigación de seguridad.
- b) Si encuentra un problema de seguridad en la red del equipo informático, debe notificar al Área de Informática inmediatamente. No señale este problema a otras personas.
- c) Es totalmente prohibido utilizar el MODEM de la computadora para realizar conexiones hacia afuera de la red institucional o hacia la misma, excepto que se cuente con la autorización del Gerente de área correspondiente, de lo cual se deberá remitir copia al Área de Informática.
- d) Si el usuario tiene alguna duda con respecto al uso de su equipo informático, debe acudir a los técnicos de la Gerencia de Sistemas, para que despejen sus dudas ampliando las explicaciones que sean necesarias.
- e) Es responsabilidad de los usuarios almacenar los archivos de forma ordenada en la computadora asignada, en una carpeta definida para ello, a fin de evitar que en un problema con la misma, los datos no se encuentren a la hora de hacer un respaldo de los datos previo a una reinstalación completa del sistema.

## **12.DATOS**

- a) Cada usuario es responsable de la información que se encuentra almacenada en su computador.
- b) El equipo informático es propiedad del estado, por lo tanto, los datos almacenados en el mismo, también son propiedad del estado.
- c) El personal de la Gerencia de Sistemas, por la naturaleza de sus funciones, puede tener acceso a la información almacenada en un equipo, pero UNICAMENTE para fines de respaldo y/o restauración de los mismos.
- d) La Gerencia de Sistemas no se responsabiliza de respaldos de archivos personales, música, películas u otros de índole NO LABORAL que se encuentren en un equipo informático.
- e) Se prohíbe terminantemente el almacenamiento excesivo de archivos personales en los equipos, lo cual provoque que el equipo responda lentamente por tener el(los) disco(s) duro(s) llenos.
- f) Se prohíbe terminantemente el almacenamiento y proceso de archivos personales en los equipos, disquetes, memorias, discos duros externos, etc. Que pongan en riesgo la INFORMACION LABORAL, tal es el caso de archivos ejecutables, y otros que puedan contener troyanos, virus, spyware y otros tipos de software malicioso.

## **13.RECURSOS DE LA INSTITUCION**

- a) No está autorizado el uso de Internet para efectos NO LABORALES, ya que se mal utiliza el ancho de banda del enlace, lo que ocasiona que otras actividades internas LABORALES, se desarrollen lentamente.
- b) No está autorizado el uso de los recursos de impresión para documentos NO LABORALES.

## **14. RESPONSABILIDADES**

- a) Las Jefaturas de cada área velaran porque en el lugar donde exista el equipo informático, los usuarios no coman, beban, fumen o mantengan productos alimenticios especialmente líquidos cerca de estos, ya que pueden representar un riesgo para los mismos, adicionalmente, deben tener cuidado en el manejo de clips, grapas y otros materiales metálicos, para que no se introduzcan en el teclado, monitor e impresores, ni mantenerlos cerca de los disquetes, discos compactos, etc.
- b) Es responsabilidad de TODOS los usuarios, guardar la confidencialidad respectiva referente a la información que se genere en la institución, en caso contrario, se apegará a lo establecido en el apartado “Faltas y Sanciones” de esta normativa.
- c) En los casos en que un usuario renunciare o fuese despedido y éste tuviere equipo informático asignado, es responsabilidad de su Jefe Inmediato Superior reportar al Área de Informática y a la Unidad de Activo Fijo, la situación de ese equipo.
- d) En caso de transportarse en vehículo, debe asegurarse de que el equipo no se deslice de un lugar a otro dentro del vehículo.
- e) Las jefaturas y los coordinadores de cada área, tendrán la autoridad necesaria para cumplir y hacer cumplir esta normativa.

## **15. FALTAS**

Las sanciones las determinará Gerencia General y Gerencia de Sistemas, de acuerdo a la gravedad de la falta cometida, tomando como parámetro los siguientes tres tipos: Leves, Graves y Muy Graves.

### **LEVES**

Se consideran faltas leves, las que perturban la disciplina del área de trabajo, por ejemplo:

- a) Utilizar volumen excesivo de parlantes.
- b) Reproducir música, videos, correos y otros de contenido inmoral, dañino, degradante, pornográfico, racista y otros que atenten contra la moralidad y la ética personal.

### **GRAVES**

Se consideran faltas graves las que ponen en riesgo la integridad de los equipos y/o generan un mal uso y manejo del equipo.

Por ejemplo:

- a) Rayar, colocar en ubicaciones de riesgo o colocar objetos peligrosos en los equipos (ej. Tazas de café, vasos de agua) o poner objetos pesados sobre ellos.
- b) Uso para fines no laborales.
- c) Sacar de la institución equipos sin la debida autorización o justificación.

### **MUY GRAVES**

Se consideran faltas tipo muy grave las que dañan a terceros y las que provocan un daño reversible o irreversible a los equipos y material tecnológico ya sea en el hardware y/o en el software.

Por ejemplo:

- a) Utilizar cuentas de otros usuarios para fines dañinos a la imagen del dueño de la cuenta o de la institución, el mandar correos electrónicos anónimos.
- b) Instalar programas sin autorización en las computadoras de la institución.
- c) Provocar daño intencional o negligente a los equipos tecnológicos de la institución.
- d) Eliminar archivos de sistema de los equipos.
- e) Navegar en sitios prohibidos o peligrosos
- f) Generar multas o sanciones a la institución o personales.
- g) Extraer y/o divulgar información confidencial de los equipos informáticos de la institución.

## **16.SANCIONES**

Clases de Sanciones

Por las infracciones que se cometan al presente reglamento se aplicarán las siguientes sanciones leves, graves y muy graves.

Aplicación de sanciones

La imposición de las sanciones se hará de acuerdo a la siguiente tabla:

Sanciones Leves:

- Amonestación verbal por el jefe inmediato
- Amonestación por escrito con copia al Gerente de Informática, Recursos Humanos de parte del jefe inmediato.

Sanciones Graves:

- Reporte por escrito con copia al expediente, Gerencia de Sistemas y Gerencia General.
- Baja en el uso de la cuenta del usuario, privilegios y derechos de red.

Sanciones Muy Graves:

- Reporte por escrito con copia al expediente, Gerencia de Sistemas y Gerencia General.
- Multa o reposición de equipo dañado (cuando este fuere el caso)
- Despido o traslado

Todo caso detectado debe ser registrado, aunque no amerite sanción, en caso de obtener tres reportes o de acuerdo a la gravedad del caso o de reincidencias, se aplicara una sanción de acuerdo a los reportes anteriores.

## **17.SOBRE LO NO PREVISTO**

Los puntos no previstos dentro de esta normativa serán resueltos por el Gerencia General y Gerencia de Sistemas, quedando a su juicio someter a consideración del resto del Personal Ejecutivo de la institución, los puntos que considere necesarios.

## **18.VIGENCIA**

La presente normativa entrará en vigencia a partir de la fecha de su autorización.



## INSTITUTO NACIONAL DE LOS DEPORTES DE EL SALVADOR

Documento elaborado:  
Gerencia de Sistemas  
Ing. Beatriz Abarca - Gerente

Revisión Administrativa:  
Lic Rubén Vásquez, Gerente General  
Lic. José René Medina, Auditor Interno Institucional  
Febrero, 2010

**El Instructivo de Uso y Manejo de los Recursos Informáticos, Versión 1.0 de febrero de 2010 ha sido aprobado por la Junta Directiva del Instituto Nacional de los Deportes de El Salvador en el artículo 6° de la sesión N° 6, acuerdo N° 028-06-2010 celebrada el 24 de febrero de 2010.**