ACTA 4427

Acta de la sesión ordinaria celebrada por la Junta Directiva del Instituto Nacional de Aprendizaje en el Centro Nacional de Formación de Comercio y Servicios INA a las diecisiete horas del quince de febrero de dos mil diez con la asistencia de los siguientes directores:

Sr. Carlos Sequeira Lépiz	Presidente Ejecutivo, quien preside
Sr. Álvaro González Alfaro	Vicepresidente
Sra. Alejandrina Mata Segreda	Viceministra de Educación Pública
Sra. Xiomara Rojas Sánchez	Directora
Pbro. Claudio Maria Solano Cerdas	Director
Sr. Manuel González Murillo	Director
Sr. Luis Fernando Monge Rojas	Director
Sr. Edgar Chacón Vega	Director

POR LA ADMINISTRACIÓN:

Sr. Ricardo Arroyo Yannarella	Gerente General
Sr. Erick Román Sánchez	Subgerente
Sr. Esteban González Maltés	Asesor Legal

POR AUDITORIA INTERNA

Sr. Elias Rodríguez Chaverri	Auditor Interno

POR LA SECRETARIA TÉCNICA:

Sr. Francisco Azofeifa González	Encargado Secretaria de Actas
Sra. Elineth Ortiz Zúñiga	Secretaria de Actas

AUSENTES

Sra. Olga Cole Beckford Por asuntos de trabajo.

ARTICULO PRIMERO:

Presentación del Orden del Día:

Se aprueba el orden de día de la siguiente manera:

1. Presentación Del Orden Del Día.
2. Estudio y Aprobación de Acta 4426.
3. Correspondencia
   3.1 SITRAINIA DOC 18-10
4. Reflexión.
5. Informe Final Proyectos año 2009 de la Unidad de Cooperación Externa
6. Reglamento de Uso de Recursos Informáticos del INA. (Entregado en la sesión 4426 de 10 de febrero)
7. Informes de la Dirección.
   - Revocatoria de vacaciones del señor Presidente Ejecutivo.
8. Mociones y Varios.

ARTICULO SEGUNDO:

Estudio y aprobación del acta N° 4426.

El señor Presidente, somete a discusión el Acta No. 4426, la cual no tiene observaciones al respecto y por acuerdo de los miembros se aprueba.

ARTICULO TERCERO

Correspondencia.

3.1 Oficio Sitraina Doc 18-10, suscrito por el Secretario General de SITRAINA.

Se da lectura a la copia dirigido a la Junta Directiva, en el cual solicitan uniformes para los funcionarios del subsector Belleza y Estética del Núcleo Procesos Artesanales, con la finalidad de protegerse de los materiales y químicos que utilizan en los servicios de capacitación.

La directora Rojas Sánchez, propone que se traslade a la administración para que ese valore la solicitud, a lo cual los señores directores y directoras manifiestan su anuencia:

Considerando:

1. Que se conoce en el apartado de correspondencia el oficio de SITRAINA DOC 18-10, suscrito por el señor Jorge Gamboa, Secretario General de SITRAINA, donde solicitan uniformes para los funcionarios del Subsector Belleza y Estética del Núcleo Procesos Artesanales, con la finalidad de protegerse de los materiales y químicos que utilizan en los servicios de capacitación.

2. Que una vez analizado y discutido dicho oficio los señores y señoras directores, consideran necesario solicitar a la administración que valore la solicitud planteada por SITRAINA:

POR TANTO ACUERDAN:

SOLICITAR A LA ADMINISTRACIÓN QUE VALORE LA SOLICITUD PLANTEADA POR EL SINDICATO DE TRABAJADORES DEL INA, MEDIANTE EL OFICIO SITRAINA DOC 18-10.

ACUERDO APROBADO POR UNANIMIDAD. N°016-2010-JD.

3.2 Publicación en la Gaceta sobre la Modificación del Decreto.

El señor Gerente General, indica que ya salió publicado en la Gaceta N°29, del 11 de febrero de 2010, la publicación de la Reforma al Decreto Ejecutivo N°15135-TSS, de 05 de enero de 1984, en el cual se da la posibilidad de hacer vinculante el tema del Sistema Nacional de Formación Profesional; por lo que considera importante tomar un acuerdo donde la Junta Directiva toma nota de la publicación e instruye a administración de que realice las modificaciones internas correspondientes y que se comunique a la Contraloría. También con esta publicación se da por cumplida la recomendación de la Contraloría General de la República.

El director Chacón Vega, consulta si el tema tiene efectos en entes privados que se dedican a la capacitación y qué previsiones habría que tomar en esta línea?

El señor Gerente General, señala que en el documento de la reorganización que se presentó hace unas semanas, ya se había incorporado el Sistema Nacional de Formación Profesional, donde Gestión Compartida, pasaba a ser la rectora del SINAFOR, y ya con el Reglamento se debe iniciar una amplio proceso de comunicación

para que los entes privados participen de los servicios que brinda el INA; sin embargo se está a la espera de la comunicación de MIDEPLAN.

El director Chacón Vega, indica que en Acreditación el mecanismo es que ente privado es el que solicita a la Institución que se le acredite; pero no sabe si el SINAFOR implica que como iniciativa INA haga un primer inventario o promueva un censo, etcétera, para que de oficio inicie con evaluaciones.

El señor Gerente General, indica que se tiene a nivel voluntario, pero habría que diseñar en acreditación el sistema y ver también el nivel de vinculación y que lo asuma el empresario; no obstante en primera instancia es publicar y ver la afluencia y reacción que se estaría dando.

El señor Presidente, somete a consideración de los señores directores y directoras, la Publicación de Gaceta 29, del 11 de febrero de 2010, sobre la comunicación de reforma al Decreto Ejecutivo N°15135-TSS, de 05 de enero de 1984.

Considerando

1. Que en cumplimiento a las disposiciones emanadas en el Informe de la Contraloría General de la República DFOE-SOC-14-2009, numeral 4.1 A; y en cumplimiento al acuerdo N° 030-2009 tomado por la Junta Directiva, la Presidencia Ejecutiva conforma una Comisión interna de trabajo, quienes se dieron a la tarea de elaborar la propuesta "Fundamentación del Sistema Nacional de Formación Profesional (SINAFOR)".

2. Que en la sesión 4389, del 04 de junio de 2009, se conoce y aprueba la propuesta de Sistema Nacional de Formación (SINAFOR), mediante comunicado acuerdo N° 052-2009-JD.

3. Que la administración superior presenta a la Junta Directiva la publicación en la Gaceta N°29, del 11 de febrero de 2010, en el cual se comunica la Reforma al Decreto Ejecutivo N°15135-TSS, de 05 de enero de 1984.

4. Que la Junta Directiva toma nota de la respectiva publicación de la Gaceta N° 29 y por unanimidad acuerdan:

POR TANTO ACUERDAN

1. **TOMAR NOTA DE LA PUBLICACIÓN EN GACETA N°29, DEL 11 DE FEBRERO DE 2010, SOBRE LA REFORMA AL DECRETO EJECUTIVO N°15135-MTTSS, DEL 05 DE ENERO DE 1984, "REGLAMENTO A LA LEY ORGANICA DEL INSTITUTO NACIONAL DE APRENDIZAJE"; REFERIDO AL TEMA DE LA ORGANIZACION Y COORDINACIÓN DEL SISTEMA NACIONAL DE FORMACION PROFESIONAL.**

2. **SE AUTORIZA A LA ADMINISTRACIÓN PARA REALIZAR LAS MODIFICACIONES CORRESPONDIENTES EN LOS DIFERENTES INSTRUMENTOS DE CONTROL, SEGUIMIENTO, PLANIFICACIÓN Y PRESUPUESTARIOS; A FIN DE CUMPLIR CON LA GESTIÓN RECTORA ENCOMENDADA AL INSTITUTO NACIONAL DE APRENDIZAJE.**

3. **ASIMISMO REMITIR COPIA DEL ACUERDO A LA CONTRALORIA GENERAL DE LA REPUBLICA.**

ACUERDO FIRME POR UNANIMIDAD. N°017-2010-JD.

ARTICULO CUARTO

Reflexión

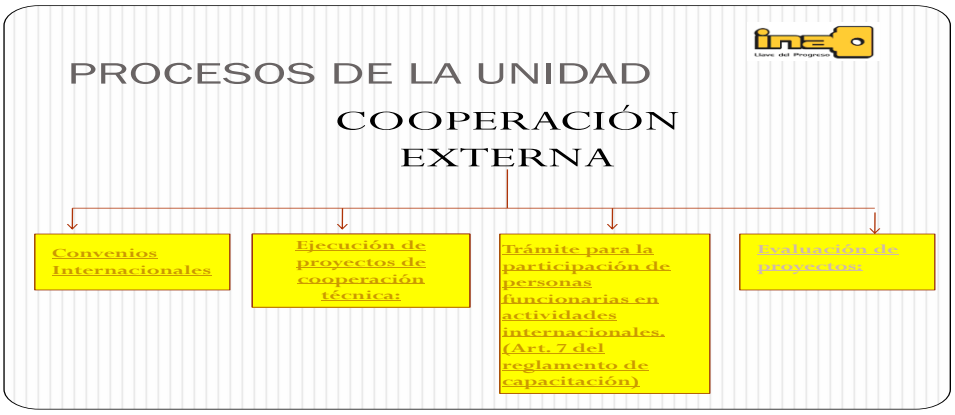
El director Chacón Vega, procede con la reflexión de hoy.

ARTICULO QUINTO

Informe Final Proyectos año 2009 de la Unidad de Cooperación Externa

El señor Presidente, somete a consideración de los integrantes de Junta Directiva la presentación del tema, que será expuesto por el señor Fernando Rodríguez Araya, Encargado de Cooperación Externa:

El señor Rodriguez Araya, procede con la presentación de acuerdo con las siguientes filminas:



Convenios de Cooperación suscritos por la institución

- 6 convenios de cooperación con países como
  - México (CP+L/Universidad de Aguas Calientes)
  - España (IMH)
  - Paraguay (SNPP/SINAFOCAL)
  - República Dominicana (INFOTEP)

Proyectos de Cooperación negociados

- Se logró negociar 20 proyectos de Cooperación con países como:
  - Francia (ECTI, GNFA, LOUIS LUMIERE y EMBAJADA)
  - Brasil (SENAI)
  - Colombia (SENA y CTD ASTIN)
  - Holanda (RADIO NEDERLAND)
  - España (AECID, JOVELLANOS, UAB y CENECOOP)
  - México (INST. TEC MONTERREY)
  - Italia (VOLUNTARIOS SENIOR)
  - Japón (JICA)
  - Israel (HAIGUD)
  - Corea (KOTRA)
  - CINTERFOR
- En total se capacitaron alrededor de 1100 (estudiantes/funcionarios). Además de la participación en proyectos de capacitación de10 empresas de los sectores.
  - Moldura y fundición
  - Panificación

De los 20 proyectos negociados, 13 se lograron ejecutar

Proyectos de Cooperación ejecutados por la institución

- Se logro atender necesidades de Unidades como el:
  - Núcleo Tecnología de Materiales (Gestión ambiental e Industria del Plástico)
  - Industria Alimentaria (Panificación/ Procesamiento prod. marinos)
  - Núcleo Metal Mecánica (Moldura y Fundición)
  - Núcleo Mecánica de Vehículos (Transmisión automática)
  - Comercio y Servicios (Locución, Producción, Idiomas)
  - Núcleo agropecuario (Hidroponía)
  - Núcleo Turismo (Servicios Turísticos/ manejo hoteles escuela)
  - Núcleo Proceso artesanal (artesanas)
  - Asesoría de la Mujer (Género)
  - UTEFOR (Aulas Mentor/ e-learning)
  - PyME's (emprendedurismo)

Capacitaciones fuera del país

- Participaron 33 funcionarios mediante su respectiva aprobación en capacitaciones fuera del país, en 21 diferentes cursos, seminarios o pasantías
- Algunas de las áreas beneficiadas:
  - Aguas residuales, manejo de desechos sólidos
  - Pequeña empresa artesanal
  - Gestión de RRHH por competencias
  - Competitividad y productividad
  - Flexografía y prensas offset
  - Formación de marinos
  - Cosecha y postcosecha de frutas
  - Pesca y acuicultura

Participación en reuniones técnicas y pasantías

- Participaron 15 funcionarios en 11 actividades diferentes

Participación de altas autoridades en el exterior

- Participaron 11 funcionarios en 14 actividades distintas

Cooperación brindada por el INA

- El Instituto Nacional de Aprendizaje logró brindar capacitación en distintas instituciones:
  - Universidad de Don Bosco (El Salvador)
    - Exposición en el Diplomado en Pedagogía de la Formación Profesional
  - INADEH (Panamá)
    - Consultoría en Normas de Calidad en una jornada de trabajo
  - INFOP (Honduras)
    - Envío de docente a taller de diseño curricular basado en competencias laborales
  - SNPP y SINAFOCAL (Paraguay)
    - Asistencia técnica-jurídica para mejorar la gestión institucional del SNPP y apoyar el proyecto de transformación institucional

Proyectos negociados para ejecución en el 2010

- Por diferentes razones, algunos de los proyectos se negociaron para el 2010, estableciéndolos como objetivos primordiales para el presente año, sin dejar de lado la búsqueda de nuevos proyectos:
  - CTD ASTIN/SENA (Colombia):"Capacitación técnica en el proceso de transformación del plástico"
  - SENA (Colombia):"Pasantía para 2 docentes del área de turismo para conocer el avance alcanzado en Colombia con relación a la implementación de la oferta formativa (cursos, seminarios, talleres, asesorías técnicas, etc) En turismo a través del aprendizaje en línea (e-learning)

- SENA (Colombia): Proyecto del Núcleo de Turismo en turismo de aventura teleférico, Rafting, Rapel, Bosque y Carretera
- SENA (Colombia): "Taller de Preparación de Bebidas a base de Café aplicando la Técnica Llatte
- Centro de Jovellanos (España):"Formación y certificación internacional de los docentes del Núcleo Náutico Pesquero"

- ECTI: Experto para el área de Genética Animal, Núcleo Agropecuario
- ECTI: Experto en el tema de confitería, Proyecto del Núcleo de Industria Alimentaria
- ECTI: Experto para curso Chef Gourmet, Proyecto del Núcleo de Turismo
- ECTI: Negociación de experto especialista en mecánica de vehículos
- Universidad Tecnológica de Aguas Calientes (México) Asistencia al Núcleo Textil
- JICA: Experto para Proyecto de Gestión de Calidad "Establecimiento e implementación de equipos de mejoramiento continuo del sistema de Gestión de Calidad.

