ACTA SESION ORDINARIA 4629

Acta de la Sesión Ordinaria número cuatro mil seiscientos veintinueve celebrada por la Junta Directiva del Instituto Nacional de Aprendizaje, en el Edificio de Comercio y Servicios en el Paseo Colón, a las diecisiete horas del once de junio del dos mil catorce, con la asistencia de los siguientes Directores: Sr. Minor Rodríguez Rodríguez, Presidente Ejecutivo; Sr. Carlos Lizama Hernández, Vicepresidente; Sr. Tyronne Esna Montero; Pbro. Claudio María Solano Cerdas; Sr. Jorge Muñoz Araya; Sr. Luis Fernando Monge Rojas; Sr. Carlos Humberto Montero Jiménez; señor Miguel Ángel Gutiérrez Rodríguez, Viceministro de Educación. Ausente el señor Víctor Manuel Mora Morales, Ministro de Trabajo y Seguridad Social, por motivos laborales. Por la Administración: señor José Antonio Li Piñar, Gerente General, señora Ileana Leandro Gómez, Subgerente Administrativa, Sr. Roberto Mora Rodríguez, Subgerente Técnico. Por la Auditoría Interna, Sra. Rita Mora Bustamante, Auditora Interna. Por la Asesoría Legal, Sr. Ricardo Arroyo Yannarella. Por la Secretaría Técnica: Sr. Bernardo Benavides Benavides, Secretario Técnico de Junta Directiva.

ARTÍCULO PRIMERO:

Presentación del Orden del Día

El señor Presidente, somete a consideración de la Junta Directiva el Orden del Día, e indica que desea agregar un espacio posterior a la Reflexión para la

presentación del señor Viceministro Miguel Ángel Gutiérrez Rodríguez y del señor Carlos Montero, quienes se integran el día de hoy a esta Junta Directiva.

El señor Director Muñoz Araya, indica que envió un correo proponiendo el tema del Sistema de Banca para el Desarrollo, dado que se acordó en la Asamblea Legislativa, pedir la consulta al INA y a otras instituciones más, por lo que desea saber si se tendría tiempo para verlo el próximo lunes.

Asimismo, solicita al señor Asesor Legal, que le indique si la Asesoría ya tiene un dictamen sobre lo último que se analizó en el Proyecto Banca para el Desarrollo, porque si el tiempo que tienen está ajustado, debería de verse el tema hoy.

Sin embargo, si se contara con más tiempo, se podría hacer la próxima semana y que la Asesoría Legal y la Gerencia General envíen los argumentos o los comentarios con respecto a la nueva Ley de Banca para el Desarrollo.

Menciona que en el correo, comentaba que el señor Francisco Marín, expresidente Ejecutivo, dijo que iba a dar la mayor prioridad porque había que monitorear desde la Asamblea Legislativa, lo que estaba pasando con este Proyecto, por lo que entiende que ya tiene que haber avances sobre el criterio del INA, dado que afecta a la Institución, porque hay un 15% que el INA aporta para Banca para el Desarrollo.

El señor Asesor Legal, indica que efectivamente desea aclarar, ya que ha sido motivo de duda en la Junta Directiva, en el sentido de que el tema había pasado a conocimiento del Plenario de la Asamblea Legislativa, sin haber dado la audiencia al Instituto Nacional de Aprendizaje y efectivamente la Sala Constitucional en la consulta previa, lo devolvió para que se hicieran esas consultas.

En ese aspecto, debe informar que la consulta ingresó a la Institución, específicamente al señor Presidente Ejecutivo, el lunes anterior, por lo que ya en la Asesoría Legal, solicitaron el criterio técnico a la Gerencia General, para lo cual dieron tres días, porque les dieron ocho día hábiles para cumplir con el tema.

Señala que el plazo vence el 19 de junio, por lo que le dieron 3 días a la Gerencia General y a PYMES, para que elaboraran el criterio técnico. El texto lo remitirá vía correo electrónico a los señores Directores, el documento viene a colores, con todas las mociones que fueron agregadas por parte de los señores Diputados, en la discusión que se hizo en el Plenario.

Por lo anterior, la meta es que entre lunes y martes, la Asesoría Legal lo trabajaría, y tiene entendido extraoficialmente, porque depende de la Junta Directiva, que se va a hacer una Sesión Extraordinaria la próxima semana, por lo que la idea es verlo ese día y estar contestando en tiempo el día jueves.

Agrega que también le elaboró al señor Presidente, una nota para eventualmente solicitar una prórroga, lo que usualmente se estila por motivo de que la Junta Directiva se reúne una vez a la semana y a veces los plazos no coinciden. La

prórroga que se solicitaría es de diez días hábiles más, mientras la Junta Directiva ve el tema. La Asesoría Legal, tendría el dictamen para el próximo martes, una vez que cuenten con los insumos de la Gerencia General.

El señor Director Muñoz Araya, señala que entonces estarían en tiempo para que la Junta Directiva pueda aprobar el informe.

El señor Asesor Legal, responde que sí.

El señor Director Muñoz Araya, solicita al señor Asesor Legal, que se ponga atención en aquellos puntos, en que el Consejo Rector pueda estar atribuyéndose algunos aspectos, en donde está sobre esta Junta Directiva, por lo que organizativamente podría haber alguna violación a la Ley del INA.

El señor Presidente, indica que aclarado el asunto, el tema de Banca para el Desarrollo, con el informe de la Asesoría Legal, estaría viéndose en la próxima Sesión.

Asimismo, estaría solicitando que el punto 10 de la Asesoría Legal, sobre el Proyecto de Formación Dual, se pueda ver en la próxima sesión, dado que se tiene programado para el día de mañana, una reunión con el Diputado Javier Cambronero, que es quien preside la Comisión de Ciencia y Tecnología, que es la que lleva este Proyecto, por lo que es conveniente ver con el señor Diputado, los detalles para luego analizarlo en Junta Directiva.

El señor Director Esna Montero, indica que le parece bien el hecho de que mañana se tenga la reunión, sin embargo, le gustaría saber cuál es la posición que se va a llevar como Institución, y tal y como lo han conversado anteriormente, este es un proyecto que no pasó por Junta Directiva y que llevó otra clase de formalidad, y como miembro de esta Junta Directiva, no está de acuerdo con eso.

Reitera que es importante saber qué es lo que se le va a plantear institucionalmente al señor Diputado, para saber qué es lo que van a apoyar como Junta Directiva.

Asimismo, estuvo leyendo lo que les remitió el señor Asesor Legal, sobre Educación Dual y cree que es importante mencionar que en el documento dice algunas cosas textuales que sería importante que se puedan analizar en el seno de esta Junta Directiva, porque es un proyecto sumamente importante, y como Órgano Colegiado han estado detrás de este tema y no ha seguido el camino que debió seguir.

El señor Presidente, indica que efectivamente se ha estado revisando y hay algunos detalles que son de revisión, pero hasta que se reúnan con el señor Diputado, podrían ver si la percepción institucional es la correcta. En ese aspecto, lo único que estarían haciendo es quitándolo del Orden del Día, para verlo con más detenimiento en la próxima sesión.

Asimismo, conociendo los criterios de las Fracciones y en este caso la del Partido Acción Ciudadana, que es el señor Javier Cambronero, esto les daría un poco más de tiempo.

El señor Director Solano Cerdas, indica que en este tema, le gustaría que les traigan la ruta crítica, para saber el camino que lleva el Proyecto.

El señor Presidente, menciona que ese aspecto también lo han pensado, es decir, el hacer un cronograma de seguimiento o ruta crítica, a efecto de ver qué es lo resta de camino en este Proyecto.

Comenta que resumiendo las modificaciones al Orden del Día, se estaría agregando la presentación de los nuevos miembros de Junta Directiva y la eliminación del punto 10.

Se aprueba el Orden del Día de la siguiente manera:

1. Presentación del Orden del Día.
2. Reflexión.
3. Discusión y aprobación del acta de la Sesión Ordinaria núm. 4628.
4. Correspondencia

   4.1 Oficio CR/SBD-0160-2014, de la Secretaría de Actas del Consejo Rector del Sistema Banca para el Desarrollo.

4.2 Oficio DFOE-EC-0305, dirigido al Secretario Técnico por la Gerencia de Servicios Económicos de la Contraloría General de la República.

4.3 Oficio SITRAINA 049-14 en relación a permiso con goce salarial por asistencia a curso internacional.

4.4 Traslado de documento TD-89-2014, dirigido a la Secretaría Técnica por la Presidencia Ejecutiva, en relación a permiso sin goce de salario del funcionario Wilberth Hernández Vargas.

5. Mociones.

6. Unidad de Recursos Financieros. Oficio URF-398-2014. Vencimiento de Título de Inversión.

7. Subgerencia Administrativa. Oficio SGA-309-2014. Trámite para la autorización de viáticos en el interior del país, para la Presidencia Ejecutiva, de conformidad con al Art. 7 del Reglamento de Gastos de Viaje y Transporte para Funcionarios Públicos de la Contraloría General de la República, y en atención al criterio emitido por la Asesoría Legal, mediante oficio ALEA-266-2014.

8. Subgerencia Administrativa. Oficio SGA-284-2014. Propuesta de modificación del Reglamento uso de Recursos Informáticos.

9. Gerencia General. Oficio GG-526-2014. Información complementaria sobre el Manual de Puestos, solicitada mediante Acuerdos Número 081-2014-JD y 092-2014-JD.

10. Asesoría Legal. Oficio ALCA-285-2014. Proyecto de resolución en Recurso de Apelación contra acto administrativo del Proceso de Adquisiciones, originado en licitación pública 2010LN-000010-01 para la “Contratación de Servicios Profesionales de Abogados para el Cobro Judicial del Tributo creado mediante la Ley 6868 del INA”.

11. Documentos distribuidos para ser vistos en próxima sesión:

- 13.1 Proceso de Adquisiciones. Oficio UCI-PA-1681-2014. Informe de recomendación para la adjudicación de la Licitación Pública 2012LN-000002-04 para la contratación de servicios de capacitación y formación profesional en el subsector de informática según demanda y cuantía inestimada para La Unidad Regional Polivalente de Liberia.

12. Asuntos de la Presidencia Ejecutiva

13. Varios

ARTÍCULO SEGUNDO:

Reflexión.

El señor Presidente, procede con la Reflexión del Día.

Indica que seguidamente, darán un espacio a los señores Directores que se integran hoy a la Junta Directiva. Asimismo, desea felicitar a los señores Directores Luis Fernando Monge Rojas y Claudio Solano Cerdas, por haber sido reelectos como miembros de esta Junta Directiva.

El señor Viceministro de Educación, señala que es un gusto y un honor el estar compartiendo los retos y desafíos que plantea esta nueva Administración, desde el Ministerio de Educación Pública y también contribuyendo en la Junta Directiva del

INA. Asimismo, desea transmitir el cordial saludo por parte de la Ministra de Educación, Señora Sonia Marta Mora, quien les desea el mayor de los éxitos en este período.

Agradece y se pone a las órdenes de la Junta Directiva, del INA y de todo el país, desde su posición como Viceministro de Educación, en el área de Planificación y Coordinación Regional.

El señor Director Montero Jiménez, indica que es el representante del Movimiento Cooperativo y que su Cooperativa base es la del Ministerio de Educación Pública, de la cual es el Presidente del Consejo de Administración. Asimismo, labora como Gerente de la Federación de Cooperativas de Ahorro y Crédito, con treinta y seis cooperativas afiliadas.

Agrega que el Movimiento Cooperativo es un gremio muy grande que agremia a más de ochocientos mil costarricenses, por lo que espera dar buenos aportes y la coordinación necesaria, para que en conjunto puedan llevar a cabo una amplia labor.

Señala que el Cooperativismo, es una forma asociativa más de empresa y no pueden perder de vista que pequeños, medianos y grandes empresarios, alrededor del Cooperativismo son fuente de empleo y de desarrollo para el país.

Reitera que espera que puedan hacer un trabajo en equipo satisfactorio, en bienestar del pueblo costarricense.

El señor Presidente, expresa la cordial bienvenida al señor Viceministro de Educación y al señor Director Montero Jiménez, e indica que tiene entendido que el señor Viceministro, por designación de la señora Ministra de Educación, les va a seguir acompañando en las sesiones de Junta Directiva.

Comenta que el señor Ministro de Trabajo, es el otro representante de Gobierno y no pudo estar presente por motivos laborales.

El señor Director Esna Montero, considera que es importante que cada uno se presente, a fin de conocer el Sector al que representa cada uno.

Se procede con la presentación.

El señor Presidente, agradece a todos los presentes.

ARTÍCULO TERCERO:

Discusión y aprobación del acta de la Sesión Ordinaria núm. 4628.

El señor Presidente, somete a consideración de la Junta Directiva, la discusión del acta de la Sesión Ordinaria 4628.

El señor Director Esna Montero, indica que en la página 85, último párrafo debe corregirse la parte que dice “ya que el equipo de trabajo ha trabajado muy unido”, para que se lea “ya que el equipo de trabajo es muy unido”.

El señor Director Muñoz Araya, señala que en la página 47 y hasta la 50, hay dos acuerdos que se toman por petición suya, uno sobre el 0.43% del aumento salarial y el otro sobre CATEAA y los dos están consignados en un solo acuerdo, sin embargo por la trazabilidad de los acuerdos y tomando en cuenta que se tomaron en dos fases diferentes, se consigne cada uno por separado.