- JICA: Envío de experto con el fin de actualizar los conocimientos técnicos de los sectores de electricidad a partir de la utilización de nuevas formas de energías renovables.
- JICA: Envió de experto que funja como facilitador del grupo de voluntarios japoneses asignados al INA, para promover un mejor entendimiento y coordinación con la contraparte técnica en cada área asignada
- JICA: Sr. Takayoshi Tanaka, experto senior para el área de Hidroponía.
- JICA (Japón): "Procesamiento de productos marinos a nivel industrial artesanal" Sr. Hitoshi Emoto
- JICA: Envío de experto para ayudar a un mejor entendimiento con los otros cooperantes japoneses
- SENAI: Aula didáctica para la enseñanza del diseño, escalonado y corte asistido por computadora

- BID: Producción de biocombustible a partir del cultivo de *jatropha curcas l.* con el fin de su utilización como alternativa energética a nivel de finca, en el centro nacional especializado en agricultura bajo riego en Bagaces, Guanacaste
- Centro Louis Lumiere: Experto para el Centro de Imagen sobre el tema uso de tecnologías para la producción y posproducción en HD y Cine Digital
- CIM: (Alemania) Asistencia de un experto para el Núcleo de Industria Gráfica
- Voluntarios Senior: (Italia) Intercambio en el área de Gastronomía italiana

Diagnóstico de necesidades 2011-2012

- Enero-marzo 2010: Detección de necesidades de cooperación externa en núcleos, regionales y centros de formación
- Marzo-abril 2010: Establecimiento de prioridades
- Abril-junio 2010: Diseño de proyectos
- Junio-julio: incorporación en presupuesto y POIA 2011
- Julio-diciembre: Inicio de proceso de negociación con distintos entes.

Sra. Yumiko Ishihama. Coordinadora de Voluntarios japoneses
Sr. Cesar Durán. Encargado de Gestión Tecnológica, Núcleo Industria Alimentaria
Sr. Hitoshi Emoto. Cooperante japonés
Sra. Eugenia Herrera. Núcleo Agropecuario
Sr. Ishihama Tanaka. Cooperante japonés

- Sr. Jeremi De Contes. Director ejecutivo de la Cámara Franco Costarricense
- Mark Matheis. Unidad de Cooperación Externa
- Sra. Ileana Leandro Gomez. Núcleo Industria Alimentaria
- Sra. Monique Ecalé.
- Sr. Dominique Ecalé. Experto Francés

La señora Viceministra de Educación, consulta cómo se compara el INA en relación con otros institutos similares? Consulto esto ya que hay un grupo de personas en un curso de cooperación Japonesa, donde están trabajando el cierre del curso con el tema de la coordinación entre la instancia formadora profesional y las entidades del mercado laboral, incluso hay personas de varios países y de Costa Rica. Además están pidiendo información sobre la forma en que se va hacer e ir sacando conclusiones; y esto lo entrelaza en cuanto a la fortaleza del INA Costa Rica en relación los modelos exitosos que se han mencionado?

El señor Rodríguez, indica que a excepción del Sistema SENAC, SENAI, a nivel Latinoamericano están muy parejos en cuanto a Instituciones similares al INA, también a nivel Centroamericano, a nivel del Caribe, aunque los modelos son un poco diferente por ejemplo México; sin embargo considera que el INA está bien posicionado a nivel de la Región para brindar cooperación, incluso en gestión administrativo.

Por otra parte indica que hay dos fortalezas en la Institución: **1.** los modelos tripartitas se ha perdido en la región. **2**. el modelo solidario y componente de la vertiente productividad; aunque muchas instituciones iberoamericanas o latinoamericanas se mantienen con la planilla de los trabajadores, muchas de ellos están tomadas por el consejo directivo empresarial y la parte social se ha dejado de lado.

También lo que se ha generado durante estos años en los Núcleos, ya que la parte técnica es muy fuerte y los docentes INA son muy apetecidos.

El director Chacón Vega, manifiesta que la exposición es interesante. **1**. Se recuerda el presupuesto aproximado de Coopex? **2**. Existe alguna coordinación con Ministerio de Relaciones Exteriores, Cámaras, Comités de Enlace, etc?

El señor Rodríguez, indica que para traer expertos en el 2009, se ejecutaron 12 millones, en pasantías (tiquetes-viáticos) 40 millones.

En cuanto a una Asociación o entidad no existe, pero si existen las entidades que aglutinas las instituciones, también están las redes que aglutinan organismos como OIT y otros.

En cuanto a los Comités de Enlace, a través de los Núcleos se mantiene relación con los Comités de Enlace.

El director Chacón Vega, consulta **3.** Por que se decía que lo Mecánica de Vehículos es difícil?

El señor Rodríguez, comenta que fue muy difícil encontrar un Experto Francés en Mecánica de Vehículos, básicamente porque la relación con los Franceses está enfocada a necesidades especiales de mecánica de vehículos; sin embargo en diciembre estuvo un experto francés en transmisión automática, y le comentaba el Encargado del Núcleo que recibió una felicitación por parte de la Pegeot.

El director Chacón Vega, señala que sigue un poco sin entender. **4.** Como divulga Coopex su labor a lo interno y externo, usa la web por ejemplo? **5.**Hay algún ente internacional o regional que agrupe entes como Coopex y sirva de facilitador y promotor de estándares, etc.? Quizás ONU, OEA, UNESCO, CINTERFOR, etc.

El señor Rodríguez, indica en cuanto a la página WEB, aun no tiene la especicidad que debería tener, sin embargo tiene como trabajo actualizarla. En cuanto a la comunicación hay una interacción persona a persona, oficina a oficina, vía correo electrónico, telefónicas, a través de la comisión de capacitación, etcétera.

El director Chacón Vega, menciona que mientras hablaban buscó en internet pasantías (internships) y becas (schoolarships) y pide se incluya parte de lo encontrado por si sirve:

- **Scholarships for Vocational School**

Vocational training is unique in that much of the learning is experiential, or hands-on. Some **scholarships** provide funds to those students pursuing a **...**
www.college**scholarships**.org/**scholarships**/**vocational**-school.htm - Cached - Similar

- **Scholarships, Fellowships, and Loans CIRI Foundation**

Semester **scholarship**: $1000; **Vocational Training**/Career Upgrade Grant: up to $1500 received during a calendar year. See Web site for more details: **...**
www.enotes.com/**scholarships**-loans/ciri-foundation - Cached - Similar

- **[PDF]**

Scholarships for Vocational Training
File Format: PDF/Adobe Acrobat - Quick View
Scholarships for **Vocational Training**. Charles & Connie Meng **Scholarship** Program. **Scholarships** up to $500 for young people in community college **...**
www.venturesfoundation.org/pubs/.../Meng_Application_Packet.pdf - Similar

- **Vocational Training Grants scholarships: scholarships for ...**

Vocational Training Grants **scholarships** - find **Vocational Training** Grants **scholarships**, **Vocational Training** Grants **scholarship** values, **Vocational Training ...**
www.**scholarship**-search.org.uk/...**vocational-training**...**scholarships**/.../page.htm - Cached - Similar

- **South Asia Foundation - SAF Vocational Training**

Among the **scholarships** given by SAF through Open University of India and Open University of Sri Lanka, some are given for **Vocational Training**. **...**
www.southasiafoundation.org/...**scholarships**/saf_**vocational_training**.htm - Cached

- **[PDF]**
- • Washoe Tribe ADULT VOCATIONAL TRAINING SCHOLARSHIP
- File Format: PDF/Adobe Acrobat - Quick View

Washoe Tribe ADULT **VOCATIONAL TRAINING SCHOLARSHIP**. The College Financial aid Officer recommends the Washoe Tribe Grant Funding level. **...**
*www.washoetribe.us/.../Adult_**Vocational_Training_Scholarship**_Forms_April09.pdf*

- Internships & vocational training: IQDoQ Dokumentenmanagement

Those who wish to experience how HyperDoc® and FormText continue to advance, how Sales and Marketing work or how IQDoQ works in commercial practice can **...**
www.iqdoq.de/en/karriere/praktika-ausbildung.html - Cached

- **Europlacement: Internship / VOCATIONAL TRAINING PROGRAMME ...**

Internship profile: **Internship** / **VOCATIONAL TRAINING** PROGRAMME / Cameroon / Muyuka - <p>Under this programme,we want volunteers who can assist in teaching **...**
www.europlacement.com › Start › Africa - Cached

- **Internship, European Centre for Development of Vocational Training ...**

28 Oct 2009 **...** Cedefop's traineeship scheme is addressed mainly to young university graduates but also to PhD students, without excluding those who – in **...**
www.caleidoscop.org/.../**internship**-european-centre-for-development-of-**vocational-training** - Cached

- **Positions, Vocational Training, Internships: Europäische Akademie ...**

The European Academy in Berlin offers interested and motivated students an opportunity to complete a period of **internship** in the seminar division. **...**

www.eab-berlin.de/Positions-**Vocational-Training-Internships**.5+M52087573ab0.0.html - Cached

iWork | Entry-level Jobs and Internships in Europe
iWork - Entry-level Jobs and **Internships in Europe ...** Entry-level job and internship opportunities for young Internationals. Login to iWork » **...**
Login to iWork - Offers - Offerte di primo impiego e stage in ...
www.iagora.com/iwork/ - Cached - Similar

European Internships | Internship opportunities in Europe
Internships programs in **europe** for practice and trainees. Get work experience in **europe**.
www.**europe**an**internships**.com/ - Cached - Similar

EPA Internships: Educational Programs Abroad
EPA **Internships in Europe**. Your passport to the experience of a lifetime! Work in an exciting and challenging internship in the field of your choice that **...**
www.epa-**internships**.org/ -

*CDS **International** | **Internships** in USA, Work Abroad, **Internships** **...***

*CDS **International** is a nonprofit organization that administers trainee exchanges , **internships**, and work/study programs for college students and young **...***
www.cdsintl.org/ - *Cached - Similar*

*Home | IE3 Global **Internships***
*IE3 Global **Internships**. Education, Experience, Employment **...** Copyright © 2008. Oregon University System. **International** Programs. All rights reserved.*
ie3global.ous.edu/ - Cached - Similar

El director González Murillo, indica que uno de los objetivos fundamentales de la red Centroamericana de Centros de Capacitación Técnica, fue homologar aspectos que eran transversales, como fue el caso los perfiles profesionales, por lo que consulta sobre el avance que se ha dado en la Red, sobre estos temas?

El señor Rodríguez, indica que se ha avanzada bastante, e incluso con el apoyo del proyecto FOIL, se le dio un impulso fuerte, no solo con la traída de expertos a cada una de las Instituciones, sino con la mayor celeridad en el trabajo de los directores y los técnicos; además se generaron documentos importantes en homologación de competencias en algunas ocupaciones del área turística, construcciones, formador de formadores. También los directores siguen trabajando en la formación de competencias en la TIC´s.

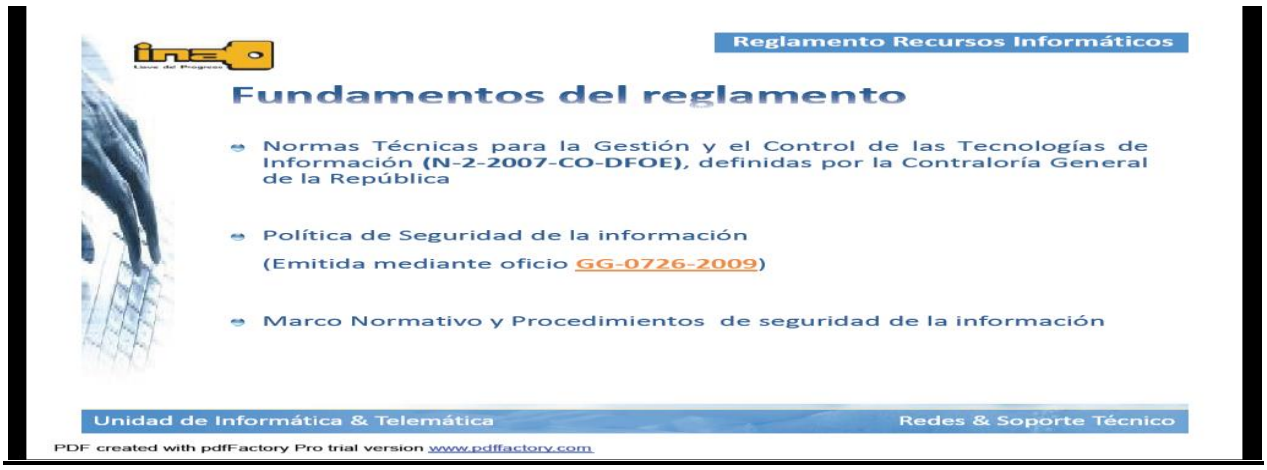
El director González Murillo, consulta en cuanto a la capacitación de instructores, existe algún plan o cronograma?

El señor Rodríguez, indica que un plan en específico de capacitación para un área específica desconoce si existe, sin embargo existe un trabajo orientado hacia la homologación de competencias hacia la documentación de perfiles por competencias, ya validados a nivel interno; pero considera que se ha trabajado bastante bien.

Se da por recibida la información.

ARTICULO SEXTO

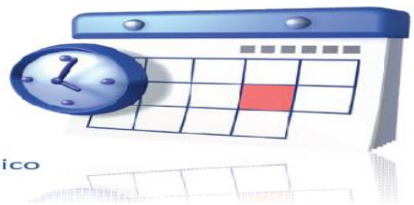
Reglamento de Uso de Recursos Informáticos del INA.



Reglamento Recursos Informáticos

Agenda

- Introducción
- Fundamentos del reglamento
- Disposiciones Generales
- Uso y seguridad de los recursos
- Control de acceso (Contraseñas)
- Uso de Internet
- Uso del servicio de correo electrónico
- Escritorio y pantalla limpia
- Privacidad y protección de la información
- Manipulación y destrucción de datos



Unidad de Informática & Telemática — Redes & Soporte Técnico

Reglamento Recursos Informáticos

Disposiciones Generales

- **Objetivo** - Normar los aspectos tecnológicos y administrativos relacionados con el aseguramiento de la información institucional (**confidencialidad**, **integridad** y **disponibilidad**), para mantener una protección adecuada sobre los recursos informáticos del INA, abarcando la información almacenada y transmitida por medio de los recursos de las tecnologías de información y comunicaciones.

- **Ambito de acción** – Lo enunciado en el presente reglamento es aplicable a todos los funcionarios del INA y usuarios de los recursos informáticos.

Unidad de Informática & Telemática — Redes & Soporte Técnico

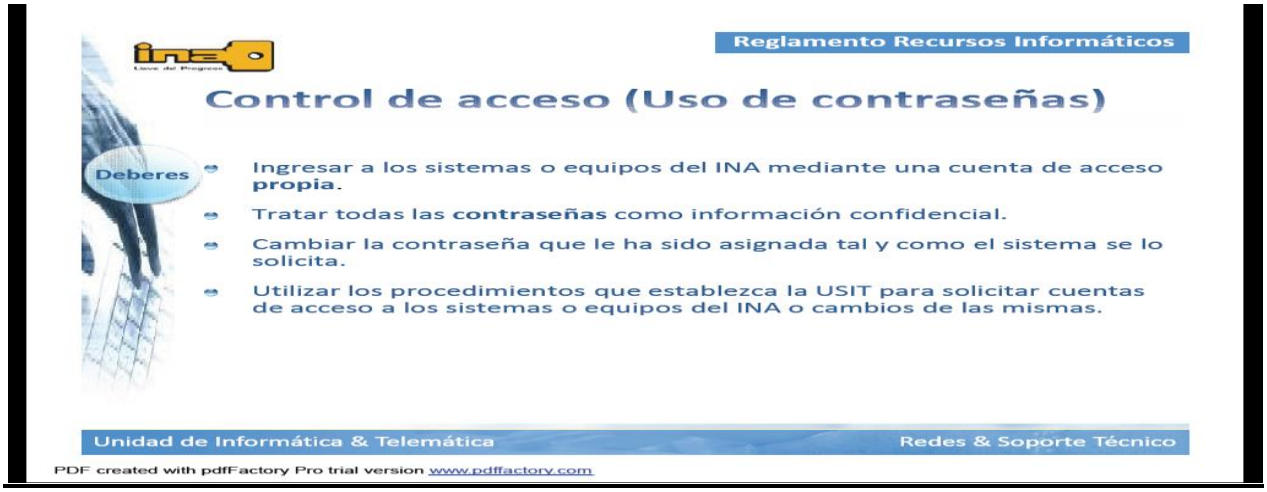
Reglamento Recursos Informáticos

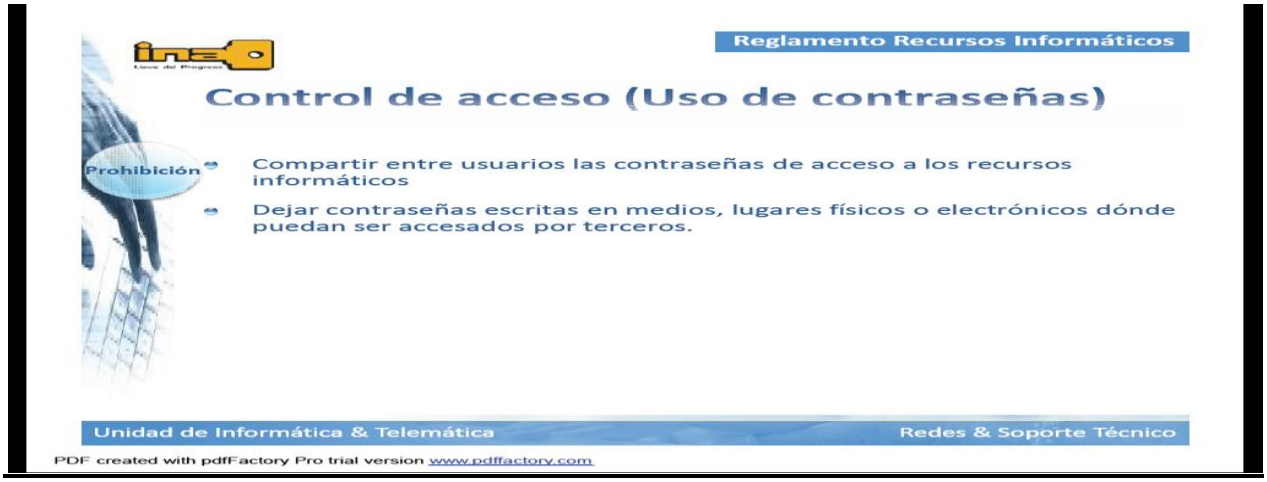
Uso y seguridad de los recursos informáticos

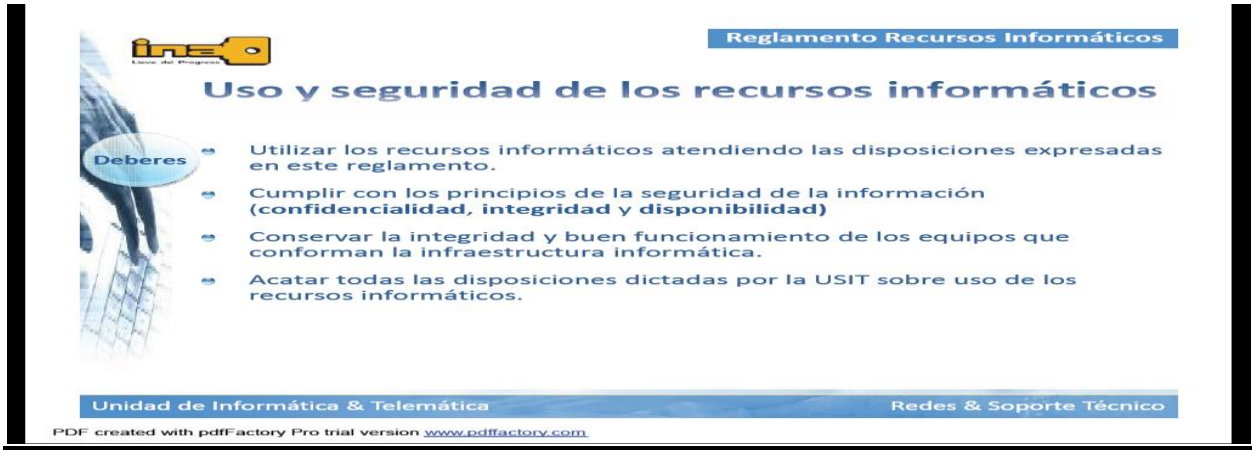
Prohibición

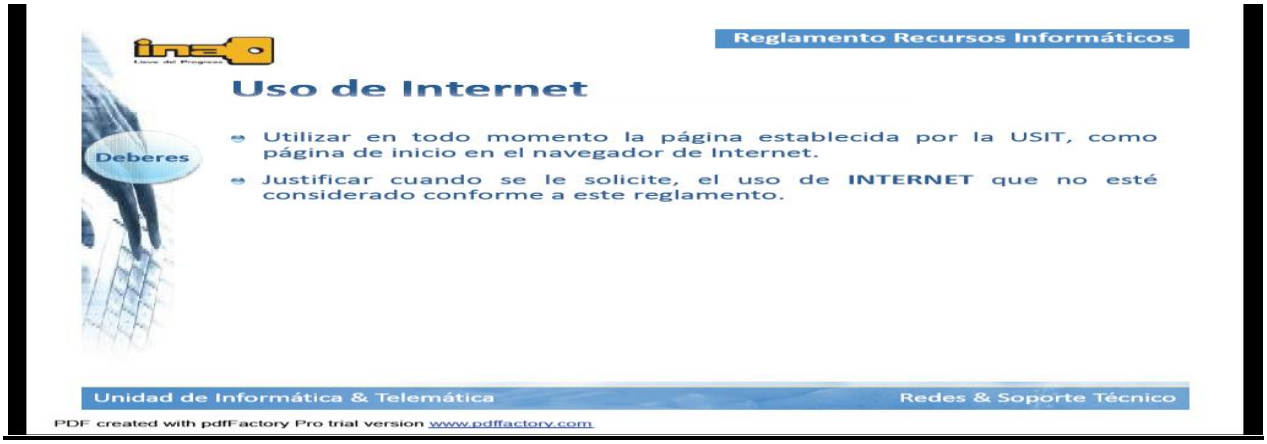
- Almacenar en el equipo asignado o en el disponible en la red, archivos de cualquier tipo ajenos a los fines e intereses de la institución.
- Guardar, distribuir materiales, fotografías, música, videos, mensajes, documentos o cualquier otro tipo de archivo que no tengan relación con sus funciones dentro del INA.
- Suprimir, modificar, borrar o alterar los medios de identificación de los equipos, o entorpecer de cualquier otra forma los controles establecidos para fines de inventario.

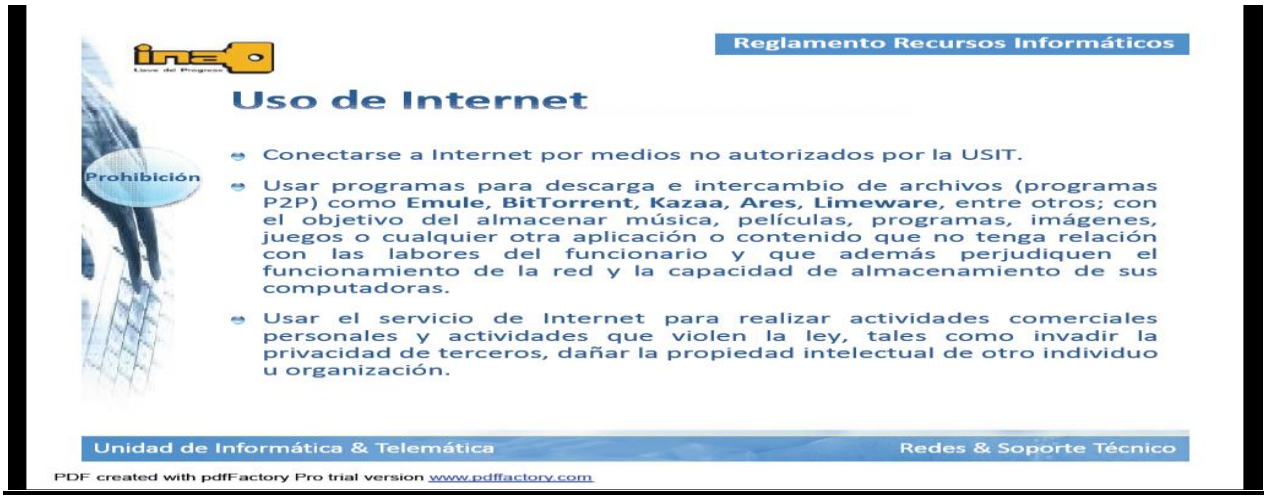
Unidad de Informática & Telemática — Redes & Soporte Técnico


Reglamento Recursos Informáticos
Control de acceso (Uso de contraseñas)
Deberes
Ingresar a los sistemas o equipos del INA mediante una cuenta de acceso **propia**.
Tratar todas las **contraseñas** como información confidencial.
Cambiar la contraseña que le ha sido asignada tal y como el sistema se lo solicita.
Utilizar los procedimientos que establezca la USIT para solicitar cuentas de acceso a los sistemas o equipos del INA o cambios de las mismas.
Unidad de Informática & Telemática
Redes & Soporte Técnico
PDF created with pdfFactory Pro trial version www.pdffactory.com

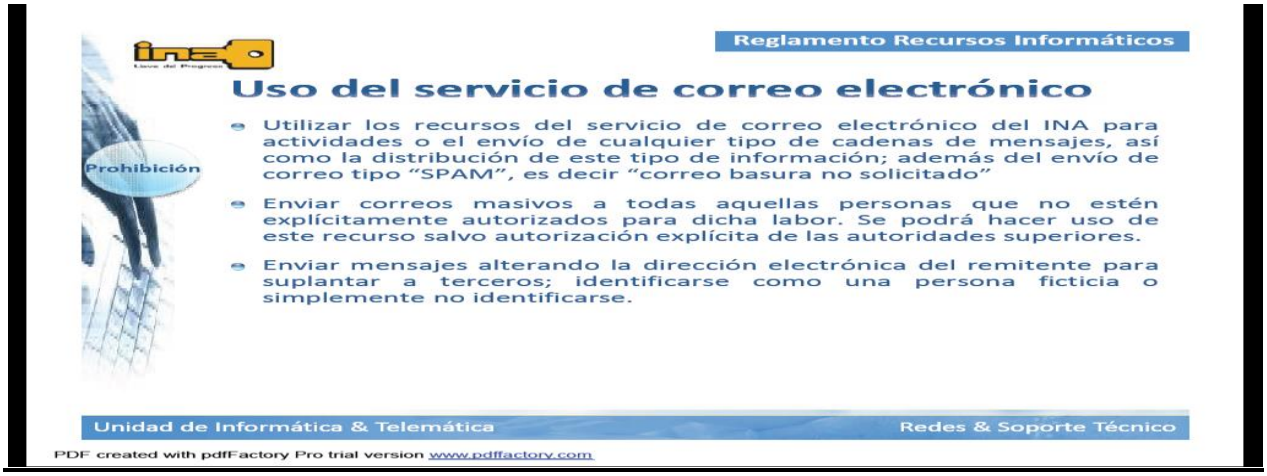

Reglamento Recursos Informáticos
Control de acceso (Uso de contraseñas)
Prohibición
Compartir entre usuarios las contraseñas de acceso a los recursos informáticos
Dejar contraseñas escritas en medios, lugares físicos o electrónicos dónde puedan ser accesados por terceros.
Unidad de Informática & Telemática
Redes & Soporte Técnico
PDF created with pdfFactory Pro trial version www.pdffactory.com