El señor Asesor Legal, consulta si el acuerdo fue tomado en firme y si se incluyeron los dos temas en uno solo.

El señor Secretario Técnico, responde que fueron acuerdos firmes y el señor Director Muñoz Araya, presentó una moción sobre informes pendientes y se dividió en dos partes y fue comunicado a las unidades ejecutoras.

El señor Asesor Legal, comenta que en ese caso, habría que revocarlo para que cada uno conste por separado, lo cual se podría hacer en el capítulo de Mociones o en Varios, porque los acuerdos fueron tomados en firme y comunicados correspondientemente.

El señor Presidente, señala que se planteará en el capítulo de Mociones.

El señor Director Montero Jiménez, señala que en el acuerdo consignado en la página 31, debe corregirse para que se lea “UNICO Aprobar el acta 4626, incorporando la observación”.

El señor Presidente, somete a aprobación el acta de la Sesión 4628, con las modificaciones señaladas.

Se abstienen de votar el acta, el señor Viceministro de Educación y el señor Director Montero Jiménez, por no haber estado presentes en dicha Sesión.

COMUNICACIÓN DE ACUERDO AC-138-2014-JD

CONSIDERANDO:

1. Que el señor Presidente de Junta Directiva, Minor Rodríguez Rodríguez, somete a discusión y aprobación de los miembros presentes, el acta número 4628 de la sesión, celebrada el pasado 26 de mayo del presente año.

2. Que los Directores realizaron las siguientes observaciones al acta: el Director Tyronne Esna Montero se refiere a un error en cuanto a redacción en la página 85; el Director Jorge Muñoz Araya indica que el acuerdo número AC-132-2014-JD debe hacerse en dos acuerdos por separado, y el Director Carlos Montero Jiménez hace una corrección de forma en la página 31.

POR TANTO:

SE ACUERDA POR MAYORÍA DE LOS DIRECTORES PRESENTES A LA HORA DE LA VOTACIÓN:

ÚNICO: APROBAR EL ACTA NÚMERO **4628** DE LA SESIÓN ORDINARIA DE JUNTA DIRECTIVA, CELEBRADA EL PASADO 26 DE MAYO DE 2014, INCORPORANDO LAS OBERVACIONES REALIZADAS POR LOS SEÑORES DIRECTORES, TAL Y COMO CONSTA EN ACTAS.

ACUERDO APROBADO EN FIRME POR MAYORÍA

SE ABSTIENEN DE VOTAR EL PRESENTE ACUERDO LOS DIRECTORES CARLOS HUMBERTO MONTERO JIMÉNEZ Y MIGUEL ANGEL GUTIÉRREZ RODRÍGUEZ, POR NO HABER ESTADO PRESENTES EN DICHA SESIÓN.

ARTÍCULO CUARTO:

Correspondencia

4.1 Oficio CR/SBD-0160-2014, de la Secretaría de Actas del Consejo Rector del Sistema Banca para el Desarrollo.

El señor Presidente, solicita al señor Secretario Técnico que proceda con la lectura del oficio.

El señor Secretario Técnico, procede con la lectura:

Banca para el Desarrollo
www.sbd.fi.cr
tel: 2248-1650 / fax: 2248-1649
Oficentro Torres del Campo.
Frente a Centro Comercial El Pueblo. Torre 2, piso 3.

27 de mayo del 2014
CR/SBD-0160-2014

Señores
Junta Directiva

José Antonio Li Piñar
Gerente General
Instituto Nacional de Aprendizaje –INA-
Presente

Estimados señores:

Mediante Oficio CR-SBD-0144-2013 de fecha 13 de mayo del presente año, les fue comunicado el Acuerdo AG-1162-138-2014, adoptado por el Consejo Rector de Banca para el Desarrollo en su Sesión Ordinaria No. 138-2014 del 30 de abril del año en curso, sin embargo, el mismo fue transmitido con un error involuntario en su contenido, indicando que el Informe de ejecución de servicios del 2013, corresponde al III Trimestre, cuando en realidad las actividades fueron ejecutadas en el IV Trimestre. Por lo anterior, me permito comunicarlo nuevamente y solicitarles de forma atenta y respetuosa sustituir la nota anterior y consignar la presente como la versión definitiva de la Resolución.

Para los efectos, el Acuerdo indicado, en lo conducente indica:

> **"ACUERDO AG-1162-138-2014:** El Consejo Rector de Banca para el Desarrollo (SBD) acuerda:
>
> **1.** Dar por conocido el Informe de ejecución de los Servicios no financieros y de Desarrollo Empresarial brindados por el Instituto Nacional de Aprendizaje (INA), en el marco de la Ley 8634 y su Reglamento, en el cual se incorporan las actividades correspondientes al IV Trimestre del 2013 y I Trimestre del 2014, elaborado con base en las directrices establecidas en el "Modelo de atención servicios no financieros y de desarrollo empresarial a la PYME", aprobado por el Consejo Rector del SBD.
>
> **2.** Externar su complacencia y reconocimiento por la labor desarrollada por el INA y muy especialmente por las mejoras realizadas en el proceso de ejecución de los recursos, de cara al cumplimiento de la Ley 8634; aspecto que se da especialmente a partir de la incorporación del Lic. José Antonio Li Piñar, en la Gerencia General del INA.
>
> **ACUERDO APROBADO POR UNANIMIDAD EN FIRME"**

Atentamente,

Secretaría de actas

Lilliana Chacón C
Secretaría de Actas
Consejo Rector del SBD

Cc.- Sra. Jeannette Fonseca. Directora de Negocios. Secretaría Técnica. SBD
Archivo CyS
Archivo

LILLIANA CHACON CORRALES (FIRMA)
Digitally signed by LILLIANA CHACON CORRALES (FIRMA)
Date: 2014.05.28 14:23:02 -06:00
Reason: Secretaria de Actas. Consejo Rector del SBD, Carta al INA
Location: Costa Rica

El señor Director Muñoz Araya, indica que le parece que ha existido una buena gestión del señor Gerente General, porque aparentemente habían algunas diferencias con el Consejo Rector y las actividades que hacía el INA, en su caso, generalmente cuando se dan los informes y especialmente los referidos a las PYMES, ha pedido ciertas características, como qué tipo de PYME se está atendiendo, si es formal o informal, si es de uno, dos o tres personas, si es de subsistencia, entre otros aspectos, pero aún no tiene el panorama claro.

En ese sentido, le gustaría que le envíen una copia de este cuarto infor, que se le envió al Consejo Rector.

El señor Presidente, solicita al señor Gerente General que tome nota de la solicitud que plantea el señor Director Muñoz Araya, para que se le remita copia del informe presentado al Consejo Rector.

El señor Gerente General, indica que la Ley 8634 de Banca para el Desarrollo y que está precisamente en revisión en la Asamblea Legislativa, establece que el INA tiene que destinar el 15% de su Presupuesto Ordinario y Extraordinario, para el desarrollo de actividades de PYMES, en ese aspecto están obligados cada trimestre, a ir a dar el informe de ejecución de ese porcentaje, que más o menos significa alrededor de 14 mil millones.

En ese aspecto, lo que está señalando el SBD es que cumplió en su totalidad con el informe, según las directrices que ellos emanaron, en cuanto a la atención de las PYMES que ellos querían que se atendieran. Además, están informando que prácticamente van al día, porque había un rezago de la información que se les entregaba, porque también aceptaron el primer trimestre del año en ejercicio, lo

que significa que en los próximos días, van a tener que ir a entregar el siguiente informe, correspondiente al segundo trimestre del presente año.

El señor Viceministro de Educación, consulta si esos fondos son exclusivamente para capacitación.

El señor General, responde que la mayoría son por concepto de capacitación, sin embargo, hay un plan que desde el año pasado se empezó a trabajar, que se refiere a ciertas actividades que contemplan no solo capacitación, sino también algunos patrocinios para actividades como las ferias a nivel nacional, para promover las PYMES, entre otros.

El señor Presidente, agradece por la información.

4.2 Oficio DFOE-EC-0305, dirigido al Secretario Técnico por la Gerencia de Servicios Económicos de la Contraloría General de la República.

El señor Presidente, solicita al señor Secretario Técnico que proceda con la lectura del oficio.

El señor Secretario Técnico, procede con la lectura:

CONTRALORÍA GENERAL DE LA REPÚBLICA
COSTA RICA

DIVISIÓN DE FISCALIZACIÓN OPERATIVA Y EVALUATIVA
ÁREA DE FISCALIZACIÓN DE SERVICIOS ECONÓMICOS

1

Al contestar refiérase
al oficio No. 05050

26 de mayo, 2014
DFOE-EC-0305

INSTITUTO NAL. DE APRENDIZAJE
RECIBIDO
Fecha: 05-06-2014
Nombre: Lourdes

Licenciado
Bernardo Benavides Benavides
Secretario Técnico
Junta Directiva
INSTITUTO NACIONAL DE APRENDIZAJE (INA)

Estimado señor:

Asunto: Se le solicita a la Junta Directiva del INA, informar sobre las acciones a ejecutar con el Proyecto CATEAA y se reitera lo señalado sobre el acuerdo Nro. 111-2013-JD, en relación con ese Proyecto.

Con el propósito de que lo haga de conocimiento de los señores miembros de la Junta Directiva, nos referimos a sus oficios Nros. STJD-104-2014 y STJD-113-2014 de fechas 9 y 23 de abril del presente año.

En el primero de los oficios, se refieren a los acuerdos tomados con el objeto de atender lo requerido por este Órgano Contralor mediante la nota Nro. 02948 (DFOE-EC-0174) del 18 de marzo, en la que se le solicita a la Junta Directiva informar sobre las acciones, debidamente justificadas, que se tienen previstas con el proyecto CATEAA. Para tales efectos, adjunta el acuerdo Nro. 093-2014-J, tomado en la sesión Nro. 4622, celebrada el 2 de abril de 2014, en el que se dispuso: "*Aprobar la moción presentada por el Director Jorge Muñoz Araya, contenida en el considerando dos del presente acuerdo*", el cual consiste en que: a) La Administración les presente a la Junta Directiva, en 5 días hábiles, un cronograma con todo lo actuado, desde su inicio hasta la fecha. b) Que la Administración les certifique, en 5 días hábiles, si existen necesidades de capacitación y bases técnicas, administrativas y legales para ejecutar en el futuro inmediato, algún proyecto relativo al quehacer institucional en el lote adquirido en la Finca La Flor. c) Que la Auditoría adicione a los informes presentados, las recomendaciones que determinen presuntas situaciones irregulares y las personas involucradas, para que la Administración ejecute las medidas correspondientes.

Sobre el particular, nos permitimos indicarle que esta Contraloría General, continúa a la espera de que la Junta Directiva informe las acciones, debidamente justificadas, que tiene previstas para el Proyecto CATEAA, las cuales quedaron sujetas al resultado de lo acordado en la referida sesión Nro. 093-214-J, según así se desprende del "Comentario General" incluido en el considerando segundo de dicha sesión, que indica: "*Con estas tres acciones puntuales que proponemos, junto con sus respectivas justificaciones,*

además de responder a la petición expresa de la Contraloría, ***podemos contar con insumos en un futuro casi inmediato, para una decisión final sobre CATEAA".***

La información requerida, debe ser remitida con un plazo de 5 días hábiles, contados a partir de la fecha de la sesión del órgano colegiado inmediata posterior al recibo de la presente solicitud.

En el segundo de los oficios, informa que el acuerdo de ese órgano colegiado Nro. 111-2013-JD, tomado en la sesión extraordinaria Nro. 4583, celebrada el 12 de junio del 2013, se encuentra vigente, el cual textualmente señala:

> *"Para que este informe de la Auditoría Interna y referido a la iniciativa CATEAA, se remita a análisis, estudio y recomendación de la Contraloría General de la República, que se suspenda todo trámite, gasto e inversión, sobre este Proyecto o Iniciativa, hasta tanto no se cuente con el pronunciamiento de la Contraloría General de la República, al respecto".*

Agrega que la Junta Directiva del INA no ha modificado la disposición de suspender indefinidamente los trámites, gastos e inversiones en relación con el mencionado proyecto, hasta que se emita el acto final, una vez cumplidas y presentadas al órgano colegiado las medidas aprobadas en el acuerdo Nro. 093-2014-JD.

Al respecto nos permitimos reiterar lo señalado en el oficio Nro. 09863 (DFOE-EC-0492) de fecha 19 de setiembre de 2013, en el cual se les advirtió lo siguiente:

> *"(...) el acuerdo tomado por la Junta Directiva de suspender todo trámite, gasto e inversión relacionado con el Proyecto CATEEA, es una decisión que se enmarca dentro de la esfera administrativa, la cual es ajena a nuestras competencias, por lo que las decisiones tomadas sobre el particular son de absoluta y exclusiva responsabilidad de ese Instituto.*
>
> *Lo anterior, sin perjuicio de las valoraciones que, conforme a sus competencias, realice este órgano contralor y el establecimiento de las eventuales acciones que correspondan, en relación con la información aportada sobre el referido Proyecto".*

Atentamente,

Licda. Marjorie Gómez
Gerente de Área

MGCH/MMC/OLAS/MOP/krq

NI: 18627 (2013), 4777-4778-5726-7338-8472-9083 (2014)

Ci Expediente (G-2013003499, P-1)

El señor Director Muñoz Araya, señala que dadas las implicaciones que tiene este oficio y algunos asuntos que tienen pendientes y del tiempo que está dando la Contraloría General de la República, le gustaría poder hacer una discusión, para lo cual le solicitaría a los funcionarios de la Gerencia y Subgerencias, que les permitan realizar este análisis en privado.