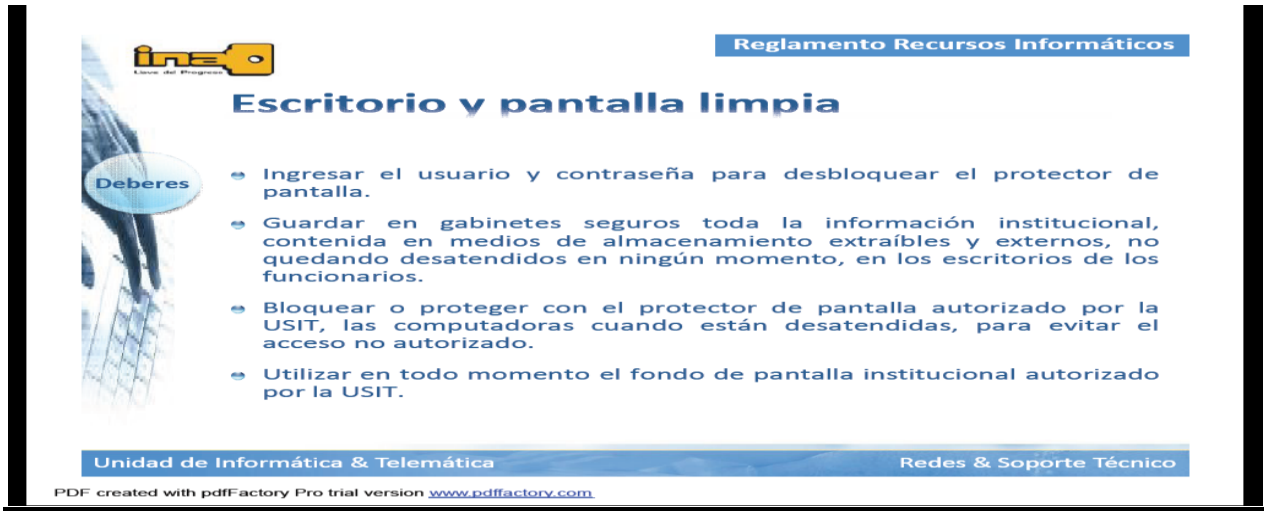

Reglamento Recursos Informáticos
Uso y seguridad de los recursos informáticos
Deberes
Utilizar los recursos informáticos atendiendo las disposiciones expresadas en este reglamento.
Cumplir con los principios de la seguridad de la información (**confidencialidad**, **integridad** y **disponibilidad**)
Conservar la integridad y buen funcionamiento de los equipos que conforman la infraestructura informática.
Acatar todas las disposiciones dictadas por la USIT sobre uso de los recursos informáticos.
Unidad de Informática & Telemática
Redes & Soporte Técnico
PDF created with pdfFactory Pro trial version www.pdffactory.com


Reglamento Recursos Informáticos
Uso de Internet
Deberes
Utilizar en todo momento la página establecida por la USIT, como página de inicio en el navegador de Internet.
Justificar cuando se le solicite, el uso de INTERNET que no esté considerado conforme a este reglamento.
Unidad de Informática & Telemática
Redes & Soporte Técnico
PDF created with pdfFactory Pro trial version www.pdffactory.com

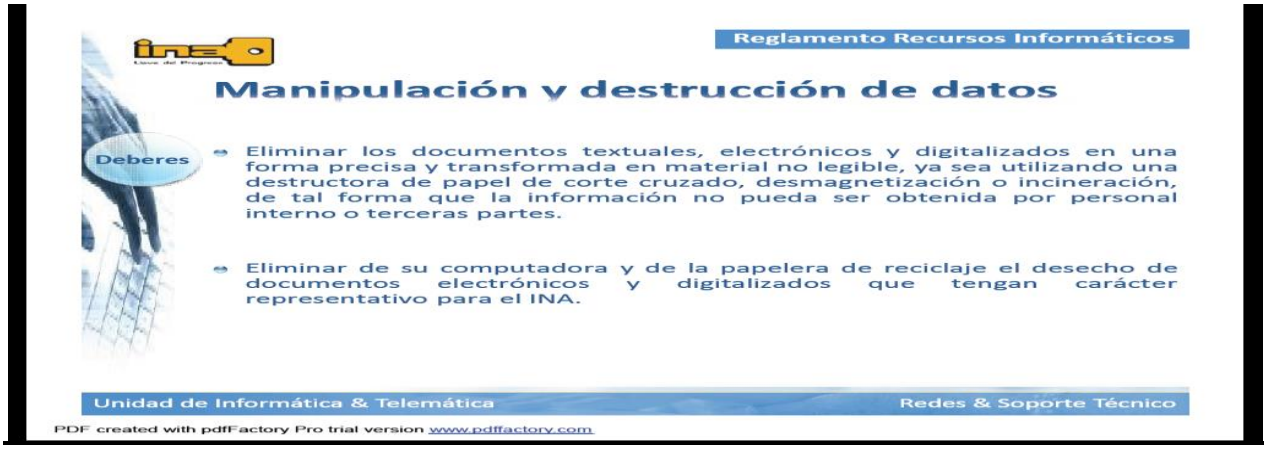

Reglamento Recursos Informáticos
Uso de Internet
Prohibición
Conectarse a Internet por medios no autorizados por la USIT.
Usar programas para descarga e intercambio de archivos (programas P2P) como Emule, BitTorrent, Kazaa, Ares, Limeware, entre otros; con el objetivo del almacenar música, películas, programas, imágenes, juegos o cualquier otra aplicación o contenido que no tenga relación con las labores del funcionario y que además perjudiquen el funcionamiento de la red y la capacidad de almacenamiento de sus computadoras.
Usar el servicio de Internet para realizar actividades comerciales personales y actividades que violen la ley, tales como invadir la privacidad de terceros, dañar la propiedad intelectual de otro individuo u organización.
Unidad de Informática & Telemática
Redes & Soporte Técnico
PDF created with pdfFactory Pro trial version www.pdffactory.com


Reglamento Recursos Informáticos
Uso del servicio de correo electrónico
Deberes
Hacer un uso responsable y adecuado del servicio de correo electrónico, en el contexto estricto de las actividades laborales asignadas por la Institución.
Revisar su cuenta de correo electrónico frecuentemente, de tal forma que descargue todos aquellos mensajes almacenados en el servidor a su computador; manteniendo con ello el espacio disponible en su cuenta de correo.
Indicar en todo correo electrónico que sea enviado desde el INA, un asunto o "subject" claro y relacionado con el contenido del mensaje, caso contrario podrá ser eliminado o ignorado
Incluir una firma automatizada en todo correo electrónico que sea enviado desde el INA (Nombre completo del usuario. -Unidad, Proceso o Núcleo, para el cual trabaja. -Correo electrónico del funcionario o usuario. -Número de teléfono o teléfonos de contacto del funcionario o usuario. -Aviso de confidencialidad.)
Unidad de Informática & Telemática
Redes & Soporte Técnico
PDF created with pdfFactory Pro trial version www.pdffactory.com


Reglamento Recursos Informáticos
Uso del servicio de correo electrónico
Prohibición
Utilizar los recursos del servicio de correo electrónico del INA para actividades o el envío de cualquier tipo de cadenas de mensajes, así como la distribución de este tipo de información; además del envío de correo tipo "SPAM", es decir "correo basura no solicitado"
Enviar correos masivos a todas aquellas personas que no estén explícitamente autorizados para dicha labor. Se podrá hacer uso de este recurso salvo autorización explícita de las autoridades superiores.
Enviar mensajes alterando la dirección electrónica del remitente para suplantar a terceros; identificarse como una persona ficticia o simplemente no identificarse.
Unidad de Informática & Telemática
Redes & Soporte Técnico
PDF created with pdfFactory Pro trial version www.pdffactory.com


Reglamento Recursos Informáticos
Escritorio y pantalla limpia
Deberes
Ingresar el usuario y contraseña para desbloquear el protector de pantalla.
Guardar en gabinetes seguros toda la información institucional, contenida en medios de almacenamiento extraíbles y externos, no quedando desatendidos en ningún momento, en los escritorios de los funcionarios.
Bloquear o proteger con el protector de pantalla autorizado por la USIT, las computadoras cuando están desatendidas, para evitar el acceso no autorizado.
Utilizar en todo momento el fondo de pantalla institucional autorizado por la USIT.
Unidad de Informática & Telemática
Redes & Soporte Técnico
PDF created with pdfFactory Pro trial version www.pdffactory.com


Reglamento Recursos Informáticos
Privacidad y protección de la información
Deberes
Firmar un contrato de confidencialidad de conformidad a lo que establece la Política de Seguridad de la Información.
Utilizar la información del INA de acuerdo con los derechos que se les asignen de conformidad con sus funciones, así como conocer y cumplir las regulaciones en materia de seguridad de la información.
Unidad de Informática & Telemática
Redes & Soporte Técnico
PDF created with pdfFactory Pro trial version www.pdffactory.com



El señor Presidente, somete a consideración de los integrantes de Junta Directiva la presentación del tema, que será expuesto por el señor Gustavo Ramírez de la Peña y el señor Randall Cheves Zamora.

El señor Gerente General, comenta que la propuesta ya fue analizado y revisado por la Comisión Gerencial de informática; además ya fue revisado por la Asesoría Legal.

También en la propuesta se incluye el tema de la autorización de la apertura de las páginas en Internet, en forma personalizada con la autorización de la jefatura correspondiente. Además se están incluyendo otros aspectos en cuanto a seguridad en el manejo de la computadora, Software Aranda (permite revisar computadora desde la Unidad de Informática), etcétera.

La señora Viceministra de Educación, indica que se hace referencia a aspectos técnicos y política, sin embargo entiende que la circular de la Contraloría, incluye la aprobación de políticas generales de informática por parte del Jerarca y hasta donde conoce la información de la comisión de informática.

El señor Gerente General, indica que desde el año 1995 se tiene políticas en este tema y en el año 2006, se habían aprobado las nuevas políticas, incluso hace unos siete meses se presentó una modificación a la política general en la TIC´s; además la comisión gerencial de informativa toma una decisión a nivel administrativo, pero la

propuesta de las políticas planteadas en el reglamento serán competencia del jerarca aprobar si consideran que es cerrado o abierto.

Por otra parte las políticas se revisan cada inicio de administración, incluso se revisaron cuando se aprobó el POIA y el PEI.

Indica que podrían preparar una presentación con el histórico de las políticas y otro con la presentación del reglamento.

Los funcionarios proceden con la presentación del tema según las siguientes filminas:

La directora Rojas Sánchez, considera que este tema se deben de regular, pero para las organizaciones como SINDICATO, ASEMINA, COOPERATIVA; sin embargo se abusa con el uso del correo por ejemplo, la cooperativa satura el correo con los anuncios de ventas, ferias, etcétera; diferentes es utilizar el medio para las convocatorias, comunicaciones de autorización para participar en las asambleas. También debería unificarse para todas las instituciones públicas.

Por otra parte consulta si le realizó alguna consulta a las organizaciones de la Institución, esto por cuanto si se les ha permitido el uso del medio, eventualmente podría pensarse que con este reglamento se está haciendo una especie de persecución; esto con la intención de mejorar.

La directora Rojas Sánchez, consulta si la propuesta se dio a conocer a los podría pensarse que existe una persecución con ese tipo de publicaciones ya que la administración ha sido tolerante con este tipo de servicios; esto con el fin de mejorar. Además se podría informar

El señor Ramírez, señala que como parte de la implementación se hará una campaña de divulgación en la Institución.

Se continúa con la presentación del tema.

El director González Murillo, comenta que los reglamentos tratar de implementarse para establecer un marco, sin embargo hay dos aspectos que le preocupan aparte del marco, y es el uso desde el mismo sistema como tal. Considera que el tema no es el uso de la herramienta, sino el tiempo que se pierde utilizando la herramienta en asuntos que no competen a las funciones de trabajo. Además con el reglamento no se va a impedir que las personas no hagan uso de la herramienta, lo que habría que ver es si las sanciones están establecidas dentro del reglamento y Cómo lograr descubrir a la persona haciendo uso indebido de la herramienta. Consulta al señor Auditor Interno: Cuál va a ser la forma que la Auditoria establecerá para detectar esto?

Por otra parte considera que la forma correcta de que las personas le den el uso correcto, no es estableciendo obstáculos para el uso, porque sería una herramienta a medias. Cómo lograr que las personas tengan la cultura de usar adecuadamente la herramienta?

El señor Ramírez, señala que el reglamento en sí mismo no genera control, sin embargo se tiene la tecnología para llevar las bitácoras adecuadas para que en este caso la Auditoría Interna, analice y determine el uso que se le está dando. También el correo electrónico ejerce cierto tipo de control.

El señor Auditor Interno, indica que efectivamente la USIT, cuenta con la herramienta necesaria para determinar el uso incorrecto que se le de al uso del correo electrónico de In; incluso el año pasado se hizo un estudio cuanto al correo electrónico; sin embargo donde tiene cierta problemática en relación con algunas resoluciones o votos de la Sala Constitucional donde se determina la inviolabilidad la información, porque se puede llegar a determinar que la persona estuvo haciendo uso inadecuado de la herramienta, pero no puede entrar a ver qué fue lo que la persona estuvo haciendo.

El director Chacón Vega, menciona el sitio de un abogado e informático tico Christian Hess ***hess-cr.blogspot.com****, que lo menciona como referencia, ligado a una Asociación en Cr.* En el blogs se comenta que hay tres tendencias legislativas a nivel de técnicas jurídicas: **a)**. el delito informático son conductas actualizadas de fraudes que ya existen. **b).** la tendencia que el delito informativo es nuevo. **c)** Que en Costa Rica se están usando un modelo mixto.

También ha leído en el Financiero publicaciones de artículos que indican que cuando el empleado deja la empresa por cualquier razón, debe existir un protocolo para que saque la información personal y lo que corresponde a la empresa.