El señor Asesor Legal, indica que en su caso también se excusa de participar en la discusión, en virtud de que el Proyecto inició cuando su persona era el Gerente General de la Institución.

Se retiran momentáneamente del Salón de Sesiones, el señor Gerente General, la señora Subgerente Administrativa, el señor Subgerente Técnico y el señor Asesor Legal.

El señor Presidente, somete a votación la propuesta que se ha discutido, en el sentido de solicitar a la Contraloría General de la República, una prórroga de hasta un mes a partir de esta fecha, para que los nuevos integrantes de la Junta Directiva, tengan tiempo de estudiar los antecedentes, actuaciones e insumos varios, relativos al Proyecto CATEAA y emanar el informe solicitado por el Ente Contralor, en el Oficio DFOE-EC-0305.

COMUNICACIÓN DE ACUERDO AC-139-2014-JD

CONSIDERANDO:

1. Que la Junta directiva ha sido puesta en conocimiento del oficio DFOE-EC-0305, de fecha 26 de mayo de 2014, remitido por la División de Fiscalización Operativa y Evaluativa de la Contraloría General de la República, dirigido al Secretario Técnico, por el cual se solicita al órgano colegiado informar sobre las acciones a ejecutar con el Proyecto CATEAA y se reitera lo señalado sobre el acuerdo número 111-2013-JD, en relación con ese proyecto.

2. Que en dicho oficio se indica que la información solicitada debe ser remitida en un plazo de cinco días hábiles contados a partir de la fecha de la sesión inmediata posterior al recibo de la solicitud.

3. Que preocupa al órgano colegiado el señalamiento de un plazo de respuesta tan reducido, por cuanto hasta la presente semana se ha juramentado un nuevo miembro de la Junta Directiva, en representación del sector cooperativo, que desconoce los amplios y complejos antecedentes y actuaciones sobre el Proyecto CATEAA. De igual manera, el Presidente Ejecutivo, el Ministro de Trabajo, y el Viceministro de Educación, también integrantes ex oficio de la Junta Directiva, son nuevos en el ejercicio de sus cargos, requiriendo de más tiempo para estudiar los insumos del mencionado Proyecto y estar en condiciones de tomar decisiones.

4. Que se hace necesario, en vista de las consideraciones anteriores, solicitar al órgano contralor, una prórroga de un mes a partir de la fecha de firmeza del presente acuerdo, para informar en forma justificada sobre las acciones a tomar en relación al Proyecto CATEAA.

POR TANTO:

SE ACUERDA POR UNANIMIDAD DE LOS MIEMBROS PRESENTES A LA HORA DE LA VOTACIÓN:

ÚNICO: SOLICITAR A LA CONTRALORÍA GENERAL DE LA REPÚBLICA UNA PRÓRROGA DE **UN MES**, A PARTIR DE LA FECHA DE FIRMEZA DEL PRESENTE ACUERDO, PARA QUE LOS NUEVOS INTEGRANTES DE LA JUNTA DIRECTIVA TENGAN TIEMPO DE ESTUDIAR LOS ANTECEDENTES, ACTUACIONES E INSUMOS VARIOS, RELATIVOS AL PROYECTO CATEAA Y EMANAR EL INFORME SOLICITADO POR DICHO ÓRGANO CONTRALOR EN OFICIO DFOE-EC-0305.

SEGUNDO: QUE LA SECRETARIA TÉCNICA PRESENTE A LA MAYOR BREVEDAD DICHA SOLICITUD A LA CONTRALORÍA GENERAL DE LA REPÚBLICA.

ACUERDO APROBADO EN FIRME POR UNANIMIDAD

Reingresan al Salón de Sesiones, el señor Gerente General, la señora Subgerente Administrativa, el señor Subgerente Técnico y el señor Asesor Legal.

4.3 Oficio SITRAINA 049-14 en relación a permiso con goce salarial por asistencia a curso internacional.

El señor Presidente, solicita al señor Secretario Técnico que proceda con la lectura del oficio.

El señor Secretario Técnico, procede con la lectura:

SINDICATO TRABAJADORES DEL INA
-SITRAINA-

San José-Costa Rica Tele 2210-6200 Fax 2220-2480
SITRAINA@ina.ac.cr

La Uruca, 30 de mayo de 2014
SITRAINA 049-14

Señores y señoras
Directores Junta Directiva
Instituto Nacional de Aprendizaje

Estimados (as) señores (as):

Reciban un saludo cordial de SITRAINA. Nuestro Sindicato ha sido invitado a participar en el Curso para Sindicalistas, que se llevará a cabo en Santa Clara, provincia de Villa Clara, Cuba del 14 al 29 de junio 2014. (Se adjunta convocatoria y temas a tratar).

Nuestra organización Sindical ha designado al compañero Jorge Alberto Castro Castro, cédula 1-421-762, Secretario de Afiliación, docente de la Unidad Regional Central Oriental, y a las compañeras Elida Mesén Anchía, cédula 1-474-534, Secretaria de Asuntos de la Mujer, funcionaria de la Unidad Regional Central Oriental y a Miriam Ramírez Azofeifa, cédula 4-108-611, Segunda Suplencia y docente del Núcleo Agropecuario, para que participen en este evento de capacitación Sindical, en representación de SITRAINA.

Por está razón y de acuerdo a lo que establece el Reglamento Autónomo de Servicios del INA, en su C apítulo VIII Licencias en general, artículo 37, inciso C, SITRAINA les solicita el respectivo permiso con goce de salario para que estas personas puedan participar en dicha capacitación Sindical. El permiso sería del 13 al 27 de junio, ambos inclusive.

En espera de la amable atención de ustedes, quedamos a la orden para cualquier información adicional.

Atentamente,

JUNTA DIRECTIVA **SITRAINA**

Jorge Gamboa Quirós
Secretario General

gmc

SITRAINA - 1979 SINDICATO DE TRABAJADORES DEL INSTITUTO NACIONAL DE APRENDIZAJE

INSTITUTO NAL. DE APRENDIZAJE
JUNTA DIRECTIVA
RECIBIDO
Fecha: 30/05/2014
Nombre: Alba

Señores y señoras
Directores Junta Directiva
Instituto Nacional de Aprendizaje

página 2

30 de mayo de 2014

Nota: En el caso de la docente Miriam Ramírez Azofeifa y el docente Jorge Castro Castro ya han sido reprogramados los SCFP asignados a ambos. Aspecto que se puede corroborar en consulta a la Licenciada Maricel Méndez Vargas, Jefe del Núcleo Agropecuario y la Licenciada Flor Rojas Rodríguez, Jefe de la Unidad de Servicio al Usuario de la Unidad Regional Central Oriental. En el caso de la compañera Élida Mesén Anchía, Encargada de Proyecto, ella elabora un listado de las diferentes actividades que le corresponde ejecutar y se lo entrega a la Licenciada Flor Rojas Rodríguez anteriormente citada para que asigne a otras personas funcionarias dichas actividades.

CONVOCATORIA

La Central de Trabajadores de Cuba (CTC) y la Escuela Nacional de Cuadros Sindicales "Lázaro Peña" convocan a las organizaciones sindicales de América Latina y el Caribe a participar en el Curso para Sindicalistas, del 14 al 29 de junio de 2014, en la provincia de Villa Clara, Cuba.

En la ciudad de Santa Clara, capital de la Provincia de Villa Clara, descansan los restos del guerrillero heroico "Ernesto Guevara de la Serna, Che" y su destacamento de refuerzo, como permanente homenaje a quién, por su ejemplo, valor y sacrificio, alcanza estatura universal.

Objetivo General:
Contribuir a la preparación política y sindical de los dirigentes sindicales de América Latina y el caribe para enfrentar el escenario internacional actual.

Contenidos Fundamentales:

1. La crisis estructural del sistema capitalista hoy. Sus manifestaciones en los trabajadores y los sindicatos.
3. El escenario político - ideológico donde desarrolla su accionar el Dirigente Sindical.
4. La integración como una vía activa de la unidad y el desarrollo de la región latinoamericana.
5. El liderazgo político revolucionario. Necesidad en la América Latina actual.
6. Necesidad de la defensa de los derechos de los trabajadores y sus organizaciones sindicales.
7. La lucha por la preservación y conservación del medio ambiente. Desafío de los trabajadores y sus sindicatos.

El horario docente comienza a partir de las 9.00 am a las 12.30 pm y de 2.00 pm a 4.25 pm.

El programa incluye visitas de interés sindical y social.

El alojamiento y desarrollo del programa docente se realizará en la Escuela Provincial de la Central de Trabajadores de Cuba en Villa Clara.

El costo de la matrícula es de **$420.00 CUC** (moneda convertible cubana), la que debe cancelarse a la llegada al Hotel, incluye: la docencia; el transporte desde y hacia el aeropuerto de La Habana, ida y regreso a la ciudad de Villa Clara, distante de la Habana en 280 kms, y a las actividades incluidas en el programa oficial del curso; el hospedaje en el Hotel "Puesta del Sol" en transito y en la Escuela Provincial de la CTC de Villa Clara con desayuno, almuerzo y cena.

El cambio de moneda debe realizarse a su llegada al Aeropuerto Internacional "José Martí". Se sugiere traer preferentemente EUROS. Los cursistas deben reservar 25.00 CUC para el pago del impuesto de aeropuerto a la salida para sus países, así como traer actualizado su seguro de salud.

Las instalaciones que se utilizaran para el desarrollo del curso son propiedad de la CTC, no están vinculadas al sistema de turismo del país.

Se solicita que en el proceso de selección de los compañeros (as) a participar en el curso se tenga en cuenta las condiciones de salud que le permitan cumplimentar el programa previsto.

Es importante en el cumplimiento de los objetivos del curso que los participantes reciban copia de esta convocatoria.

SITRAINA
RECIBIDO
FECHA 12-5-14

Deben enviar **antes del viernes 30 de mayo** la solicitud con los datos que a continuación se relacionan y se confirmará la matrícula por nuestra parte el **lunes 2 de junio**. Sin esta confirmación no es posible acceder al curso, ya que la cifra de participantes es limitada.

- Nombres y apellidos.
- Organización sindical a la que pertenece.
- Responsabilidad que ostenta en ella.
- País.
- Ciudadanía.
- Número de pasaporte.

Los aspirantes aceptados deberán remitir antes del **día 6 de Junio**, la fecha, hora y línea aérea de arribo a la Habana.

Importante:

La llegada a la Habana, tiene que ser los días 14 y 15 de Junio, ya que el día 16 de junio a las 7.00 am parte el ómnibus con los cursistas para la Provincia de Villa Clara.

La salida a sus respectivos países tiene que ser a partir del día 28 de junio, ya que el regreso desde Villa Clara se realizará el viernes 27 de junio en horas de la tarde.

Los días de estancia en el Hotel Puesta del Sol antes del día 14 y después del día 29, serán abonados al Hotel por los precios vigentes en la instalación.

Escuela Nacional de Cuadros Sindicales
"Lázaro Peña"
Calle: 264 esq. 33, San Agustín,
La Lisa, La Habana.
Teléf. 53 7 271 -07-72, 271-94-39.
E.mail: bertha@escuela.ctc.cu
reglita@escuela.ctc.cu

Central de Trabajadores de Cuba (CTC)
Teléf. 53 7 877- 5312
Email: ri.america2@ctc.cu

Regla María Águila Hernández
Directora

Raymundo Navarro Fernández
Miembro del Secretariado

El señor Asesor Legal, menciona para que se tome en cuenta a la hora de hacer el acuerdo, que la solicitud del Sindicato tiene su fundamento, en el Reglamento Autónomo de Servicios y en la Convención Colectiva, por lo que se debe hacer alusión a los mismos, en los considerandos del acuerdo correspondiente.

El señor Director Esna Montero, indica que de acuerdo con la información, los funcionarios saldrían el 13 de junio, por lo que se deben apurar con la comunicación del acuerdo, porque queda muy poco tiempo, para evitar algún contratiempo.

El señor Presidente, somete a votación la solicitud presentada por el Sindicato mediante oficio SITRAINA-049-14.

COMUNICACIÓN DE ACUERDO AC-140-2014-JD

CONSIDERANDO:

1. Que mediante oficio SITRAINA 049-14, de fecha 30 de mayo de 2014, el Sindicato de Trabajadores del INA, remite para conocimiento y eventual aprobación por parte de los miembros de la Junta Directiva, solicitud de permiso con goce salarial para tres funcionarios del INA, con el fin de que puedan participar en el curso para Sindicalistas que se llevará a cabo en Santa Clara, provincia de Villa Clara, Cuba, del 14 al 29 de junio del presente año.
2. Que se ha designado a los siguientes funcionarios para que asistan al curso de marras en representación de SITRAINA: **JORGE ALBERTO CASTRO CASTRO**, con cédula de identidad 1-421-762, Secretario de Afiliación y docente de la Unidad Regional Central Oriental, señora **ELIDA MESÉN ANCHÍA,** con cédula de identidad 1-474-534, Secretaria de Asuntos de la Mujer y funcionaria de la Unidad Regional Central Oriental, y a la señora **MIRIAM RAMÍREZ AZOFEIFA**, con cédula de identidad 4-108-611, Segunda Suplencia y docente del Núcleo Agropecuario.
3. Que el permiso anteriormente mencionado, se solicita con base al artículo 18 de la Convención Colectiva, el cual establece:

"Permisos con goce de salario. Para otorgar permisos con goce de salario, debe estar el caso dentro de lo establecido en esta convención y las previsiones del artículo 37 del Reglamento Autónomo de Servicios, aplicándose para los efectos de esta convención; todo lo regulado en la citada normativa…"

4. Que el artículo 37, inciso c) del Reglamento Autónomo de Servicios del INA, establece lo siguiente:

"c- Podrá otorgarse permiso con goce de salario hasta por un máximo de tres meses, a funcionarios que en su condición de dirigentes o miembros activos de las diversas asociaciones gremiales y sociales de la Institución, cuando soliciten licencia para participar en seminarios o cursos de entrenamiento, dentro o fuera del país relacionados con el campo específico de la asociación que representan.

El otorgamiento de esa licencia quedará sujeto a que no se perjudique el normal desarrollo de las actividades de la oficina donde presta sus servicios el solicitante, para lo cual se considerará el criterio de la jefatura respectiva. Se tomará en cuenta también la importancia del seminario o curso en cuestión, en cuyo caso, el órgano encargado de resolver podrá solicitar en caso de duda, un informe previo al Ministerio de Trabajo y Seguridad Social.

En los mismos términos indicados en los párrafos anteriores, podrá otorgarse licencia con goce de salario a los funcionarios institucionales que en ocasión de misiones especiales deben desplazarse al extranjero para representar al país en eventos deportivos, culturales o educativos, siempre que esas actividades sean de interés nacional y revistan carácter oficial.

En ambos supuestos, corresponde a la Gerencia resolver la solicitud cuando la actividad se desarrolle dentro del país o el permiso no exceda de un mes, en los demás casos, corresponde a la Junta Directiva adoptar la resolución del caso."

5. Que la solicitud de permiso con goce salarial a favor de los funcionarios anteriormente mencionados, rige a partir del 13 al 27 de junio del presente año, ambos días inclusive
6. Que los señores Directores de Junta Directiva aprobaron en un todo, lo solicitado por el Sindicato de Trabajadores del INA, contenido en el oficio SITRAINA 049-14 de fecha 30 de mayo de 2014, el cual literalmente indica:

SINDICATO TRABAJADORES DEL INA
-SITRAINA-

San José-Costa Rica Tele 2210-6200 Fax 2220-2480
SITRAINA@ina.ac.cr

La Uruca, 30 de mayo de 2014
SITRAINA 049-14

Señores y señoras
Directores Junta Directiva
Instituto Nacional de Aprendizaje

Estimados (as) señores (as):

Reciban un saludo cordial de SITRAINA. Nuestro Sindicato ha sido invitado a participar en el Curso para Sindicalistas, que se llevará a cabo en Santa Clara, provincia de Villa Clara, Cuba del 14 al 29 de junio 2014. (Se adjunta convocatoria y temas a tratar).

Nuestra organización Sindical ha designado al compañero Jorge Alberto Castro Castro, cédula 1-421-762, Secretario de Afiliación, docente de la Unidad Regional Central Oriental, y a las compañeras Elida Mesén Anchía, cédula 1-474-534, Secretaria de Asuntos de la Mujer, funcionaria de la Unidad Regional Central Oriental y a Miriam Ramírez Azofeifa, cédula 4-108-611, Segunda Suplencia y docente del Núcleo Agropecuario, para que participen en este evento de capacitación Sindical, en representación de SITRAINA.

Por está razón y de acuerdo a lo que establece el Reglamento Autónomo de Servicios del INA, en su C apítulo VIII Licencias en general, artículo 37, inciso C, SITRAINA les solicita el respectivo permiso con goce de salario para que estas personas puedan participar en dicha capacitación Sindical. El permiso sería del 13 al 27 de junio, ambos inclusive.

En espera de la amable atención de ustedes, quedamos a la orden para cualquier información adicional.

Atentamente,

JUNTA DIRECTIVA **SITRAINA**

Jorge Gamboa Quirós
Secretario General

gmc

SITRAINA - 1979
SINDICATO DE TRABAJADORES DEL INSTITUTO NACIONAL DE APRENDIZAJE

INSTITUTO NAL. DE APRENDIZAJE
JUNTA DIRECTIVA
RECIBIDO
Fecha 30/05/2014
Nombre: Alba

1

POR TANTO:

SE ACUERDA POR UNANIMIDAD DE LOS MIEMBROS PRESENTES A LA HORA DE LA VOTACIÓN:

ÚNICO: APROBAR EL PERMISO CON GOCE SALARIAL, SOLICITADO POR EL SINDICATO DE TRABAJADORES DEL INA, CONTENIDO EN EL OFICIO SITRAINA 049-14, DE FECHA 30 DE MAYO DE 2014, PARA LOS SIGUIENTES FUNCIONARIOS: **JORGE ALBERTO CASTRO CASTRO**, CON CÉDULA DE IDENTIDAD 1-421-762, SECRETARIO DE AFILIACIÓN Y DOCENTE DE LA UNIDAD REGIONAL CENTRAL ORIENTAL, SEÑORA **ELIDA MESÉN ANCHÍA,** CON CÉDULA DE IDENTIDAD 1-474-534, SECRETARIA DE ASUNTOS DE LA MUJER Y FUNCIONARIA DE LA UNIDAD REGIONAL CENTRAL ORIENTAL, Y A LA SEÑORA **MIRIAM RAMÍREZ AZOFEIFA**, CON CÉDULA DE IDENTIDAD 4-108-611, SEGUNDA SUPLENCIA Y DOCENTE DEL NÚCLEO AGROPECUARIO.

ACUERDO APROBADO EN FIRME POR UNANIMIDAD

4.4 **Traslado de documento TD-89-2014, dirigido a la Secretaría Técnica por la Presidencia Ejecutiva, en relación a permiso sin goce de salario del funcionario Wilberth Hernández Vargas.**

El señor Presidente, solicita al señor Secretario Técnico que proceda con la lectura del oficio.

El señor Secretario Técnico, procede con la lectura:

Instituto Nacional de Aprendizaje
Llave del Progreso

TRASLADO DE DOCUMENTO

PRESIDENCIA EJECUTIVA

Tel. :(506)2210-6133 Fax: 2231-6303
E-mail: pmejiasarrieta@ina.ac.cr •

Traslado No.: TD-89- 2014

Fecha: 2 de junio del 2014

Para: Bernardo Benavides
Secretaría Técnica Junta Directiva

De: Minor Rodríguez Rodríguez
Presidente Ejecutivo

PRESIDENCIA EJECUTIVA

Asunto: Remito copia de los documentos de solicitud de permiso sin goce de salario del funcionario Wilberth Hernández Vargas, de la Unidad Regional Brunca, para laborar como Asesor en la Asamblea Legislativa, con el fin de que sea incluido entre los temas de agenda de la Junta Directiva.

Trámite:

Urgente ___

Normal _X___

PRESIDENCIA EJECUTIVA

Observaciones:

AL CONTESTAR, FAVOR REFERIRSE AL NÚMERO DE TRASLADO

INSTITUTO NAL DE APRENDIZAJE
JUNTA DIRECTIVA
RECIBIDO
Fecha: 04-06-2014
Nombre: Lourdes

Pérez Zeledón, 02 de mayo del 2014.

Licenciado
Francisco Marín Monge
Presidente Ejecutivo
Instituto Nacional de Aprendizaje

Atento saludo:

El suscrito Wilberth Hernández Vargas, cédula de identidad 1-0767-0601, funcionario de la Unidad Regional Brunca, de manera atenta le solicito un permiso sin goce de salario para laborar como Asesor en la Asamblea Legislativa durante el período del 15 de mayo del 2014 al 30 de abril del 2018.

Por lo que le agradezco interponer sus buenos oficios para obtener la autorización del permiso por parte de la Junta Directiva del Instituto Nacional de Aprendizaje y poder aprovechar esta nueva oportunidad laboral.

Actualmente me desempeño como Profesional de Apoyo IB, en la clave N° 500113 y mi puesto se encuentra en propiedad. Esta solicitud cuenta con el visto bueno del señor Jorge Fallas Bogarin, Director de la Unidad Regional Brunca.

Agradeciendo su colaboración.

DIRECCION
UNIDAD REGIONAL BRUNCA

Mba. Wilberth Hernández Vargas
Profesional de Apoyo IB
Unidad Regional Brunca.

C. Msc. José Antonio Li Piñar. Gerente General.
Lic. Ricardo Arroyo Yanarella. Asesor Despacho Presidencia Ejecutiva.
Lic. Bernardo Benavides Benavides, Secretario Junta Directiva.
M.ed. Jorge Fallas Bogarin. Director Unidad Regional Brunca.
whv

Jefatura de Fracción
Partido Liberación Nacional

5 de Mayo 2014
JF-PLN-003- 2014

Señor
Francisco Marín Monge
Presidente Ejecutivo
Instituto Nacional de Aprendizaje
S.D.

Estimado Señor

Reciba un cordial saludo de parte de los Diputados de la Fracción del PLN. El motivo de la presente es para informarle que el Sr. Wilberth Hernández Vargas Céd. 1-0767-0601 funcionario del INA, será contratado por dicha fracción a partir del 15 del presente mes hasta el 30 de abril del 2018.

De usted muy atentamente,

Partido Liberación Nacional
Jefatura de Fracción
2010 - 2014
ASAMBLEA LEGISLATIVA

Juan Luis Jiménez Succar
JEFE DE FRACCION PLN

C: interezado
Archivo

ASAMBLEA LEGISLATIVA

12 de mayo del 2014
DRH965-05

Señor(a)
Hernández Vargas Wilberth
Despacho Dip. Aracelli Segura Retana
Fracción del Partido Liberación Nacional
Presente

Asunto: Artículo 9, Sesión ordinaria 001-2014 del 06/05/2014.

Estimado(a) señor(a):

En sesión ordinaria No. 001-2014, celebrada por el Directorio Legislativo del 06 de mayo 2014, se tomaron los acuerdos que a continuación transcribo:

ARTICULO 9 SE ACUERDA

Nombrar al señor(a) Hernández Vargas Wilberth , cédula Nº 107670601 , en el puesto de ASESOR ESPECIALIZADO B-R , a partir del 15 de mayo del 2014 y hasta el 30 de abril del 2018.

Nota: Favor presentarse dentro de los próximos tres días hábiles en el Área de Gestión de Recursos Humanos, este Departamento iniciará el trámite de pago hasta que el beneficiario actualice su expediente personal.

Cordialmente,

ASAMBLEA LEGISLATIVA
DIRECCION
Departamento
Recursos
Humanos
REPUBLICA DE COSTA RICA

Licda. Eunice Pandolfi C.
DIRECTOR

Cc: Dip. Aracelli Segura Retana
Expediente
Archivo

/gra*

El señor Presidente, solicita al señor Asesor Legal que se refiera a este tema.

El señor Asesor Legal, indica que en este caso pediría a la Junta Directiva que se le traslade el caso a la Asesoría Legal, en virtud de que la redacción de la normativa de la Convención Colectiva no es muy clara, y entiende que este funcionario ya disfrutó de un permiso por dos años, para trabajar en el IMAS en el Gobierno anterior y se reintegró al INA el 1 de mayo y en teoría, luego de su reintegro a la Institución, deben pasar seis meses como mínimo, para poder tener derecho a un nuevo permiso sin Goce de Salario.

Asimismo, debe constar el acuerdo del Directorio y en los documentos solo se hace referencia y no consta el mismo.

Reitera que solicitaría, para poder emitir un dictamen y que los señores Directores tengan toda la seguridad, que se le remita a la Asesoría Legal, para lo cual el próximo lunes estaría dando el informe.

El señor Presidente, indica que el acuerdo que se tomaría sería en el sentido de trasladar el oficio a la Asesoría Legal, para tener mejor criterio con respecto al permiso sin Goce de Salario, solicitado por el señor Wilberth Hernández Vargas, el cual se estaría viendo nuevamente en la próxima Sesión.

Somete a votación la propuesta.

COMUNICACIÓN DE ACUERDO AC-141-2014-JD

CONSIDERANDO:

1. Que mediante oficio de traslado de documento número TD-89-2014, la Presidencia Ejecutiva remite a la Secretaría Técnica de la Junta Directiva, permiso sin goce salarial solicitado por el funcionario Wilberth Hernández Vargas, de la Unidad Regional Brunca, según oficio de fecha 02 de mayo de 2014.

2. Que el señor Hernández Vargas, indica en su oficio que su solicitud en con el fin de laborar como Asesor en la Asamblea Legislativa, durante el período del 15 de mayo del presente año, al 30 de abril del 2018, por tal motivo, solicita la aprobación respectiva por parte de la Junta Directiva del INA.