2. Por otra parte considera que no convendría aprobar el Reglamento hoy, porque hay ciertos aspectos y definiciones que podría mejorarse: por ejemplo la definición de usuario. **3.** El capítulo de las sanciones, es una simple referencia al Art. 70 del Reglamento Autónomo de Servicios, y puede ser que en la práctica esto deje espacios vacíos.

El señor Gerente General, en cuanto a las sanciones hay que recordar que las relaciones obreros patronales se regulan únicamente en el Reglamento Autónomo de Servicios; sin embargo lo que se puede hacer es retomar los que cita el Reglamento Autónomo e incluirlo en el Reglamento.

El director Chacón Vega, indica **4**. Comenta que el TSE, prohibió ingresar con celulares y cámaras; sin embargo hay un derecho que cada uno tiene y el punto es cómo implementar este tipo de medidas. **5**. Hay un sitio de UCR, Unidad de Informática Jurídica creada a mediados de los años 80, donde participa la Corte Suprema, Facultad de derecho, Procuraduría; lo menciona porque quizás podría ser un insumo para los reglamentos. Finalmente felicita la iniciativa y la propuesta ha sido interesante y quizás sería tomar la decisión de aprobar el Reglamento en una o dos semanas.

La señora Viceministra de Educación, señala que en su caso ya no tiene preocupación del Reglamento y su coherencia con las políticas, ya que la síntesis que se hizo fue muy clara y el tema está muy claro en la circular de la Contraloría.

El director González Murillo, reitera lo mencionado por don Edgar, en cuanto a que se deben establecer claramente las sanciones; además le preocupa lo que el señor Auditor menciona, como se relaciona el delito con el castigo; porque el reglamento no le permite castigar mucho.

El señor Gerente General, indica que el reglamento remite al régimen disciplinario que señala el reglamento autónomo de servicios y como tal la falta puede se sancionada ; sin embargo lo que el señor Auditor señala las dimensiones del voto de la Sala Constitucional de en qué consiste el material privado y que no, pero no el uso de los procedimientos; y en esto se debe tener cuidado, porque es normal que alguna persona tenga carpetas o información personal en la computadora, sin embargo la Sala IV, indica que en el momento de darse alguna investigación, la persona puede tener derecho a tener este tipo de información y respaldarla; no obstante diferente es hacer uso de los sistemas institucionales para fines personales.

En cuanto al Software Aranda, se señaló que en caso de que un técnico de soporte de informática tuviese que accesar una computadora para repararla a través de este software, tenía que haber un consentimiento de la persona usuaria; además si es personal la atención la persona usuaria siempre debe estar presente.

Por otra parte cada caso concreto se revisaría y se podría determinar si se violenta el voto de la sala Constitucional. Considera que esta propuesta viene a dar la posibilidad a la administración la vía para poder sancionar este tipo de uso personal a los recursos informáticos institucionales.

El director Chacón Vega, Reitera que el usuario está definido en una forma que va en contra de la Institución; porque quizás podría haber otro tipo de usuario, como por ejemplo el que viene a reparar una computadora.

El señor Ramirez, señala que el utilizar la red del INA, lo convierte en usuario.

El director Chacón Vega, se ubica en la posición de un estudiante o ciudadano interesado en accesar los recursos informáticos del INA, por ejemplo para ver como se construye un tanque séptico? y consulta: Puede un ciudadano con esa filosofía, accesar una nota técnica o en aras de la seguridad se restringe esto? En otras palabras, que la seguridad informática no sea un obstáculo para poner al alcance del ciudadano, 24 hrs, contenidos de notas técnicas en cantidad cada vez mayor, en espacios cibernéticos aislados, abiertos y especiales para solo navegar con enorme facilidad. Con lo que ha oído, cree que podría entonces aprobarse hoy este Reglamento.

El señor Cheves, indica que en este momento a nivel de acceso a la red INA, se manejan dos usuarios: los que están conectados a la Red vía cable y la modalidad usuario móvil.

El señor Gerente General, indica que para ello existe la plataformas Educativas, página WEB que tienen diferentes niveles de seguridad establecidos.

El señor Asesor Legal, comenta que en la revisión que realizaron, hicieron la observación de que el Reglamento abarcaría principalmente a funcionarios que tiene el contrato firmado y la persona que tiene un usuario creado se le abre una contraseña empieza a formar parte del sistema.

En cuanto a terceras personas, en la revisión también se le indicó a la Unidad de Informática que ellos debían de velar que este tipo situaciones se prevean en el momento de realizar los trámites de contrataciones.

El director Solano Cerdas, comenta que había leído un artículo donde se mencionaba que en una Institución inglesa, sobre la substracción de llaves mallas con información muy importante para la empresa; en ese sentido qué se haría en la Institución si eventualmente sucedería, ya sea con los empleados o usuarios externos, porque sería un nivel de inseguridad?

El señor Cheves, indica que a ese nivel podría bloquearse los puerto USB y a nivel de Red, se envía una política INA donde se bloquearían unos o todos los puertos USB.

El señor Ramirez, señala que hay diferentes usuarios a nivel de computador, por ejemplo no todos los usuarios tienen el nivel de administrador de la computadora.

El señor Presidente, indica somete a consideración de los señores directores y directoras la propuesta de Reglamento del Uso de Servicios Informáticos:

Considerando:

1.-Que mediante el oficio GG-0122-2010, del 04 de febrero de 2010, la Gerencia General, remite para conocimiento y eventual aprobación de Junta Directiva, la propuesta de Reglamento de uso de Recursos Informáticos del Instituto Nacional de Aprendizaje".

2.- Que mediante oficio GNSA-0541-2009, señor Norberto García Céspedes, remite a la Gerencia General el documento con la propuesta de Reglamento para con el propósito de que se haga del conocimiento de los señores miembros de Junta Directiva.

3.- Que la Asesoría Legal, mediante oficio AL-65-2010, remite la Propuesta de Reglamento con el criterio de legalidad respectivo.

4.- Que el presente Reglamento consta de 14 Capítulos y 35 Artículos, que fueron analizados y discutidos por los integrantes de la Junta Directiva.

5.- Que el Encargado de la Unidad de Informática y Telemática, señor Gustavo Ramirez de Peña y el técnico Randall Cheves Zamora, exponen ante los miembros de Junta Directiva la propuesta del Reglamento en cita.

6. Que en los señores directores y directoras conocen y discuten la propuesta de Reglamento, y luego de realizar las observaciones y consideraciones correspondientes manifiestan su anuencia.

7. Que de conformidad con el art. 7 inciso d, de la ley N°6868, y al haberse sometido el presente Reglamento al conocimiento de la Junta Directiva, se acuerda.

POR TANTO ACUERDAN:

1-) APROBAR EL REGLAMENTO USO DE RECURSOS INFORMATICOS DEL INSTITUTO NACIONAL DE APRENDIZAJE; DE CONFORMIDAD CON LA PROPUESTA REALIZADA MEDIANTE EL OFICIO GG-0122-2010, DEL 04 DE FEBRERO DE 2010, SUSCRITO POR GERENTE GENERAL Y EL OFICIO GNSA-0541-2009, DE LA GESTION DE NORMALIZACIÓN Y SERVICIOS DE APOYO; SEGÚN SE INDICA A CONTINUACIÓN:

REGLAMENTO USO DE RECURSOS INFORMATICOS

CAPÍTULO I:

DISPOSICIONES GENERALES

ARTICULO 1. OBJETIVO

El presente reglamento tiene como finalidad normar los aspectos tecnológicos y administrativos relacionados con el aseguramiento de la información institucional, para mantener una protección adecuada sobre los recursos informáticos del INA, abarcando la información almacenada y transmitida por medio de los recursos de las tecnologías de información y comunicaciones.

ARTICULO 2. AMBITO DE ACCION

Lo enunciado en el presente reglamento es aplicable a todos los funcionarios del INA y usuarios de los recursos informáticos. Será responsabilidad de los usuarios en general de los recursos informáticos conocer y cumplir lo aquí estipulado.

ARTICULO 3. DEFINICIONES Y NOMENCLATURA

Para el mejor entendimiento de los diferentes artículos descritos en este reglamento, se presentan las siguientes definiciones:

Acceso Remoto: Ingresar desde una computadora a un recurso ubicado físicamente en otra computadora dentro de la institución, a través de una red local o externa.

Acuerdo de confidencialidad: Es un acuerdo explícito y formal para compartir alguna información y conservar su carácter confidencial o secreto, como parte de una relación comercial o laboral.

Acuerdo de licenciamiento: Contrato entre el titular del derecho de autor (propietario) y el usuario de un programa informático (usuario final), para utilizar éste en una forma determinada y de conformidad con las condiciones convenidas.

Administrador de Recursos Informáticos (ARI): Funcionario en informática encargado de administrar los recursos informáticos tanto en USIT como en Unidades Regionales.

Antivirus: Aplicación o grupo de aplicaciones dedicadas a la prevención, búsqueda, detección y eliminación de programas malignos en sistemas informáticos.

Autenticación: Acto de establecimiento o confirmación de la identidad de un usuario como válida.

Autoridades Superiores: Comprende la Junta Directiva, Presidencia Ejecutiva, Gerencia General, Subgerencia Administrativa y Subgerencia Técnica.

Autorizaciones: Permiso explícito otorgado formalmente por parte de la jefatura de la UO.

Caracteres: Cualquier símbolo en una computadora. Pueden ser números, letras, puntuaciones, espacios, etc.

Chat: Distintas formas posibles de comunicarse en tiempo real entre dos o más personas por medio de mensajes escritos, audio y video, a través de los recursos informáticos institucionales.

Clave de usuario: Contraseña compuesta por un conjunto finito de caracteres que el usuario emplea para acceder a un servicio, sistema o programa.

Confidencialidad: Garantía que la información sea accesible sólo para aquellas personas autorizadas.

Control Remoto: Servicio que ofrecen algunas herramientas informáticas que permite dar soporte técnico a través de la red y que supone el control directo del recurso informático por parte del soportista.

Correo Electrónico: servicio de red dentro y fuera del INA que permite a los usuarios enviar y recibir mensajes rápidamente mediante sistemas de comunicación electrónicos.

Correo masivo: Envío de un mensaje a una gran cantidad de destinatarios.

Cuenta: Nombre único que identifica a cada usuario (conocido como login), se autentica mediante una contraseña (password)

Cuotas de disco: Espacio de almacenamiento en disco asignado a un usuario.

Disponibilidad de la Información: Acceso a la información y a los recursos relacionados con ella toda vez que se requiera.

Dispositivos Móviles: Tipo de equipo informático pequeño; considerado como un tipo de computador móvil.

Documento: Son documentos los escritos, los impresos, los planos, los dibujos, los cuadros, las fotografías, las fotocopias, las cintas de respaldo, los discos, las grabaciones magnetofónicas y en general, todo objeto que tenga carácter representativo o declarativo para la institución.

Documento digitalizado: Transformación o representación electrónica que se puede almacenar y acceder por medio de una computadora.

Documento electrónico: Cualquier manifestación con carácter representativo o declarativo expresamente, o transmitida por un medio electrónico o informático.

Dueño de los datos: Sujeto que puede autorizar o denegar el acceso a determinados datos, y es responsable de la integridad, disponibilidad y confidencialidad de los mismos.

Encriptación: Proceso para codificar la información a un formato más seguro.

Firewall: Elemento utilizado en redes de computadoras para controlar las comunicaciones, permitiéndolas o denegándolas.

Gestión de incidentes: Reporte, registro, atención y escalamiento de cualquier evento o situación que cause una interrupción en el servicio de la manera más rápida y eficaz posible.

Hardware: Corresponde a todos los componentes físicos (tangibles) de una computadora y sus periféricos (impresoras, teclados, enrutadores, switches, etc.).
INA: Instituto Nacional de Aprendizaje

Incidentes de Seguridad de la Información: Eventos inesperados que amenazan la seguridad de la información de una organización y comprometen las operaciones de la misma.

Integridad de la Información: Exactitud y totalidad de la información y los métodos de procesamiento.

Internet: Conjunto de servidores interconectados electrónicamente, integrado por las diferentes redes de cada país del mundo.

Intranet (red Interna): Red privada que permite acceso a información institucional que se basa en las mismas tecnologías que Internet.

Jefaturas: Funcionario de la administración activa responsable de una Unidad o Proceso, con autoridad para ordenar y tomar decisiones.

Licenciamiento: Conjunto de permisos que un desarrollador o empresa brinda para la distribución, uso y/o modificación de la aplicación que desarrolló o de la cual es propietario.

Medio de almacenamiento: Cualquier dispositivo en el cual se puede guardar información.

Módem: Dispositivo utilizado para la conexión a Internet.

Normas Técnicas para la gestión y el control de las Tecnologías de la Información: Normativa emitida por la Contraloría General de la República que establece los criterios básicos de control que deben observarse en la gestión de esas tecnologías.

Perfil: Conjunto de derechos y atribuciones que tienen los usuarios de los recursos informáticos.

Privilegio: Permiso para realizar una actividad dentro de los sistemas, equipos o servicios de la Institución.

Programas Informáticos de uso especializado: Es aquel software adquirido por el INA, para ser utilizado en aplicaciones específicas.

Protector de Pantalla: Programa que se activa cuando la computadora se encuentra inactiva por un período determinado de tiempo y muestra efectos gráficos en la pantalla, generalmente ocultando el contenido con el que se está trabajando.

Recurso informático: Cualquier equipo tecnológico (computadoras, portátiles, faxes, impresoras, fotocopiadoras, teléfonos, etc.) dentro del INA.

Registros Vitales: Cualquier registro, contrato, documento, formulario o cualquier unidad de información que no esté almacenada en la red de área local o servidor central, pero que en el momento de un desastre, puede ser necesario recrear esta información para que las áreas usuarias puedan ejecutar sus actividades en un ambiente de contingencia.

Reporte de navegación: Informe emitido mediante un sistema o herramienta que permite mostrar los sitios de Internet que un usuario ha accesado durante un periodo definido.

Respaldos: Copia de seguridad de la información en un medio de almacenamiento externo.