3. Que el Asesor Legal, Licenciado Ricardo Arroyo Yannarella, expone su criterio legal con respecto al permiso de marras, indicando que el funcionario Hernández Vargas ya disfrutó de un permiso de dos años para trabajar en el IMAS en el gobierno anterior, y que el artículo 17 de la Convención Colectiva establece que cuando un funcionario haya disfrutado de cualquiera de las licencias sin goce salarial establecidas en ese numeral, no podrá concedérsele nuevo permiso si previamente no se ha reintegrado a su trabajo, por un período mínimo de seis meses, además de que no consta el acuerdo del Directorio Legislativo respectivo.

4. Que por lo anteriormente expresado, el Asesor Legal solicitó a la Junta Directiva remitir el permiso de marras a la Asesoría Legal, con el fin de que esa Unidad revise el expediente correspondiente y emitir un dictamen legal para la Junta Directiva para la próxima sesión, para que ese órgano colegiado tome la decisión definitiva al respecto.

5. Que los señores Directores aprueban la solicitud del Asesor Legal.

POR TANTO:

SE ACUERDA POR UNANIMIDAD DE LOS DIRECTORES PRESENTES A LA HORA DE LA VOTACIÓN:

ÚNICO: TRASLADAR A LA ASESORÍA LEGAL LA SOLICITUD DE PERMISO SIN GOCE SALARIAL DEL FUNCIONARIO WILBERTH HERNÁNDEZ VARGAS, CON EL FIN DE QUE ESA ASESORÍA EMITA UN DICTAMEN SOBRE LA LEGALIDAD DEL PERMISO RESPECTIVO Y PRESENTARLO A LA JUNTA DIRECTIVA EN LA SESIÓN DEL 16 DE JUNIO DE 2014.

ACUERDO APROBADO EN FIRME POR UNANIMIDAD

ARTÍCULO QUINTO:

Mociones.

El señor Director Muñoz Araya, menciona que en la Sesión anterior se tomó un acuerdo que está consignado en el acta correspondiente, de la página 47 a la 50, y cuyo número es el AC-132-2014, por lo que solicita que se revoque ese acuerdo y que se comuniquen los dos temas que allí se abarcan, en acuerdos separados, dado que uno corresponde al informe del 0.43% y el segundo es sobre CATEAA.

El señor Presidente, indica que el acuerdo sería para que el acuerdo AC-132-2014, consignado en la página 47, se comuniquen por separado los temas abarcados en el acuerdo.

Somete a votación la moción.

COMUNICACIÓN DE ACUERDO AC-142-2014-JD

CONSIDERANDO:

1. Que el Director Jorge Muñoz Araya interpone recurso de revocatoria, de conformidad con el artículo 58 de la Ley General de Administración Pública y el artículo 20 del Reglamento de Junta Directiva del INA, para que, por objeción de forma, se deje sin efecto en su totalidad el acuerdo de Junta Directiva número **AC-132-2014-JD**, tomado en la sesión número 4628 de fecha 26 de mayo del presente año.
2. Que el Director Muñoz Araya en la sesión celebrada el pasado 26 de mayo, mocionó para solicitar a Gerencia General la presentación del informe pendiente solicitado en el acuerdo AC-081-2014-JD, sobre el impacto que sobre salarios hubiera tenido el INA con el último aumento del 0.43%, si se hubiera aprobado el Manual de Clases, y cuál sería también el impacto en cuanto a las finanzas de la institución. Así como también solicitó a la Auditoría Interna el informe pendiente sobre el tema de CATEAA.

3. Que las anteriores solicitudes del Director Muñoz Araya, se consignaron en un solo acuerdo, siendo lo conveniente, por facilidad de seguimiento, dos acuerdos

por separado, y por tal razón solicita que se revoque el acuerdo AC-132-2014-JD y se hagan los acuerdos respectivos, ya que ambos corresponden a diferentes informes.

4. Que los miembros de la Junta Directiva expresaron su anuencia para acoger el recurso de revocatoria por las razones expuestas por el Director Muñoz Araya, y se deja sin efecto, en su totalidad, el acuerdo de Junta Directiva número AC-132-2014-JD de fecha 26 de mayo de 2014. La Secretaría Técnica consignará en dos acuerdos por separado el contenido del mismo, que permanece inalterado, por tratarse de dos temas diferentes que conviene separar por la forma y no por el fondo.

POR TANTO:

SE ACUERDA POR UNANIMIDAD DE LOS DIRECTORES PRESENTES A LA HORA DE LA VOTACIÓN:

ÚNICO: ACOGER EL RECURSO DE REVOCATORIA INTERPUESTO POR EL DIRECTOR JORGE MUÑOZ ARAYA, PARA DEJAR SIN EFECTO, EN SU TOTALIDAD, POR LA FORMA Y NO POR EL FONDO, EL ACUERDO NO. AC-**132-2014-JD,** APROBADO EN LA SESIÓN NÚMERO 4628 DEL 26 DE MAYO DE 2014. LA SECRETARÍA TÉCNICA CONSIGNARÁ EN DOS ACUERDOS SEPARADOS EL CONTENIDO DEL MISMO, QUE PERMANECE INALTERADO, POR TRATARSE DE TEMAS DIFERENTES QUE CONVIENE SEPARAR PARA EFECTOS DE SEGUIMIENTO.

ACUERDO APROBADO EN FIRME POR UNANIMIDAD

COMUNICACIÓN DE ACUERDO AC-143-2014-JD

CONSIDERANDO:

1. Que mediante acuerdo de Junta Directiva número AC-142-2014-JD, de fecha 11 de junio de 2014, el Director Jorge Muñoz Araya interpuso recurso de revocatoria en cuanto a la forma, del acuerdo número AC-132-2014-JD, tomado en la sesión número 4628 de fecha 26 de mayo de 2014, toda vez que por un asunto de trazabilidad, y tratándose de dos temas diferentes, el mismo tenía que realizarse en dos acuerdos por separado, por lo que en el acuerdo AC-142-2014-JD, se acordó que la Secretaría Técnica consignara las mociones presentadas por el Director Muñoz Araya en la sesión del pasado 26 de mayo, mediante dos acuerdos por separados, manteniéndose de forma incólume el contenido del mismo.

2. Que el Director Muñoz Araya en el acuerdo AC-132-2014-JD, solicitó a la Gerencia General el informe sobre "EL IMPACTO QUE SOBRE SALARIOS HUBIERA TENIDO EL INA CON EL ÚLTIMO AUMENTO DEL 0.43%, SI SE HUBIERA APROBADO EL MANUAL DE CLASES, Y CUÁL SERÍA TAMBIÉN EL IMPACTO EN CUANTO A LAS FINANZAS DE LA INSTITUCIÓN".

3. Que el señor Gerente General informó que dicho informe ya se encuentra presentado a la Secretaría Técnica para ser agendado.

POR TANTO:

SE ACUERDA POR UNANIMIDAD DE LOS DIRECTORES PRESENTES A LA HORA DE LA VOTACIÓN:

ÚNICO: QUE EL INFORME PENDIENTE DE PRESENTAR A LA JUNTA DIRECTIVA POR PARTE DE LA GERENCIA GENERAL, MENCIONADO EN EL CONSIDERANDO SEGUNDO DEL PRESENTE ACUERDO, SE INCLUYA EN LA AGENDA DE LA PRÓXIMA SESIÓN PARA SER CONOCIDO POR ESE ÓRGANO COLEGIADO.

ACUERDO APROBADO EN FIRME POR UNANIMIDAD

COMUNICACIÓN DE ACUERDO AC-144-2014-JD

CONSIDERANDO:

1. Que mediante acuerdo de Junta Directiva número AC-142-2014-JD, de fecha 11 de junio de 2014, el Director Jorge Muñoz Araya interpuso recurso de revocatoria en cuanto a forma, sobre el acuerdo número AC-132-2014-JD, tomado en la sesión número 4628 de fecha 26 de mayo de 2014, toda vez que por un asunto de trazabilidad, y tratándose de dos temas diferentes, el mismo se tenía que realizarse en dos acuerdos por separado, por lo que en el acuerdo AC-142-2014-JD, se acordó que la Secretaría Técnica consignara las mociones presentadas por el Director Muñoz Araya en la sesión del pasado 26 de mayo, mediante dos acuerdos por separados, manteniéndose de forma incólume el contenido del mismo.

2. Que el Director Muñoz Araya mocionó en la sesión del 26 de mayo de 2014, para que la Auditoría Interna presentara ante ese órgano colegiado, el informe pendiente sobre el tema del proyecto CATEAA.

3. Que la señora Auditora Interna solicitó una prórroga para presentar dicho informe, toda vez que la funcionaria a cargo del mismo, se encuentra incapacitada, por lo que solicita dos semanas de prórroga, sea, para la sesión del 09 de junio del presente año.

POR TANTO:

SE ACUERDA POR UNANIMIDAD DE LOS DIRECTORES PRESENTES A LA HORA DE LA VOTACIÓN:

ÚNICO: APROBAR UNA PRÓRROGA DE DOS SEMANAS, PARA QUE LA AUDITORÍA INTERNA PRESENTE EL INFORME SOBRE EL PROYECTO CATEAA EN LA SESIÓN DEL PRÓXIMO **9 DE JUNIO** DEL PRESENTE AÑO.

ACUERDO APROBADO EN FIRME POR UNANIMIDAD

El señor Director Muñoz Araya, comenta que hay una invitación para asistir el próximo 19 de junio, a un Encuentro Empresarial en Liberia, Guanacaste, pero lamentablemente en su caso no puede asistir, porque tiene Sesión del Consejo Asesor del Tecnológico, pero le parece importante que alguien pueda asistir, para lo cual debe tomarse el acuerdo, a fin de que puedan cumplir con la aprobación de los viáticos correspondientes.

El señor Presidente, indica que una vez realizada la consulta, el señor Vicepresidente Lizama Hernández y el señor Director Monge Rojas, estarían asistiendo al Encuentro Empresarial, que se llevará a cabo en Liberia Guanacaste,

por lo que somete a votación la aprobación de los viáticos y de la logística correspondiente.

COMUNICACIÓN DE ACUERDO AC-145-2014-JD

CONSIDERANDO:

1. Que el señor Director Jorge Muñoz Araya, se refiere a la invitación al acto inaugural del FORO ECONÓMICO EMPRESARIAL GUANACASTECO, INA 2014, el cual se llevará a cabo el próximo jueves 19 de junio del presente año, en la Unidad Regional Chorotega.

2. Que el señor Muñoz Araya informa que él no podrá asistir a dicho evento, pero que considera que es importante que los miembros de la Junta Directiva que puedan asistir al mismo, se les autorice los viáticos respectivos

POR TANTO:

SE ACUERDA POR UNANIMIDAD DE LOS DIRECTORES PRESENTES A LA HORA DE LA VOTACIÓN:

PRIMERO: APROBAR LA PARTICIPACIÓN DE LOS SEÑORES DIRECTORES QUE PUEDAN ASISTIR AL ACTO INAUGURAL DEL **"FORO ECONÓMICO EMPRESARIAL GUANACASTECO, INA 2014",** A REALIZARSE EL PRÓXIMO 19 DE JUNIO DEL PRESENTE AÑO, EN LA UNIDAD REGIONAL CHOROTEGA.

SEGUNDO: AUTORIZAR LOS GASTOS DE VIÁTICOS Y UTILIZACIÓN DE TRANSPORTE INSTITUCIONAL, DE LOS DÍAS 18 Y 19 DE JUNIO DE 2014, E INSTRUIR A LA SECRETARÍA TÉCNICA DE LA JUNTA DIRECTIVA PARA QUE REALICE LAS ACCIONES CORRESPONDIENTES EN CUANTO A LA LOGÍSTICA DE DICHA GIRA.

ACUERDO APROBADO EN FIRME POR UNANIMIDAD

El señor Director Montero Jiménez, consulta si es posible que se pueda trasladar o cambiar el día en que se realizan las sesiones de Junta Directiva, de manera que no sean los lunes, debido a que tiene problemas de agenda.

El señor Presidente, menciona que las sesiones son los días lunes a las 5 de la tarde y la de hoy se realizó miércoles, por motivo de que los Directores se juramentaron hasta el día de ayer.

El señor Director Montero Jiménez, consulta cuál es el procedimiento para informar que no puede venir el próximo lunes a la Sesión, en virtud de que tiene que salir del país.

El señor Presidente, indica que no considera que se tenga problema por ser solo un lunes el que no puede asistir y en ese caso, se le comunica al señor Secretario Técnico, para que tome nota.

El señor Director Esna Montero, menciona que en la Sesión del 26 de mayo, se tomó un acuerdo en el sentido de que se les trajera un informe sobre la situación que se dio con la supuesta estafa de los 80 millones en contra del INA, el mismo debió presentarse el día 9 de junio, pero en virtud de que no hubo sesión, debió presentarse hoy y no lo ve dentro del Orden del Día de hoy, por lo que consulta cuándo se traerá la información.

El señor Gerente General, señala que le el informe ya fue enviado, por lo que le extraña la situación, en ese caso solicitaría que se le dé la oportunidad de verificarlo, en caso de que no haya entrado a la Secretaría, estaría trayéndolo para el próximo lunes.

El señor Presidente, somete a votación la propuesta para que se traiga para el próximo lunes, el informe de la supuesta estafa de 80 millones, en contra del INA.