Rol: Conjunto de permisos que se asignan a un usuario que se autentican o accesa a un servicio, aplicación o sistema.

Seguridad de la Información: Conjunto de regulaciones, procedimientos y acciones dirigidas a preservar la confidencialidad, integridad y disponibilidad de la información institucional.

Service Desk: Gestiona eventos que causan o pueden causar una pérdida en la calidad de un servicio, mantiene proactivamente informados a los usuarios de todos los eventos relevantes con el servicio que les pudieran afectar.

Servicio de correo electrónico: Sistema de mensajería que permite enviar o recibir mensajes electrónicos, a uno o varios destinatarios.

Servicios de red: Se denominan servicios de red a aquellas utilidades, dispositivos o herramientas disponibles en la red que brindan una funcionalidad especial a los usuarios.

Servidor de respaldos: Servidor dedicado como medio de almacenamiento para respaldos de información.

Servidor de archivos: Computadora con características especiales propia del INA, dedicada exclusivamente al almacenamiento de la información de los usuarios de cada unidad organizativa.

Sesión: Período de tiempo que un usuario mantiene activa una aplicación. La sesión de usuario comienza cuando el mismo accede a la aplicación y termina cuando se cierra.

Software: Todo programa, instrucción o aplicación que se ejecuta, en el equipo informático necesario para su funcionamiento.

Solicitud de servicio: Son todas las consultas y eventos que pueden causar o no una interrupción o una reducción de la calidad del servicio y reportadas por los usuarios.

SPAM: Correo electrónico no deseado.

Spyware: Programa que recopila información de un computador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del computador.

Terceros o usuarios externos: Todas aquellas personas naturales o jurídicas, que no son funcionarios del INA pero prestan algún tipo de servicio profesional o técnico a la Institución.

Unidad Organizativa (UO): Forma en que están divididas las diferentes Unidades Técnicas y Administrativas del INA.

Unidad Técnica Especializada (UTE): Núcleos de Formación y Servicios Tecnológicos y otras Unidades de la Institución que realizan estudios técnicos especializados.

USIT: Unidad de Servicios de Informática y Telemática

Usuario o Usuario Final: Todas aquellas personas que utilicen sistemas, software, equipos informáticos y los servicios de red provistos por el INA.

UTEFOR: Unidad de Tecnología de la Formación

Virus Informático: Software que tiene la capacidad de registrar, dañar, eliminar datos, puede replicarse a sí mismo y propagarse a otros equipos.

Vulnerabilidad: Debilidad o fisura en la estructura de un sistema que lo vuelven susceptible a daños provocados por las amenazas.

CAPITULO II
USO Y SEGURIDAD DE LOS RECURSOS INFORMATICOS

ARTICULO 4: Deberes y prohibiciones de los Usuarios

Son deberes de los usuarios en el uso y seguridad de los recursos informáticos:

1. Utilizar los recursos informáticos atendiendo las disposiciones expresadas en este reglamento.
2. Hacer uso adecuado de todos los activos o recursos de Información.
3. Cumplir con los principios de la seguridad de la información: confidencialidad, integridad y disponibilidad.
4. Cumplir la política de seguridad de la información del INA.
5. Custodiar, resguardar, manipular y utilizar los recursos informáticos según lo establecido por la USIT.
6. Comportarse apegado a los más altos valores éticos y morales, a las buenas costumbres y estándares de conducta socialmente aceptados, de tal forma que no se dañe la integridad moral de un tercero, interno o externo al INA.
7. Solicitar la conexión de los equipos que se requieran en la red institucional por medio de la UO bajo el procedimiento establecido.
8. Informar de los problemas que presenten los recursos informáticos institucionales por medio del procedimiento establecido por la USIT.
9. Custodiar los programas, manuales, cables y otros dispositivos del recurso informático que le sean asignados.
10. Conservar la integridad y buen funcionamiento de los equipos que conforman la infraestructura informática.
11. Acatar todas las disposiciones dictadas por la USIT sobre uso de los recursos informáticos.

12. Apagar los equipos tecnológicos al finalizar su jornada laboral, salvo casos en los que sea estrictamente necesario que permanezcan encendidos, lo cual deberá ser justificado debidamente por la jefatura inmediata.

Son prohibiciones de los usuarios en el uso y seguridad de los recursos informáticos:
1. Utilizar la red eléctrica conectada al sistema de respaldo de energía del INA para otros fines distintos a la conexión de computadoras portátiles o de escritorio autorizados por la USIT.
2. Utilizar software en los equipos que no haya sido instalado ni autorizado por la USIT.
3. Almacenar en el equipo asignado o en el disponible en la red, archivos de cualquier tipo ajenos a los fines e intereses de la institución.
4. Descargar, instalar, implementar o hacer uso de software no autorizado y/o sin licenciamiento.
5. Guardar, distribuir materiales, fotografías, música, videos, mensajes, documentos o cualquier otro tipo de archivo que no tengan relación con sus funciones dentro del INA.
6. Utilizar los recursos informáticos de la Institución para exhibir, copiar, mover, reproducir o manipular de cualquier otra forma material de contenido que atente contra la ética, la moral o las buenas costumbres.
7. Suprimir, modificar, borrar o alterar los medios de identificación de los equipos, o entorpecer de cualquier otra forma los controles establecidos para fines de inventario.
8. Utilizar los recursos informáticos de la institución para realizar actividades personales o con fines lucrativos.
9. Utilizar los recursos informáticos para la transferencia de información que afecte los derechos de autor o propiedad intelectual.
10. Realizar acciones para dañar o alterar los recursos informáticos o la seguridad de la red.
11. Realizar modificaciones en el equipo (remover, cambiar o intercambiar los componentes internos), instalar conexiones y otros dispositivos de comunicación del INA.
12. Utilizar telefonía convencional o móvil como módem para el acceso a Internet.
13. Cambiar la configuración de los recursos informáticos establecidos por la USIT.
14. Conectar recursos informáticos a la red de computadoras, sin que su configuración sea la aprobada por la USIT.
15. Utilizar herramientas espías para la recolección de datos que puedan interferir la privacidad de los usuarios.

ARTICULO 5: Deberes de la UO
Son deberes de la UO en el en el uso y seguridad de los recursos informáticos:
1. Adquirir y custodiar los programas de uso especializado.
2. Actualizar las licencias y fiscalizar el uso de los programas especializados.
3. Supervisar los trabajos que deban ser realizados por terceros que por sus labores necesiten hacer uso de la red o recursos de la institución con equipos de su propiedad.
4. Solicitar a la USIT la revisión y autorización del recurso informático que vaya a ser utilizado por terceros, antes de tener acceso a la red o a los recursos que utilice.

ARTICULO 6: Deberes de la USIT
Son deberes de la USIT en el en el uso y seguridad de los recursos informáticos:
1. Administrar la seguridad de la información.

2. Velar por las funciones de planeación, coordinación y administración de los servicios de seguridad de la información.
3. Garantizar la seguridad en las operaciones realizadas, a través del control de procesos, normativas, reglas, políticas y estándares.
4. Asegurar una adecuada protección de los recursos informáticos, velando por la confidencialidad, integridad y disponibilidad de la información del INA.
5. Incorporar en las contrataciones de servicios informáticos a realizar con terceros, las cláusulas referentes a temas de seguridad de la información.
6. Renovar cada 6 meses, la respectiva autorización para el uso de los recursos informáticos de los terceros.
7. Dar solución pronta y efectiva a los usuarios a los problemas que suscite el uso de los recursos informáticos institucionales, la cual puede ser remota o en sitio.

ARTICULO 7: Deberes del ARI
Son deberes del ARI en el en el uso y seguridad de los recursos informáticos:
1. Verificar el estado de los equipos previa asignación a los funcionarios.
2. Informar de forma escrita a la Jefatura de la UO correspondiente, las modificaciones en el equipo, cambio de lugar, configuración, ampliación, renovación y conexión a red que presentan en la Unidad.
3. Dar a conocer a todos los usuarios, los estándares y procedimientos para el uso de recursos informáticos, de acuerdo con los lineamientos y políticas dictadas por la USIT en el cumplimiento de su deber.
4. Asesorar de forma oportuna a los usuarios acerca del uso de los recursos informáticos y la transmisión de datos.
5. Brindar el soporte técnico a los equipos, impresoras, equipos de comunicación de la institución; en un plazo no mayor a lo establecido en el catálogo de servicio.
6. Vigilar el funcionamiento y uso de la red mediante monitoreos de la plataforma de comunicaciones.
7. Instalar y desinstalar software licenciado debidamente autorizado en los servidores de la red y computadoras en general.

CAPITULO III
USO DE CONTRASEÑAS

ARTICULO 8: Deberes y prohibiciones de los Usuarios
Son deberes de los usuarios en el uso de las contraseñas:
1. Ingresar a los sistemas o equipos del INA mediante una cuenta de acceso propia.
2. Tratar todas las contraseñas como información confidencial.
3. Cambiar la contraseña que le ha sido asignada tal y como el sistema se lo solicita.
4. Velar por que su clave de usuario, sea lo más segura posible respetando los procedimientos establecidos para tal fin.
5. Velar por las acciones que se reporten y ejecuten con su contraseña.

6. Utilizar los procedimientos que establezca la USIT para solicitar cuentas de acceso a los sistemas o equipos del INA o cambios de las mismas.

Son prohibiciones de los usuarios en el uso de las contraseñas:

1. Compartir entre usuarios las contraseñas de acceso a los recursos informáticos.
2. Solicitar cuentas de acceso a los sistemas o equipos del INA o cambios de las mismas vía telefónica o correo electrónico (salvo correo electrónico firmado digitalmente).
3. Dejar contraseñas escritas en medios, lugares físicos o electrónicos donde puedan ser accesados por terceros.
4. Buscar palabras claves de otros usuarios o cualquier intento de encontrar y aprovechar agujeros en la seguridad de los sistemas informáticos del INA o del exterior, o hacer uso de programas para acceder cualquier sistema informático.

ARTICULO 9: Deberes de la USIT
Son deberes de la USIT en el uso de las contraseñas:
1. Entregar a su propietario la cuenta de acceso y clave de usuario a los sistemas o equipos del INA, utilizando mecanismos establecidos para tal fin.
2. Solicitar identificación con cédula de identidad, pasaporte vigente o carné de funcionario para hacer entrega de la clave de usuario a los sistemas o equipos del INA.
3. Suspender todas las cuentas asociadas al funcionario cuando deja de laborar para la Institución.
4. Bloquear automáticamente después de un intervalo de tiempo de inactividad definido por la USIT, toda computadora, estación de trabajo o terminal.
5. Conceder a los usuarios, acceso a los sistemas de información, previa solicitud de la UO correspondiente.

ARTICULO 10: Deberes de la URH
Son deberes de la URH en el uso de las contraseñas:
1. Comunicar inmediatamente a la USIT la finalización del contrato de un funcionario para que procedan a la eliminación de los privilegios.
2. Informar de manera inmediata a la USIT cuando un funcionario del INA está en periodo de vacaciones, incapacidad o por cualquier otro motivo se ausentara por un periodo igual o superior a 10 días hábiles, para gestionar la inhabilitación de todo acceso a los sistemas de información institucional.

ARTICULO 11: Deberes de la UO
Son deberes de la UO en el uso de las contraseñas:
1. Solicitar a la USIT el acceso a los sistemas de información que le concederá a un usuario.
2. Informar a la USIT los cambios en los privilegios otorgados a los funcionarios de su Unidad.

3. Notificar a la USIT acerca de la contratación de cualquier funcionario en su área, debiendo enviar por escrito el nombre del usuario, fecha de ingreso, descripción de trabajo e información que necesita accesar para realizar sus labores, lo último, utilizando los formularios establecidos para este fin.

ARTICULO 12: Deberes del ARI
Son deberes del ARI en el uso de las contraseñas:
1. Tramitar las solicitudes de apertura de las cuentas y cambios correspondientes a los usuarios de la Unidad, así como su eliminación o inhabilitación temporal por ausencia del funcionario.
2. Notificar a la USIT sobre cualquier cambio de perfil que se genere a un usuario, así como la razón de ese cambio.

CAPITULO IV
USO DE INTERNET

ARTICULO 13: Deberes y prohibiciones de los Usuarios
Son deberes de los usuarios en el uso de internet:
1. Utilizar en todo momento la página establecida por la USIT, como página de inicio en el navegador de Internet.
2. Justificar cuando se le solicite, el uso de INTERNET que no esté considerado conforme a este reglamento.

Son prohibiciones de los usuarios en el uso de internet:
1. Conectarse a Internet por medios no autorizados por la USIT.
2. Usar programas para descarga e intercambio de archivos (programas P2P) como Emule, BitTorrent, Kazaa, Ares, Limeware, entre otros; con el objetivo del almacenar música, películas, programas, imágenes, juegos o cualquier otra aplicación o contenido que no tengan relación con las labores del funcionario y que además perjudiquen el funcionamiento de la red y la capacidad de almacenamiento de sus computadoras.
3. Usar el servicio de Internet para realizar actividades comerciales personales y actividades que violen la ley, tales como invadir la privacidad de terceros, dañar la propiedad intelectual de otro individuo u organización.
4. Utilizar los servicios de Internet del INA para propagar intencionalmente virus o cualquier aplicación maliciosa.
5. Utilizar direcciones electrónicas de la Institución para colocar información en sitios públicos de Internet sin la previa autorización de las Autoridades Superiores, en coordinación con la USIT.
6. Ingresar a páginas de contenido pornográfico, violencia, racismo o la descarga de programas que permitan realizar conexiones automáticas o visores de sitios clasificados como pornográficos; también se prohíbe la utilización de los recursos para distribución o reproducción de este material, ya sea vía web o medios magnéticos excepto en aquellos casos en que por la naturaleza de la labor a realizar esto se requiera y sea aprobado por las Autoridades Superiores de forma explícita.

7. Navegar en Internet desde un equipo que no reúna las condiciones de configuración y seguridad definidas por la USIT.

ARTICULO 14: Deberes de la USIT
Son deberes de la USIT en el uso de internet:
1. Registrar en bitácora todo sitio accesado y emitir reportes de navegación.

2. Inhabilitar el servicio de Internet cuando por razones de seguridad, oportunidad y conveniencia del INA, así se disponga.
3. Implementar dispositivos o mecanismos para identificar, administrar, controlar y monitorear la utilización del servicio de Internet.
4. Revisar el historial de uso y acceso del servicio de un usuario que esté haciendo mal uso del servicio de Internet, así como cancelar el servicio.

CAPITULO V
USO DEL SERVICIO DE CORREO ELECTRÓNICO

ARTICULO 15: Deberes y prohibiciones de los Usuarios
Son deberes de los usuarios en el servicio de correo electrónico:

1. Hacer un uso responsable y adecuado del servicio de correo electrónico, en el contexto estricto de las actividades laborales asignadas por la Institución.

2. Revisar su cuenta de correo electrónico frecuentemente, de tal forma que descargue todos aquellos mensajes almacenados en el servidor a su computador; manteniendo con ello el espacio disponible en su cuenta de correo.

3. Indicar en todo correo electrónico que sea enviado a través del Sistema de Correo Electrónico del INA, un asunto o “subject” claro y relacionado con el contenido del mensaje, caso contrario podrá ser eliminado o ignorado.

4. Incluir una firma automatizada en todo correo electrónico que sea enviado desde el Sistema de Correo Electrónico del INA, configurada en cada cliente de correo electrónico, en la cual se destaquen únicamente los datos del remitente en el siguiente orden: -Nombre completo del usuario. -Unidad, Proceso o Núcleo, para el cual trabaja. -Correo electrónico del funcionario o usuario. -Número de teléfono o teléfonos de contacto del funcionario o usuario. -Aviso de confidencialidad.

5. Reportar inmediatamente, a su jefe o a la USIT, cualquier situación que pueda comprometer la seguridad y buen funcionamiento del servicio del correo electrónico.

6. Velar por la administración de los mensajes descargados en un computador portátil o de escritorio.

Son prohibiciones de los usuarios en el servicio de correo electrónico:

1. Utilizar algún tipo de fondo que no sea el autorizado o definido por la USIT para el envío de correos electrónicos.

2. Abrir correos de dudosa procedencia, los cuales no han sido solicitados explícitamente, o que provengan de un remitente desconocido. Tampoco aquellos que no tengan un asunto o “Subject” específico, o que en su interior contengan un archivo adjunto no solicitado con una extensión considerada como peligrosa, por ejemplo: .com, .exe, .src, .bat, .cpl, .hta, .vbs, .cmd, .pif, .bmp, .gif; .hlp. El correo debe ser eliminado en caso de existir duda.

3. Enviar copias no autorizadas de programas informáticos.

4. Utilizar claves o cuentas de correo de otros usuarios.

5. Permitir a otros usuarios utilizar cuenta de correo institucional.

6. Dejar sesiones abiertas sin control alguno.

7. Ver, copiar, alterar o destruir el contenido del correo de otra persona sin el consentimiento explícito del dueño de la cuenta de correo.

8. Utilizar los recursos del servicio de correo electrónico del INA para actividades o el envío de cualquier tipo de cadenas de mensajes, así como la distribución de este tipo de información; además del envío de correo tipo “SPAM”, es decir “correo basura no solicitado”

9. Enviar correos masivos a todas aquellas personas que no estén explícitamente autorizados para dicha labor. Se podrá hacer uso de este recurso salvo autorización explícita de las autoridades superiores.

10. Difundir correos electrónicos sin identificar plenamente el (los) autor(es) o enviar anónimos que atenten contra esta Institución.

11. Enviar mensajes alterando la dirección electrónica del remitente para suplantar a terceros; identificarse como una persona ficticia o simplemente no identificarse.

12. Violentar las medidas de seguridad que soportan el entorno del servicio de correo electrónico.

ARTICULO 16: Deberes de la USIT
Son deberes de la USIT en el servicio de correo electrónico:

1. Crear a cada cuenta de correo una clave de usuario o contraseña para acceder al contenido de la misma.

2. Administrará la capacidad de almacenamiento de correo para cada usuario.

3. Instalar a cada cliente de correo electrónico una firma automatizada, en la cual se destaquen únicamente los datos del remitente en el siguiente orden: -Nombre completo del usuario. -Unidad, Proceso o Núcleo, para el cual trabaja. -Correo electrónico del

funcionario o usuario. -Número de teléfono o teléfonos de contacto del funcionario o usuario. -Aviso de confidencialidad.

4. Elaborar el aviso de confidencialidad.

CAPITULO VI
CONTROL DE VIRUS Y SOFTWARE MALICIOSO

ARTICULO 17: Deberes y prohibiciones de los Usuarios
Son deberes de los usuarios en el control de virus y software malicioso:
1. Velar por el correcto funcionamiento de la herramienta antivirus y reportarlo a la USIT cuando se encuentra deshabilitado.
2. Seguir un proceso de verificación de virus antes de proceder a la lectura de la información obtenida de fuentes externas en cualquier medio de almacenamiento (discos flexibles, CD´s, DVD´s, Cintas o cualquier otro similar.) o correo electrónico.

3. Reportar inmediatamente a la USIT por el medio establecido, cuando detecte una alerta en su antivirus, reciba un correo con un anexo dudoso, sospeche de una infección o note un comportamiento anormal en su computadora (bloqueo, lentitud inusual, reinicio inesperado cada cierto tiempo).
4. Retirar los dispositivos USB, disquetes o discos de la unidad respectiva antes de iniciar o apagar su computadora.

Son prohibiciones de los usuarios en el control de virus y software malicioso:
1. Se prohíbe deshabilitar el software de antivirus, o alterar la configuración del mismo.
2. Abrir mensajes o solicitudes provenientes desde Internet, que impliquen instalar software malicioso en sus equipos; esto con el objetivo de prevenir el contagio y propagación de virus.
3. Utilizar directorios, carpetas o unidades de disco compartidos. Si su uso es necesario debe estar autorizado por la Jefatura de la UO correspondiente y además estar claramente definidos los permisos de seguridad sobre lo que se comparte.
4. Modificar la frecuencia del escaneo automático del software.

ARTICULO 18: Deberes de la UO
Son deberes de la UO en el control de virus y software malicioso:
1. Solicitar a la USIT la autorización de la herramienta de antivirus perteneciente a un tercero que requiera realizar algún tipo de labor en los recursos informáticos.
2. Autorizar a los usuarios a utilizar directorios, carpetas o unidades de disco compartido y definir los permisos de seguridad sobre lo que se comparte.

ARTICULO 19: Deberes de la USIT
Son deberes de la USIT en el control de virus y software malicioso:
1. Velar por que todo equipo de cómputo propiedad de la Institución cuente con el software oficial de antivirus del INA, el cual debe ser actualizado de forma periódica.

2. Habilitar o deshabilitar los servicios relacionados con el software de antivirus o aplicaciones instaladas para combatir el software malicioso, tanto a nivel de servidor como de los demás dispositivos.

ARTICULO 20: Deberes del ARI
Son deberes del ARI en el control de virus y software malicioso:
1. Desconectar o aislar de la red las computadoras infectadas con virus u otras formas de código malicioso para prevenir la propagación viral a otros dispositivos o evitar efectos perjudiciales, hasta que se haya eliminado la infección.
2. Notificar, al momento de detectar cualquier anomalía de seguridad detectada, a la USIT y la UO correspondiente.
3. Comunicar los cambios realizados en las políticas, estándares, configuración y mantenimiento de equipos para mantener la seguridad informática.

CAPITULO VII
ESCRITORIO Y PANTALLA LIMPIA

ARTICULO 21: Deberes y prohibiciones de los Usuarios

Son deberes del usuario en el uso del escritorio y pantalla limpia:
1. Ingresar el usuario y contraseña para desbloquear el protector de pantalla.
2. Utilizar en todo momento el fondo de pantalla institucional autorizado por la USIT.
3. Guardar en gabinetes seguros toda la información institucional, contenida en medios de almacenamiento extraíbles y externos, no quedando desatendidos en ningún momento, en los escritorios de los funcionarios.
4. Bloquear o proteger con el protector de pantalla autorizado por la USIT, las computadoras cuando están desatendidas, para evitar el acceso no autorizado.

Son prohibiciones del usuario en el uso del escritorio y pantalla limpia:
1. Desactivar o modificar la configuración del protector de pantalla establecido por la USIT.
2. Cambiar el fondo de pantalla institucional autorizado por la USIT.
3. Desplegar en los monitores de las computadoras información institucional a la vista de otras personas, que no sean las autorizadas para tener acceso a esa información.

CAPITULO VIII
PRIVACIDAD Y PROTECCIÓN DE LA INFORMACIÓN

ARTICULO 22: Deberes y prohibiciones de los Usuarios
Son deberes del usuario para resguardar la privacidad y protección de la información
1. Firmar un contrato de confidencialidad de conformidad a lo que establece la Política de Seguridad de la Información.
2. Ingresar o extraer de las bases de datos del INA, a través de los procedimientos establecidos para tal fin, los cuales deben contar con los mecanismos de seguridad adecuados.

3. Utilizar la información del INA de acuerdo con los derechos que se les asignen de conformidad con sus funciones, así como conocer y cumplir las regulaciones en materia de seguridad de la información.

Son prohibiciones del usuario en la privacidad y protección de la información
1. Publicar, reproducir, trasladar ni ceder información sin autorización del INA.
2. Crear, usar y/o almacenar programas de información que pudiesen ser utilizados para atacar a los sistemas informáticos del INA o del exterior.
3. Alterar la integridad, uso o manipulación indebida de los datos o de la información.

ARTICULO 23: Deberes del ARI
Es deber del ARI guardar la debida confidencialidad, cuando por razones de trabajo se tenga acceso incidental a información no autorizada por los usuarios.

CAPITULO IX
SEGURIDAD FÍSICA Y AMBIENTAL

ARTICULO 24: Deberes y prohibiciones de los Usuarios
Son deberes del usuario para garantizar la seguridad física y ambiental:

1. Velar por el uso adecuado de los dispositivos de seguridad que se han implementado en las distintas áreas.

Son prohibiciones del usuario para garantizar la seguridad física y ambiental:
1. Ingreso de personas no autorizadas a las áreas restringidas.
2. Almacenar en los cuartos de servidores y telecomunicaciones, cualquier material, herramientas o equipos que no sean para este fin.
3. El ingreso o salida de un funcionario a cualquier área, utilizando el carné o credenciales de otro funcionario.
4. Dañar o sustraer cualquier elemento físico de la instalación informática o de la infraestructura.
5. Trasladar a otras dependencias, sin la debida autorización, cualquier elemento físico de la instalación informática o de la infraestructura.

ARTICULO 25: Deberes de la UO
Son deberes de la UO para garantizar la seguridad física y ambiental:
1. Identificar las áreas restringidas y establecer los controles de acceso necesarios.
2. Dotar y mantener las condiciones ambientales necesarias para la correcta operatividad de los recursos informáticos.
3. Velar que todo funcionario o terceros que prestan servicios profesionales y técnicos al INA porten una identificación en un lugar visible.
4. Escoltar a la visita, desde el ingreso hasta la salida de la UO correspondiente.

ARTICULO 26: Deberes del ARI
Son deberes del ARI para garantizar la seguridad física y ambiental:
1. Notificar, al momento de detectar cualquier anomalía de seguridad detectada, a la USIT y la UO correspondiente.
2. Comunicar los cambios realizados en las políticas, estándares, configuración y mantenimiento de equipos para mantener la seguridad informática.
3. Indicar a la USIT, sobre remodelaciones en el área física que alteren la disposición del cableado de la red de datos.

CAPITULO X
RESPALDOS Y RECUPERACIÓN

ARTICULO 27: Deberes de los Usuarios
Son deberes del usuario en el respaldo y recuperación de la información:
1. Almacenar la información de carácter institucional incluyendo los registros vitales en una localidad definida, de acuerdo al procedimiento establecido para estos fines.
2. Realizar los debidos respaldos de la información contenida en sus computadoras.

ARTICULO 28: Deberes del ARI

Es deber del ARI instruir a solicitud de los usuarios, acerca de la elaboración y recuperación de respaldos.

CAPITULO XI
MANIPULACIÓN Y DESTRUCCIÓN DE DATOS

ARTICULO 29: Deberes y prohibiciones de los Usuarios

Son deberes del usuario en la manipulación y destrucción de datos

1. Eliminar los documentos textuales, electrónicos y digitalizados en una forma precisa y transformada en material no legible, ya sea utilizando una destructora de papel de corte cruzado, desmagnetización o incineración, de tal forma que la información no pueda ser obtenida por personal interno o terceras partes.
2. Eliminar de su computadora y de la papelera de reciclaje el desecho de documentos electrónicos y digitalizados que tengan carácter representativo para el INA.

Son prohibiciones del usuario en la manipulación y destrucción de datos

1. Eliminar documentos institucionales por medios tradicionales o almacenarlos para reciclaje.
2. Usar o distribuir información institucional para fines ilícitos (propios o para terceros).

CAPITULO XII
DE LAS SOLICITUDES DE SERVICIO.

ARTICULO 30: Deberes de los Usuarios

Son deberes del usuario en las solicitudes de servicio

1. Realizar las solicitudes de servicios a través del procedimiento establecido por la USIT.
2. Autorizar la atención a la solicitud de servicio vía control remoto para que este sea ejecutado por el ARI.
3. Permitir la revisión del equipo asignado por parte del ARI respectivo, ya sea por control remoto o de forma presencial.
4. Estar presente cuando reciba soporte técnico presencial o remoto, para garantizar la privacidad, confidencialidad e integridad de su información.
5. Calificar a través del Service Desk, la atención a la solicitud de servicio una vez finalizado.

ARTICULO 31: Prohibiciones del ARI

Son prohibiciones del ARI en las solicitudes de servicio

1. Accesar de forma remota sin previa autorización del usuario.
2. Accesar a información confidencial sin previa autorización del usuario.