COMUNICACIÓN DE ACUERDO AC-146-2014-JD

CONSIDERANDO:

1. Que mediante acuerdo AC-130-2014-JD, con fecha 26 de mayo de 2014, se acordó, con base en la moción presentado por el Director Tyronne Esna Montero, que la Gerencia General presentara a la Junta Directiva, **en la sesión del 9 de junio de 2014**, el informe solicitado en el acuerdo número AC-025-2014-JD, de fecha 27 de enero de 2014, referente a la supuesta estafa de 80 millones en perjuicio del INA.

2. Que el Director Tyronne Esna Montero, indica que como no hubo sesión el pasado 9 de junio, tampoco se incluyó dentro del Orden del Día de la presente sesión, por lo que nuevamente solicita que se dé cumplimiento al acuerdo de marras.

3. Que el Gerente General informa que dicho informe ya está listo, por lo que se va a presentar en la próxima sesión.

POR TANTO:

SE ACUERDA POR UNANIMIDAD DE LOS DIRECTORES PRESENTES A LA HORA DE LA VOTACIÓN:

ÚNICO: QUE LA GERENCIA GENERAL PRESENTE A LA JUNTA DIRECTIVA, **EN LA SESIÓN DEL PRÓXIMO 16 DE JUNIO DE 2014**, EL INFORME SOLICITADO EN EL ACUERDO NÚMERO AC-130-2014-JD, DE FECHA 26 DE MAYO DE 2014.

ACUERDO APROBADO EN FIRME POR UNANIMIDAD

El señor Director Muñoz Araya, comenta que dentro de los informes pendientes, está el de la situación de riesgo de la Sede del INA en Barranca, que está a la par de una planta que se llama INOLASA, en ese sentido, la Junta Directiva solicitó que se hiciera un plan de mitigación, que contemplara una serie de aspectos, que en caso de una catástrofe, se pudiera tener el mínimo riesgo para los funcionarios que laboran en ese Centro.

Agrega que a pesar de que ya debió haberse entregado el informe, no le tienen todavía, lo cual le preocupa por la responsabilidad que tiene la Junta Directiva, porque ya tienen conocimiento de que hay una situación de riesgo, por lo que solicitaron que se hiciera este plan, para el caso de algún riesgo que se pueda tener.

El señor Secretario Técnico, indica que el informe al que se refiere el señor Director Muñoz Araya, ya está en la Secretaría y le quedaría verificar si el informe al que hace alusión el señor Director Esna Montero, sobre la supuesta estafa, se recibió en la Secretaría.

Asimismo, desea comentar con todo respeto a los señores Directores, que se hizo una acumulación de temas de Agenda, por motivo de la falta de Quórum estructural que motivó que no se realizaran las sesiones.

En ese sentido, las unidades han seguido enviando puntos para Agenda, por lo que le sugirió al señor Presidente Ejecutivo, que se pudiera realizar una Sesión Extraordinaria, aparte de la que se ha conversado para ver el tema CATEAA, a efecto de poner al día los temas que están pendientes y que son muchos.

En ese sentido solicita comprensión, porque pueden haber algunos plazos vencidos a juicio de los señores Directores, relacionados con acuerdos de Junta Directiva y que se ha dado por los motivos señalados, por lo que se han ido incluyendo por orden de prioridad Institucional.

El señor Presidente, señala que el acuerdo sería solicitarle al Secretario Técnico, que incluya en la Agenda lo señalado por el señor Director Muñoz Araya, sobre el tema de la Sede de Barranca, con la petición de que se tenga el cuidado de no saturar las siguientes agendas.

El señor Director Esna Montero, considera que si hay temas que están pendientes y que quedaron con una fecha de cumplimiento, al menos se les debería informar a los señores Directores, porque los acuerdos se deben cumplir en las fechas señaladas.

Indica que es una consigna de la Junta Directiva, el hecho de que los acuerdos se van a seguir cumpliendo en la fecha señalada y es por eso que a todas las decisiones que se toman se les señala el plazo. En caso de que no se pueda cumplir con la fecha, se debe solicitar la prórroga correspondiente.

El señor Director Montero Jiménez, señala que comparte plenamente el hecho de que es discrecionalidad del jerarca, si ve un asunto o no, considera que no puede ser de otra manera.

El señor Presidente, somete a votación que el señor Secretario Técnico agende los temas que sean posibles y de quedar algunos pendientes, que les informe previamente, para tener la claridad de los temas que quedarán para verse en sesiones posteriores.

COMUNICACIÓN DE ACUERDO AC-147-2014-JD

CONSIDERANDO:

ÚNICO: Que el Presidente Ejecutivo mociona para que el Secretario Técnico de la Junta Directiva incluya dentro del Orden del Día de la próxima sesión, los temas que sean posibles de presentar ante ese órgano colegiado, teniendo en cuenta el interés concreto de varios señores directores y el vencimiento de los plazos, como consta en actas, e informar sobre aquellos que queden pendientes.

POR TANTO:

SE ACUERDA POR UNANIMIDAD DE LOS DIRECTORES PRESENTES A LA HORA DE LA VOTACIÓN:

ÚNICO: QUE EL SECRETARIO TÉCNICO DE LA JUNTA DIRECTIVA INCLUYA DENTRO DEL ORDEN DEL DÍA DE LA PRÓXIMA SESIÓN, LOS TEMAS QUE SEAN POSIBLES DE PRESENTAR ANTE ESE ÓRGANO COLEGIADO, TENDIENDO EN CUENTA EL INTERÉS DE LOS DIRECTORES, COMO CONSTA EN ACTAS, ASÍ COMO EL VENCIMIENTO DE LOS PLAZOS E INFORMAR SOBRE AQUELLOS TEMAS QUE QUEDEN PENDIENTES.

ACUERDO APROBADO EN FIRME POR UNANIMIDAD

El señor Vicepresidente Lizama Hernández, consulta si se vio en Junta Directiva el informe de la gira que realizaron a la zona Sur, o solamente se remitió.

La señora Subgerente Administrativa, responde que se remitió.

El señor Vicepresidente Lizama Hernández, menciona que le llamó la atención que una de las primeras giras que realizó el señor Presidente de la República, fue a la zona Sur, particularmente a Golfito y Puerto Jiménez, que son zonas que personalmente le motivan mucho, porque cree que tienen un gran potencial de desarrollo, no solo turístico sino en otros ámbitos también, pero que lamentablemente llevan muchos años en una situación de abandono y deterioro.

Por esa razón, le gustó mucho el hecho del énfasis que el señor Presidente de la República, le quiere dar al desarrollo de esas zonas periféricas, que tienen los más bajos índices de desarrollo comparativo en el país.

Indica que este tema coincidió con la última gira que hizo esta Junta Directiva, hace cerca de dos meses, a toda la zona Sur, incluyendo Golfito, donde lograron identificar una serie de hechos o hallazgos, que permiten determinar un plan de acción por parte del INA, para mejorar su presencia en la zona.

Agrega que en la gira se identificaron una gran cantidad de oportunidades, y eso está muy bien reflejado, en el informe que hizo la señora Subgerente Administrativa, quien les acompañó en esa oportunidad.

Comenta que uno de los temas que se menciona en el informe, es que la parte Náutico-pesquera- náutico-deportiva y turística, en lugar de estar en Golfito, el INA

la tiene en Río Claro, a bastantes kilómetros de distancia, lo cual tiene el agravante de que las embarcaciones, al tener que estar recorriendo unos caminos muy malos, se deterioran mucho más allá, porque no están hechas para andar por caminos llenos de huecos, sino para navegar.

Señala que incluso algunos motores, ni siquiera han sido sacados de las cajas, precisamente porque no hay instalaciones adecuadas en Río Claro para esos fines. Asimismo, un agravante mayor todavía, es que de las seis lanchas que tienen, hay tres que no han podido echarse al agua porque no tienen la patente, porque supuestamente la Asesoría Legal del INA, tiene ese trámite pendiente desde hace dos o años, por lo que todavía no tienen patente.

Acota que todo esto muestra que se tienen recursos, pero que hay que ponerlos en el lugar que corresponde y es un ejemplo de las muchas cosas, que se podrían hacer en la zona Sur por parte del INA, para apoyar su desarrollo, por lo que estaría mocionando, para que se aborde este tema como Junta Directiva y que como punto de partida, se reciba el informe de la señora Subgerente Administrativa en una sesión, sobre la gira que realizaron a la Zona Sur.

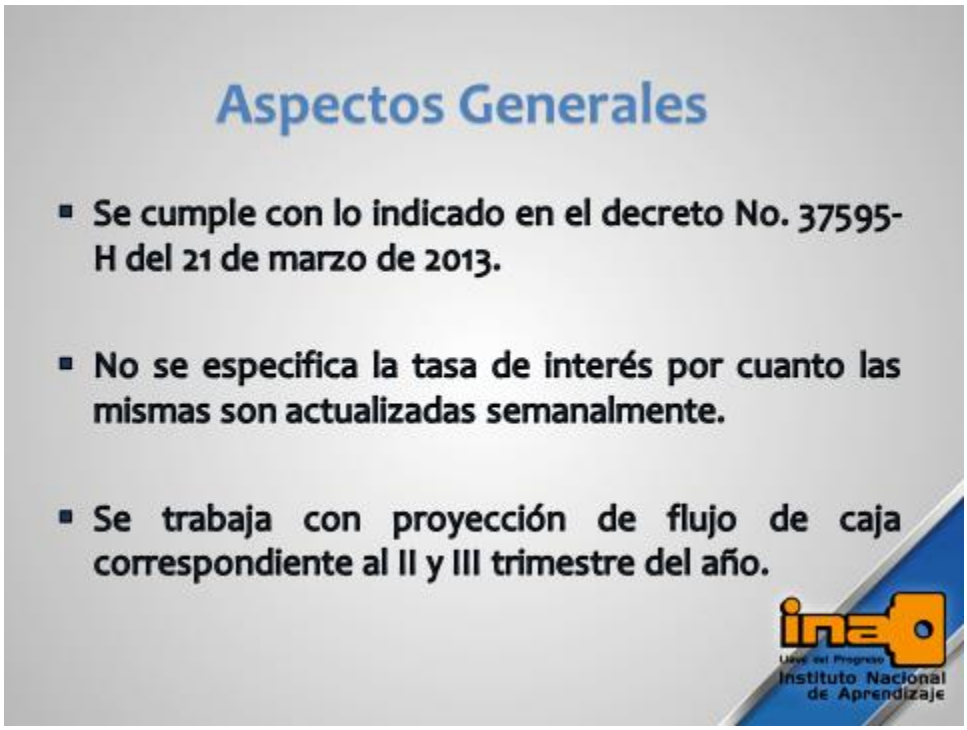
La señora Subgerente Administrativa, indica que ya el informe fue enviado a la Junta Directiva, incluso se podría actualizar, porque ya se han hecho acciones, como el diagnóstico a nivel de Salud Ocupacional, para algo específico que se vio en esa gira, incluso se está extendiendo el diagnóstico para otros Centros.

ARTÍCULO SEXTO:

Unidad de Recursos Financieros. Oficio URF-398-2014. Vencimiento de Título de Inversión.

El señor Presidente, somete a consideración de la Junta Directiva el tema que será presentado por la señora Mayela Vargas, Encargada del Proceso de Tesorería.

La señora Vargas, procede con la presentación de acuerdo con las siguientes filminas:


Aspectos Generales
Se cumple con lo indicado en el decreto No. 37595-H del 21 de marzo de 2013.
No se especifica la tasa de interés por cuanto las mismas son actualizadas semanalmente.
Se trabaja con proyección de flujo de caja correspondiente al II y III trimestre del año.
Instituto Nacional de Aprendizaje


Fuentes de información
Requerimiento de fondos de:
La Gestión Regional
Unidad de Recursos Humanos
Proceso de Adquisiciones Sede Central
Unidad de Servicio al Usuario
Proyecciones de Ingresos:
Proceso de Presupuesto
Instituto Nacional de Aprendizaje

Flujo de caja proyectado

Resumen de efectivo	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE
Saldo inicial de caja	16.659.212.911	17.399.649.330	18.628.628.823	12.082.897.052	13.424.266.480	9.268.358.187
Total Ingresos	6.089.871.163	6.443.429.115	13.781.647.942	6.565.715.273	16.874.190.515	6.565.715.273
Contribuciones Sociales	6.005.157.268	6.288.834.377	6.411.120.535	6.411.120.535	6.411.120.535	6.411.120.535
Ingresos no tributarios	84.713.895	154.594.738	154.594.738	154.594.738	154.594.738	154.594.738
Vencimiento de Inversiones			7.215.932.669		10.308.475.242	
Total Egresos	5.349.434.744	5.214.449.621	20.327.379.713	5.224.345.846	21.030.098.807	5.812.738.522
Remuneraciones	3.360.810.768	3.360.810.768	3.360.810.768	3.360.810.768	3.360.810.768	3.360.810.768
Servicios	1.305.830.033	1.095.119.291	1.088.610.813	981.669.013	1.140.817.096	1.390.365.098
Materiales y suministros	327.204.648	407.519.562	495.017.162	527.921.065	564.619.329	472.102.656
Bienes duraderos	5.589.295	1.000.000	32.940.970	3.945.000	613.851.614	239.460.000
Transferencias corrientes	350.000.000	350.000.000	350.000.000	350.000.000	350.000.000	350.000.000
Inversiones			15.000.000.000		15.000.000.000	
Saldo final de caja	17.399.649.330	18.628.628.823	12.082.897.052	13.424.266.480	9.268.358.187	10.021.334.938

Instituto Nacional de Aprendizaje

Propuesta de reinversión

Fecha de Emisión	13 de junio 2014
Fecha de vencimiento	17 de marzo 2015
Plazo en días	274
Monto	¢15.000.000.000,00

Instituto Nacional de Aprendizaje

El señor Presidente, menciona que verificaron que aún no ha sido publicado en el Diario Oficial La Gaceta su nombramiento, por lo que consulta al señor Asesor Legal si al hacer este tipo de inversiones, su firma está debidamente avalada.

El señor Asesor Legal, indica que si bien es cierto la publicación es para efectos de terceros, hay trámites que por la urgencia, se acepta una certificación notarial del acuerdo del Consejo de Gobierno, en el cual fue juramentado. Obviamente por seguridad jurídica con terceras personas, sí es necesario el tema de la publicación.

En este caso, no ve que el tema pueda ser afectado por una situación de este tipo.

El señor Presidente, consulta a la señora Auditora si desde el punto de vista de la Auditoría podría existir algún problema.

La señora Auditora Interna, responde que no.

El señor Presidente, agradece a la señora Vargas por la presentación. Se retira del Salón de Sesiones.

Somete a votación de la Junta Directiva, el contenido del Oficio URF-398-2014, sobre Vencimiento de Título de Inversión.

COMUNICACIÓN DE ACUERDO AC-148-2014-JD

CONSIDERANDO:

1. Que mediante oficio URF-398-2014, la Unidad de recursos Financieros, remite para conocimiento y eventual aprobación por parte de los miembros de la Junta Directiva, la propuesta de reinversión del TÍTULO DE INVERSIÓN.

2. Que la señora Mayela Vargas Cascante, de Proceso de Tesorería, de la Unidad de Recursos Financieros, expone ante los miembros de la Junta Directiva presentes, los alcances de la propuesta de reinversión antes descrita.

3. Que la señora Vargas Cascante, indica que se está cumpliendo con lo indicado en el decreto **No. 37595-H del 21 de marzo 2013,** el cual establece que las inversiones o reinversiones de activos financieros se harán únicamente con títulos de deuda interna del Gobierno emitidos por el Ministerio de Hacienda, y que no se indica una tasa de interés porque las mismas varían de forma semanal, y que se está trabajando con una proyección de flujo de caja correspondiente al segundo y tercer trimestre del presente año.

4. Que la propuesta de inversión sería por la suma de QUINCE MIL MILLONES DE COLONES EXACTOS (₡15.000.000.000,00), a partir del 13 de junio del presente año, con una fecha de vencimiento al 17 de marzo de 2015 y con un plazo de 274 días.

5. Que los miembros de la Junta Directiva realizan un análisis de la inversión solicitada y expresan sus comentarios, con el objeto de buscar las mejores y seguras inversiones para la Institución.

POR TANTO:

POR UNANIMIDAD DE LOS MIEMBROS PRESENTES SE ACUERDA:

ÚNICO: APROBAR LA REINVERSIÓN DEL TÍTULO INVERSIÓN POR UN MONTO DE **¢15.000.000,000,00** (*QUINCE MIL MILLONES DE COLONES EXACTOS*), DE CONFORMIDAD CON LO EXPUESTO POR LA SEÑORA MAYELA VARGAS CASCANTE, DEL PROCESO DE TESORERÍA, SEGÚN OFICIO URF-398-2014 Y LO QUE CONSTA EN ACTAS, BAJO LAS SIGUIENTES CONDICIONES:

ACUERDO APROBADO EN FIRME POR UNANIMIDAD

ARTÍCULO SÉTIMO:

Subgerencia Administrativa. Oficio SGA-309-2014. Trámite para la autorización de viáticos en el interior del país, para la Presidencia Ejecutiva, de conformidad con al Art. 7 del Reglamento de Gastos de Viaje y Transporte para Funcionarios Públicos de la Contraloría General de la República, y en atención al criterio emitido por la Asesoría Legal, mediante oficio ALEA-266-2014.

El señor Presidente, solicita al Secretario Técnico que se refiera al tema.

El señor Secretario Técnico, indica que la Secretaría Técnica ha tenido a la vista la documentación presentada, en la cual se encuentra un oficio de la Asesoría Legal, el cual es sumamente claro, en el sentido de que la responsabilidad de efectuar esta autorización por gastos de viajes, realizados por el Presidente Ejecutivo en el interior del país y las respectivas liquidaciones, está a cargo del órgano superior de la Administración que es la Junta Directiva, sin embargo, esa competencia puede ser delegada en otro funcionario de la Institución.

Agrega que para efectos prácticos, se ha sugerido que esta competencia esté asignada al Director del Despacho de la Presidencia Ejecutiva. En ese sentido, se ha preparado un proyecto de borrador de acuerdo, en el cual se indica concretamente que la Junta Directiva, acuerda delegar en el Director de Despacho de la Presidencia Ejecutiva, las autorizaciones previas, así como las liquidaciones correspondientes, sobre los gastos de viaje que el Presidente Ejecutivo realice en el interior del país, todo de conformidad con el oficio ALEA-266-2014, del 27 de mayo del 2014.

El señor Director Solano Cerdas, menciona que no es por desconfianza, pero desea saber si esa cercanía del Jefe de Despacho con el Presidente Ejecutivo, eventualmente pueda representar algún problema.

El señor Director Esna Montero, consulta cómo se estilaba anteriormente.

El señor Asesor Legal, responde que lo que se estilaba era que para efectos de control, de que no sea el mismo Presidente Ejecutivo quien se autorizaba y aprobaba la liquidación de viáticos, que es un tema meramente administrativo, se encargaba a una persona diferente, así se venía haciendo en la práctica.

Sin embargo, a raíz de una consulta que hace el Proceso de Tesorería, en el cual la Asesoría Legal revisa a fondo el tema y se determina que la Contraloría General de la República, señala que debería ser la Junta Directiva o quien delegue.

Menciona que obviamente, el tema de la delegación es muy importante, porque es una aspecto meramente administrativo, lo que implica que si el Presidente Ejecutivo, el día de mañana desea hacer una gira, no va a tener derecho a cobrar viáticos o hacer liquidaciones posteriores.

Reitera que es un tema meramente administrativo y era eso lo que se acostumbraba.

El señor Director Esna Montero, comenta que no recuerda que en los últimos cuatro años, la Junta Directiva haya aprobado algo, para darle la funcionalidad a alguna persona, ya sea jefe de despacho, secretaria, es decir absolutamente a nadie, es por eso que consultó como era que se realizaba anteriormente.

El señor Asesor Legal, reitera que esto obedece a una consulta que realizó el Proceso de Tesorería hace semana y media o dos, en realidad es hasta este momento que se empieza aplicar en la Institución.

Señala que antes lo aprobaba una persona diferente al Presidente Ejecutivo, como lo comentó anteriormente.

El señor Presidente, indica que la consulta del señor Director Solano Cerdas, se quedó sin responder, la cual era que si la cercanía del Presidente Ejecutivo y del Jefe de Despacho tiene algún problema.

El señor Asesor Legal, responde que esta es una situación muy "Sui géneris", que se presenta en materia administrativa, ya que todos tienen claro que el superior jerárquico del Presidente Ejecutivo, es el Consejo de Gobierno que lo nombra.

En ese aspecto, es obvio que el Consejo de Gobierno, no va estar autorizando los vales por viáticos, cada vez que el señor Presidente Ejecutivo sale en razón de su función, es ahí que la Contraloría General de la República, interpreta que debe ser el jerarca de la institución, que este caso es la Junta Directiva, es como una jerarquía impropia, como se podría llamar.

En este sentido, como es un tema meramente administrativo, no le ve inconveniente porque por ejemplo, para efectos de salir del país, la autorización debe ser dada por la Junta Directiva, y de lo que se trata en este caso, en más que todo para la aprobación y liquidación de viáticos, para las giras que realice el señor Presidente Ejecutivo, a lo interno del país.

El señor Presidente, menciona que es importante destacar que en el INA, para todo movimiento hay un sistema automatizado, es decir se lleva un control detallado de cada trámite.

Somete a votación, que se delegue en la señora Eva Papili, Jefa de Despacho de la Presidencia, para que sea la que realice la autorización de los viáticos y la liquidación de gastos, a lo interno del país, para el señor Presidente Ejecutivo.

El señor Asesor Legal, indica que está bien que mencionara el nombre de la Jefa de Despacho, pero para efectos del acuerdo, es mejor dejar el cargo específico únicamente, porque la persona puede cambiar.

El señor Presidente, señala que entonces quedaría consignado que se delega en el Jefe de despacho o el director de despacho de la Presidencia Ejecutiva.

El señor Director Montero Jiménez, acota que es importante que se redacte en términos de género, es decir “La persona que ocupa la”, por si es hombre o mujer tampoco interfiera con el acuerdo.

La señora Auditora Interna, indica que se puede agregar en la comunicación, que todo de acuerdo con los procedimientos institucionales, en materia de viáticos.

El señor Presidente, indica que efectivamente e incluso en materia de presupuesto, porque no puede haber viáticos, si el presupuesto se agota.

COMUNICACIÓN DE ACUERDO AC-149-2014-JD

CONSIDERANDO:

1. Que el Secretario Técnico de Junta Directiva hace mención sobre el criterio de la Asesoría Legal, basado en pronunciamientos de la Contraloría General de la República, según consta en el oficio ALEA-266-2014, de fecha 27 de mayo de 2014, en el cual se indica que la competencia para autorizar los viáticos de la Presidencia Ejecutiva en el interior del país y las respectivas liquidaciones, está localizada jurídicamente en la Junta Directiva del INA.

2. Que continúa indicando el señor Secretario, que sin embargo, la Junta Directiva puede delegar dicha competencia, como lo indica el mismo dictamen legal, en otro funcionario de la Institución, y es por esa razón que, para efectos prácticos, se sugiere que la misma sea asignada al Director del

Despacho de la Presidencia Ejecutiva, mediante un acuerdo de Junta Directiva.

3. Que los señores Directores presentes analizan y realizan sus consultas al Asesor Legal sobre los alcances de dicha propuesta, con el fin de tomar una decisión y no afectar los trámites de adelantos y liquidaciones de gastos de viaje dentro del país que deba realizar el Presidente Ejecutivo.

POR TANTO:

POR MAYORÍA DE LOS MIEMBROS PRESENTES SE ACUERDA:

ÚNICO: DELEGAR EN LA PERSONA QUE OCUPA EL CARGO DE DIRECCIÓN DE DESPACHO DE LA PRESIDENCIA EJECUTIVA, LAS AUTORIZACIONES PREVIAS, ASÍ COMO LAS LIQUIDACIONES CORRESPONDIENTES SOBRE LOS GASTOS DE VIAJE QUE EL PRESIDENTE EJECUTIVO REALICE EN EL INTERIOR DEL PAÍS, TODO DE CONFORMIDAD CON EL CRITERIO LEGAL QUE CONSTA EN EL OFICIO ALEA-266-2014 DE FECHA 27 DE MAYO DE 2014.

ACUERDO APROBADO EN FIRME POR MAYORÍA

SE ABSTIENE DE VOTAR EL PRESENTE ACUERDO EL SEÑOR MINOR RODRÍGUEZ RODRÍGUEZ, PRESIDENTE EJECUTIVO.

ARTÍCULO OCTAVO:

Subgerencia Administrativa. Oficio SGA-284-2014. Propuesta de modificación del Reglamento uso de Recursos Informáticos.

El señor Presidente, somete a consideración de la Junta Directiva, el tema que será presentado por el señor Gustavo Ramírez de la Peña, Gestor de Tecnologías de Información.

El señor Ramírez de la Peña, procede con la presentación de acuerdo con las siguientes filminas:

Gestión de Tecnologías de Información y Comunicación

Reglamento de uso de Recursos Informáticos

GTIC

Instituto Nacional de Aprendizaje

Los cambios se realizan de acuerdo a lo indicado por:

- ✓ La Auditoría Interna en su Informe 46-2011 recomendación No. 3 .
- ✓ Observaciones de Auditoría oficio AI-00199-2013
- ✓ Manual de Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE).
- ✓ Estructura actual de la GTIC (ajuste por competencias)
- ✓ Lenguaje incluyente

GTIC

Instituto Nacional de Aprendizaje

Observaciones de Auditoría AI-00199-2013

- Artículo 1, 2 y 3
- Artículo 4, inciso 13 y 14
- Artículo 6, inciso 5
- Artículo 7, inciso 9
- Artículo 13, inciso 2

GTIC

Instituto Nacional de Aprendizaje

Observaciones de Auditoría AI-00199-2013

- Artículo 13, inciso 7
- Artículo 14, inciso 4
- Artículo 17, inciso 1
- Artículo 29

GTIC

Instituto Nacional de Aprendizaje

Manual de Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE).

- Artículo 3 Definiciones y Nomenclaturas:
  Acuerdo de confidencialidad
  Confidencialidad
  Disponibilidad de la información
  Dispositivos móviles
  Hardware
  Integridad.