CAPITULO XIII
RÉGIMEN DISCIPLINARIO

El presente reglamento se encuentra alineado con las leyes vigentes de la república de Costa Rica, sancionará a todo aquel usuario que incumpla lo dispuesto en este Reglamento. Las sanciones serán impuestas según las disposiciones contenidas en el artículo 70 y siguientes del Reglamento Autónomo de Servicios del INA

ARTÍCULO 32. FALTAS LEVES
Se considera falta leve el incumplimiento a cualquier obligación, deber y/o responsabilidad dispuesta en el presente reglamento. El incumplimiento de los puntos establecidos en los siguientes artículos e incisos; se le aplicará lo estipulado en el artículo 48 del Reglamento Autónomo de Servicios del Instituto Nacional de Aprendizaje.

- **Artículo 4**

Son prohibiciones de los usuarios en el uso y seguridad de los recursos informáticos:

1. Utilizar la red eléctrica conectada al sistema de respaldo de energía del INA para otros fines distintos a la conexión de computadoras portátiles o de escritorio autorizados por la USIT.
2. Utilizar los recursos informáticos para la transferencia de información que afecte los derechos de autor o propiedad intelectual.
3. Realizar modificaciones en el equipo (remover, cambiar o intercambiar los componentes internos), instalar conexiones y otros dispositivos de comunicación del INA.
4. Utilizar telefonía convencional o móvil como módem para el acceso a Internet.
5. Cambiar la configuración de los recursos informáticos establecidos por la USIT.

- **Artículo 13**

Son prohibiciones de los usuarios en el uso de internet:

1. Utilizar direcciones electrónicas de la Institución para colocar información en sitios públicos de Internet sin la previa autorización de las Autoridades Superiores, en coordinación con la USIT.

- **Artículo 15**

Son prohibiciones de los usuarios en el servicio de correo electrónico:

1. Utilizar algún tipo de fondo que no sea el autorizado o definido por la USIT para el envío de correos electrónicos.
2. Abrir correos de dudosa procedencia, los cuales no han sido solicitados explícitamente, o que provengan de un remitente desconocido. Tampoco aquellos que no tengan un asunto o “Subject” específico, o que en suinterior contengan un archivo adjunto no solicitado con una extensión considerada como peligrosa, por ejemplo: .com, .exe, .src, .bat, .cpl, .hta,

.vbs, .cmd, .pif, .bmp, .gif; .hlp. El correo debe ser eliminado en caso de existir duda.

3. Utilizar los recursos del servicio de correo electrónico del INA para actividades o el envío de cualquier tipo de cadenas de mensajes, así como la distribución de este tipo de información; además del envío de correo tipo “SPAM”, es decir “correo basura no solicitado”
4. Enviar correos masivos a todas aquellas personas que no estén explícitamente autorizados para dicha labor. Se podrá hacer uso de este recurso salvo autorización explícita de las autoridades superiores.

- **Artículo 17**

Son prohibiciones de los usuarios en el control de virus y software malicioso:

1. Abrir mensajes o solicitudes provenientes desde Internet, que impliquen instalar software malicioso en sus equipos; esto con el objetivo de prevenir el contagio y propagación de virus.
2. Utilizar directorios, carpetas o unidades de disco compartidos. Si su uso es necesario debe estar autorizado por la Jefatura de la UO correspondiente y además estar claramente definidos los permisos de seguridad sobre lo que se comparte.
3. Modificar la frecuencia del escaneo automático del software de antivirus.

- **Artículo 21**

Son prohibiciones del usuario en el uso del escritorio y pantalla limpia:

1. Desactivar o modificar la configuración del protector de pantalla establecido por la USIT.
2. Cambiar el fondo de pantalla institucional autorizado por la USIT.
3. Desplegar en los monitores de las computadoras información institucional a la vista de otras personas, que no sean las autorizadas para tener acceso a esa información.

- **Artículo 22**

Son prohibiciones del usuario en la privacidad y protección de la información

1. Publicar, reproducir, trasladar ni ceder información sin autorización del INA.

- **Artículo 24**

Son prohibiciones del usuario para garantizar la seguridad física y ambiental:

1. El ingreso o salida de un funcionario a cualquier área, utilizando el carné o credenciales de otro funcionario.

- **Artículo 29**

Son prohibiciones del usuario en la manipulación y destrucción de datos

1. Eliminar documentos institucionales por medios tradicionales o almacenarlos para reciclaje.

ARTÍCULO 33. FALTAS GRAVES

Se considera faltas graves el incumplimiento de los siguientes puntos y se le aplicará lo estipulado en el artículo 49 del Reglamento Autónomo de Servicios del Instituto Nacional de Aprendizaje.

- **Artículo 4**

Son prohibiciones de los usuarios en el uso y seguridad de los recursos informáticos:

1. Utilizar software en los equipos que no haya sido instalado ni autorizado por la USIT.
2. Almacenar en el equipo asignado o en el disponible en la red, archivos de cualquier tipo ajenos a los fines e intereses de la institución.
3. Descargar, instalar, implementar o hacer uso de software no autorizado y/o sin licenciamiento.
4. Guardar, distribuir materiales, fotografías, música, videos, mensajes, documentos o cualquier otro tipo de archivo que no tengan relación con sus funciones dentro del INA.
5. Utilizar los recursos informáticos de la Institución para exhibir, copiar, mover, reproducir o manipular de cualquier otra forma material de contenido que atente contra la ética, la moral o las buenas costumbres.
6. Suprimir, modificar, borrar o alterar los medios de identificación de los equipos, o entorpecer de cualquier otra forma los controles establecidos para fines de inventario.
7. Utilizar los recursos informáticos de la institución para realizar actividades personales o con fines lucrativos.
8. Realizar acciones para dañar o alterar los recursos informáticos o la seguridad de la red.
9. Conectar recursos informáticos a la red de computadoras, sin que su configuración sea la aprobada por la USIT.
10. Utilizar herramientas espías para la recolección de datos que puedan interferir la privacidad de los usuarios.

- **Artículo 8**

Son prohibiciones de los usuarios en el uso de las contraseñas:

1. Compartir entre usuarios las contraseñas de acceso a los recursos informáticos.
2. Solicitar cuentas de acceso a los sistemas o equipos del INA o cambios de las mismas vía telefónica o correo electrónico (salvo correo electrónico firmado digitalmente).
3. Dejar contraseñas escritas en medios, lugares físicos o electrónicos donde puedan ser accesados por terceros.
4. Buscar palabras claves de otros usuarios o cualquier intento de encontrar y aprovechar agujeros en la seguridad de los sistemas informáticos del INA o del exterior, o hacer uso de programas para acceder cualquier sistema informático.

- **Artículo 13**

Son prohibiciones de los usuarios en el uso de internet:

1. Conectarse a Internet por medios no autorizados por la USIT.
2. Usar programas para descarga e intercambio de archivos (programas P2P) como Emule, BitTorrent, Kazaa, Ares, Limeware, entre otros; con el objetivo del almacenar música, películas, programas, imágenes, juegos o cualquier otra aplicación o contenido que no tengan relación con las labores del funcionario y que además perjudiquen el funcionamiento de la red y la capacidad de almacenamiento de sus computadoras.
3. Usar el servicio de Internet para realizar actividades comerciales personales y actividades que violen la ley, tales como invadir la privacidad de terceros, dañar la propiedad intelectual de otro individuo u organización.
4. Utilizar los servicios de Internet del INA para propagar intencionalmente virus o cualquier aplicación maliciosa.
5. Ingresar a páginas de contenido pornográfico, violencia, racismo o la descarga de programas que permitan realizar conexiones automáticas o visores de sitios clasificados como pornográficos; también se prohíbe la utilización de los recursos para distribución o reproducción de este material, ya sea vía web o medios magnéticos excepto en aquellos casos en que por la naturaleza de la labor a realizar esto se requiera y sea aprobado por las Autoridades Superiores de forma explícita.
6. Navegar en Internet desde un equipo que no reúna las condiciones de configuración y seguridad definidas por la USIT.

- **Artículo 15**

Son prohibiciones de los usuarios en el servicio de correo electrónico:

1. Enviar copias no autorizadas de programas informáticos.
2. Utilizar claves o cuentas de correo de otros usuarios.
3. Permitir a otros usuarios utilizar cuenta de correo institucional.
4. Dejar sesiones abiertas sin control alguno.
5. Ver, copiar, alterar o destruir el contenido del correo de otra persona sin el consentimiento explícito del dueño de la cuenta de correo.
6. Difundir correos electrónicos sin identificar plenamente el (los) autor(es) o enviar anónimos que atenten contra esta Institución.
7. Enviar mensajes alterando la dirección electrónica del remitente para suplantar a terceros; identificarse como una persona ficticia o simplemente no identificarse.
8. Violentar las medidas de seguridad que soportan el entorno del servicio de correo electrónico.

- **Artículo 17**

Son prohibiciones de los usuarios en el control de virus y software malicioso:

1. Se prohíbe deshabilitar el software de antivirus, o alterar la configuración del mismo.

- **Artículo 22**

Son prohibiciones del usuario en la privacidad y protección de la información

1. Crear, usar y/o almacenar programas de información que pudiesen ser utilizados para atacar a los sistemas informáticos del INA o del exterior.
2. Alterar la integridad, uso o manipulación indebida de los datos o de la información.

- **Artículo 24**

Son prohibiciones del usuario para garantizar la seguridad física y ambiental:

1. Ingreso de personas no autorizadas a las áreas restringidas.
2. Almacenar en los cuartos de servidores y telecomunicaciones, cualquier material, herramientas o equipos que no sean para este fin.
3. Dañar o sustraer cualquier elemento físico de la instalación informática o de la infraestructura.
4. Trasladar a otras dependencias, sin la debida autorización, cualquier elemento físico de la instalación informática o de la infraestructura.

- **Artículo 29**

Son prohibiciones del usuario en la manipulación y destrucción de datos

1. Usar o distribuir información institucional para fines ilícitos (propios o para terceros).

- **Artículo 31**

Son prohibiciones del ARI en las solicitudes de servicio

1. Accesar de forma remota sin previa autorización del usuario.
2. Accesar a información confidencial sin previa autorización del usuario.

CAPITULO XIV:
DISPOSICIONES FINALES

ARTÍCULO 34: VIGENCIA.

Este Reglamento rige a partir del día hábil siguiente a su publicación en el diario oficial La Gaceta.

ARTÍCULO 35: TRANSITORIO

La USIT deberá en un plazo no mayor a dos meses posteriores a su publicación adaptar los procedimientos de su competencia con relación a este documento.

ACUERDO FIRME POR UNANIMIDAD. N°018-2009

ARTICULO SETIMO

Informes de Dirección

Derogatoria de Vacaciones para el señor Presidente:

El señor Presidente, informa que por asuntos que se presentaron en último momento no podrá tomar las vacaciones programadas del 16 al 19 febrero.

Se retira de la sesión el señor Vicepresidente.

ARTICULO OCTAVO

Mociones y Varios

Mociones.

No hay mociones.

Varios

1. Publicación en el Financiero sobre.

El director Monge Rojas, hace referencia a una nota del Financiero de hoy, en cual se pública una nota sobre: "Contraloría critica debilidad a las compras públicas en la mayoría de la Instituciones Públicas"; comenta que en la nota hay un cuadro donde mencionas Instituciones que son los mayores compradores, pero no aparece el INA; sin embargo no está demás considerar que la Contraloría está detectando este tipo de fallas en la entidades públicas.

Comenta esto para que la Institución esté alerta a las compras. Considera que es un esfuerzo grande y merece darle la publicidad.

2.Nota de opinión publicada en la Nación por el señor Alexander Mora, sobre "Delicuencia y Desempleo".

El director Monge Rojas, comenta sobre la nota de opinión publicada en la Nación, en el tema de Informes del Estado de la Nación en materia de Educación y de la importancia de la Formación Técnica Profesional. Menciona el tema porque seria importante que se evaluará, sobre todo en el momento de transición que está viviendo el país; además tenerlo como alerta para la Institución.

La directora Rojas Sánchez, comenta la publicación de hoy en la Extra y la Teja, da respuesta a la apertura de la oferta de capacitación de la Institución, en las diferentes Regiones, por lo que invita a que se vea la publicación.

Por otra parte agradece la recomendación del director Monge Rojas, sin embargo considera en su caso personal que las publicaciones del estado de la Nación, perdieron respeto ya que perdió la confianza que tenía en este tipo publicación.

También felicita a la administración por la publicación sobre la promoción de los servicios de capacitación que salió hoy en los medios de comunicación.

El señor Gerente General, menciona que en una de las primeras sesiones de este año, un funcionario del Núcleo Comercio y Servicio, expuso la validación de la oferta formativa que se había realizado con la Cámara Costarricense de Tecnologías de Información y comunicación, donde había dos nuevos programas y que estaban por empezar en el mes de julio.

El director Monge Rojas, señala que precisamente por el conocimiento que tiene sobre los convenios con CANTIC y otras Cámaras, consideró importante traer la publicación. Además como bien cita el señor Gerente, la Junta Directiva, conoce en qué se va a invertir el superávit, sin embargo a veces es importante divulgar lo que la Institución hace y no solo a nivel de oferta formativas, sino en temas de ciertas políticas internas.

Felicitación por la herramienta del Sistema Intermediación de Empleo, via WEB.

El director Monge Rojas, felicita y agradece por el Sistema de Empleo, vía WEB, considera que es un esfuerzo grande y merece que se divulgue.

Sobre la importancia realizar visitas a los Centro Formación del INA.

La directora Rojas Sánchez, solicita al señor Auditor Interno, que realicen visitas a los diferentes Centros de Formación del INA, ya que considera que no pueden hacer

informes de auditoría desde un escritorio, porque primero debe conocerse cuales son las condiciones y limitaciones de las personas.

Sobre el tema utilización del superávit institucional.

El señor Gerente General; comenta que hace unas semanas se hizo una presentación en el tema de superávit y lo significa realmente recursos ociosos, en el entendido de que ya no existen porque son recursos ligados a proyectos de equipamiento o infraestructura próximos a definir por la Junta Directiva.

Sin más asuntos por tratar se cierra la sesión a las diecinueve horas y cuarenta y cinco minutos del mismo día y lugar.