GTIC

- Artículo 3, 4, 6, 7 y 9

GTIC

- Artículos 2, 3, 4, 6 al 18, 20 al 32

GTIC

Reglamento de uso de Recursos Informáticos

GTIC

El señor Ramírez, señala que el Reglamento vigente, dice que el objetivo del mismo, *"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".*

En ese sentido, la Auditoria Interna consideró, que se debía ampliar ya que estaba muy general y que era necesario establecer, que existen diferentes tipos de usuario, por lo que quedó consignado que *"el Objetivo el presente reglamento, tiene como finalidad normar el uso de los recursos, de los servicios informáticos y los servicios de red, que están a disposición de las personas funcionarias, para su utilización en actividades adjetivas y sustantivas"*

Indica que en el artículo 2, lo que originó la modificación se pone en dos colores, para distinguir la fuente u origen de la modificación, este es un poco el alcance y le dan la razón a la posición de la Auditoría, en el sentido de especificar un poco más, ya que hablaba solo de los usuarios.

El este caso, el ámbito de acción se modificó de manera que dijera que en *"Lo enunciado en el presente Reglamento, es aplicable tanto para las personas usuarias finales, como para las personas técnico-informáticas, así como de las personas proveedoras de los recursos y servicios informáticos. Será responsabilidad de las personas citadas anteriormente, cumplir lo aquí estipulado"*

El fundamento de la modificación en este artículo, hablaba de los usuarios de los recursos, pero el uso que le da un informático que trabaja en planta con ellos, es diferente al uso que le da una secretaria o un usuario de un sistema, es necesario realizar esa separación por los ámbitos de competencia para cada uno de esos y los privilegios que tienen sobre el manejo de información son diferentes.

Menciona que el artículo es importante y el aporte de la Auditoria Interna, ya que establece que debe existir una diferenciación. Como lo indicó antes, no es el mismo uso que se vaya a dar, sobre los recursos que tiene en la Institución un tercero, o sobre el uso que se haga sobre ellos mismos, que se tienen las bases de datos los recurso de red, ese en particular le llamó la atención y le parece atinada la posición de la Auditoria Interna.

El señor Viceministro de Educación Pública, consulta si las observaciones de la Auditoría Interna, se tomaron en cuenta y se incorporaron a las modificaciones que se realizaron.

El señor Ramírez de la Peña, responde que sí y que se aplicaron al 100% las observaciones de la Auditoría.

El señor Presidente, consulta si la nueva versión con las modificaciones, ya las tiene la Auditoría Interna.

El señor Ramírez de la Peña, responde que aún no han sido enviadas.

El señor Director Esna Montero, consulta si esto tiene el visto bueno de la Asesoría Legal.

El señor Ramírez de la Peña, responde que sí.

El señor Director Montero Jiménez, consulta a la señora Auditora Interna si pudo observar el documento.

La señora Auditora Interna, aclara que la Auditoría Interna dentro de las competencias, no tienen obligación de revisar la reglamentación previo a la aprobación. En ese sentido, se ha acostumbrado a nivel Institucional, hacer una colaboración en temas de fondo que consideren relevantes, sin entrar mucho a la toma de decisiones, con respecto a los temas.

Asimismo, debe señalar que le preocupaba en este caso y así se lo comentó a la señora Subgerente Administrativa, que desde la última vez que había venido este Reglamento a la Junta Directiva, hasta el día de hoy e incluso posterior a que la Auditoria Interna, realizara estas observaciones, faltaba la revisión legal del Reglamento y que no tenía conocimiento la Auditoria, si había surgido alguna nueva normativa que afectara y les parece que pueda ser que haya surgido, con el tema de la ley de Protección de Datos, por ejemplo, o la Ley de Firma Digital, entre otras, que han surgido últimamente, y que las activadas de Gobierno Digital, vayan encaminadas a ir avanzando en esos temas y no sabe hasta qué nivel se está regulando con el nuevo Reglamento.

En ese sentido, trasladaría la consulta a la Administración, haciendo la reserva de la Auditoria Interna, para referirse a los temas en un proceso de fiscalización.

La señora Subgerente Administrativa, indica que en la Comisión Gerencial de Informática, se está revisando todo lo que tenga que ver con la Ley de Protección de Datos, incluso existe un pronunciamiento legal de la Asesora Legal de la Subgerencia Administrativa, que indica que la Ley como está escrita, está más

ligada a la parte financiera, pero en el INA ya se tomaron las previsiones del caso y están determinando cuáles son los tipos de documentos y de información que tiene que ser resguardada.

Señala que se van a revisar tres cosas, que consideran la recomendación que realiza la señora Auditora Interna, que son muy importantes, una es que se aparte de la Ley de Protección de Datos que ya fue vista, y como ha pasado algún tiempo, y ha salido alguna regulación, normativa o ley nueva que no hayan considerado, por lo que se comprometen a realizar la revisión inmediatamente y notificaran si es necesario traerlo nuevamente.

Asimismo, otra de las cosas es el correo, en este momento tienen un correo en la nube, que es un correo solo para estudiantes, por lo que se deberá revisar esa parte en la protección del conocimiento.

Comenta que otra de las cosas, es todo lo que tiene que ver con tema de la firma digital, y están muy esperanzados de que se pueda entrar a trabajar con MERLINK pronto.

Indica que se compromete junto con el señor Ramírez de la Peña, a hacer la revisión en esos tres aspectos y si no es necesario, se enviaría mediante oficio firmado a la Junta Directiva, para que el Reglamento salga, y si hay algún cambio inmediatamente se traería en el corto tiempo, ya que el Reglamento es una herramienta, que es necesaria para el INA.

La señora Auditora Interna, señala que comprende que la parte de la tecnología avanza vertiginosamente en estos días, y que es prácticamente imposible contemplar el 100% de las cosas en un instrumento, en ese sentido, no quiere atrasar el proceso de aprobación de la reglamentación.

Sin embargo, desea que quede planteado, que hay temas que siguen faltando por revisar, y entre ellos está el hecho de que la información en este tiempo, se considera un activo en la Administración, y así lo disponen las NICSP, las Normas de Contabilidad para el Sector Público, que entiende que su implementación, es todo un proceso que finaliza hasta el año 2016, pero que son temas que se deben ir discutiendo, por lo que debe tomarse en la Administración, las decisiones de hacer un corte, y ver qué se va incluir y qué se va ir incluyendo con fechas y planes de trabajo, acordes a las necesidades institucionales.

El señor Presidente, acota que con la rapidez que cambian los temas tecnológicos en este tiempo, debería haber un artículo final, que diga que los que no estén contemplados en este Reglamento, deberán ser regulados de otra forma, porque de pronto hay tantas opciones, como por ejemplo, que se puede tener acceso con el celular, a las diferentes plataformas del INA, entonces cómo regular el uso de los recursos tecnológicos y que quede blindado el INA ante posibles abusos o fallas.

El señor Asesor Legal, explica que no se puede redactar un artículo en ese sentido, y aclara que cuando la Asesoría Legal revisa el Reglamento, lo hacen

porque se reglamenta lo que la Institución tiene, por ejemplo, cuando se habla de la Firma Digital, hay un Reglamento en la Institución de Firma Digital, que incluso es muy viejo.

En ese aspecto, la Contraloría General de la República, pasó un tema en el sentido de si en el INA existe la firma digital, y no existe, por lo tanto no se tienen certificaciones afuera y no todo el mundo las tiene, las tiene ciertas personas como por ejemplo Allan Altamirano de Adquisiciones, que necesita acceder a la Imprenta Nacional y lo que pasa es que se toma una foto en un momento determinado y eso es lo que se regula.

En ese sentido, hay muchas leyes tal y como lo señala la señora Auditora Interna, que a futuro van a establecer mecanismos, pero primero se tienen que hacer los ajustes técnicos, para poder reglamentarlo en ley o en reglamentos.

En el caso de los móviles, hay todo un capítulo sobre lo que es el sistema de seguridad, el acceso a las plataformas, uso del celular, accesos a través de WI-FI, es decir este tipo de situaciones está reglamentado.

Agrega que si se lee el Reglamento, se ve que es bastante extenso, porque desmenuza mucho las posibles opciones, de lo que se tiene hoy en día en sistemas.

El señor Presidente, consulta si con este Reglamento se le da una protección suficiente a los recursos.

El señor Ramírez de la Peña, responde que es una protección razonable, y como lo apunta el señor Asesor Legal, lo importante en esto es que conforme salgan, se norme todo lo que tienen al día de hoy, y conforme salgan las nuevas cosas, tener la capacidad de reacción y la oportunidad de ir implementando los controles que se requieran.

En ese sentido, es difícil poner un control para una cosa que se va a materializar a futuro, en esa parte si hay una dificultad tácita, pero el Reglamento es muy extenso, cree que tiene muchas de las cosas muy protegidas, tiene sanciones, muchos artículos e incisos orientados para tal fin.

El señor Presidente, agradece al señor Ramírez de la Peña por la presentación. Se retira del Salón de Sesiones.

El señor Asesor Legal, recomienda que por tratarse de un Reglamento tan amplio y los reglamentos posteriormente se deben publicar en la Gaceta y quedan exactamente como irían en el acuerdo, prefiere que no quede en firme, para poder revisar que no exista ningún error y que la Junta Directiva lo pueda corroborar y con la aprobación del acta lo tendrían totalmente claro.

Menciona esto, porque si hubiese algún error, habría que traerlo a modificar por lo que piensa que esperar una semana, no tiene ningún problema.

El señor Presidente, somete a votación las modificaciones del Reglamento uso de Recursos Informáticos.

COMUNICACIÓN DE ACUERDO AC-150-2014-JD

CONSIDERANDO:

1. Que mediante oficio SGA-284-2013, la Subgerencia Administrativa remite para conocimiento y eventual aprobación por parte de la Junta Directiva, la propuesta de modificación al **"Reglamento Uso de Recursos Informáticos".**

2. Que el señor Gustavo Ramírez de la Peña, Gestor de Tecnologías de Información y Comunicación, expone ampliamente cada modificación propuesta a los miembros de la Junta Directiva presentes, indicando que dicho Reglamento lo que pretende es normar aspectos tecnológicos y administrativos en el uso de la tecnología, tanto para usuarios finales, técnicos y para terceros que usen la plataforma del INA.

3. Que el señor Ramírez de la Peña informa que el Reglamento está actualmente vigente y que la propuesta de modificación está motivada en las recomendaciones y observaciones que hizo la Auditoría Interna en sus informes números 46 y 199. Así como también, por normas técnicas generadas por la misma Contraloría General de la República.

4. Que la propuesta de modificación al reglamento de marras, en la siguiente:

REGLAMENTO VIGENTE	REGLAMENTO PROPUESTA	MODIFICACIONES	OBSERVACIONES
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.	**CAPÍTULO I: DISPOSICIONES GENERALES** **ARTICULO 1. OBJETIVO** El presente reglamento tiene como finalidad normar el uso de los recursos, de los servicios informáticos y los servicios de red, que está a disposición de las personas funcionarias para su utilización en actividades adjetivas y sustantivas.	Se ajusta según observaciones de Auditoría. AI-00199-2013	
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 2. AMBITO DE ACCION** Lo enunciado en el presente reglamento es aplicable tanto para las **personas usuarias** finales, como para las **personas técnicas** informáticas, así como de las **personas proveedoras** de los recursos y servicios informáticos. Será responsabilidad de las personas citadas anteriormente, cumplir lo aquí estipulado.	Lenguaje incluyente Se ajusta según observaciones de Auditoría. AI-00199-2013	
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	**ARTICULO 3. DEFINICIONES Y NOMENCLATURA** Para el mejor entendimiento de los diferentes artículos descritos en este reglamento, se presentan las siguientes definiciones: **Acceso Remoto: Acceder** 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: Convenio entre empresas y contrato entre las personas**		

secreto, como parte de una relación comercial o laboral.	**funcionarias** que tengan acceso a consulta y/o modificación (crear, actualizar y eliminar) de datos de los servicios informáticos, o bien, entre instituciones que comparten datos o sistemas, para garantizar el manejo discreto de la información. También se utiliza el concepto "cláusulas de confidencialidad", que son aquellas que imponen una obligación negativa: de no hacer o de abstenerse; es decir, de no utilizar la información recibida con fines distintos a los estipulados (véanse los artículos 71 del Código de Trabajo)
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.	**Acuerdo de licenciamiento:** Contrato entre **persona proveedora** debidamente autorizado o entre el fabricante y la institución, 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.	**Administrador de Recursos Informáticos (ARI): Persona funcionaria** técnico informática, designada por la jefatura para administrar los recursos informáticos tanto en la **GTIC** como en Unidades Regionales.
Antivirus: Aplicación o grupo de aplicaciones dedicadas a la prevención, búsqueda, detección y eliminación de programas malignos en sistemas informáticos.	**Antivirus:** Aplicación o grupo de aplicaciones dedicadas a la prevención, búsqueda, detección, bloqueo, desinfección, prevención y eliminación de programas malignos en sistemas informáticos **o en internet.**
Autenticación: Acto de establecimiento o confirmación de la identidad de un usuario como válida.	**Autenticación:** Acto de establecimiento o confirmación de la identidad de una **persona usuaria** como válida.
Autoridades Superiores: Comprende la Junta Directiva, Presidencia Ejecutiva, Gerencia General, Subgerencia Administrativa y	**Autoridades Superiores:**

Subgerencia Técnica.	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.	**Autorizaciones:** Permiso explícito otorgado formalmente por parte de la jefatura de la UO, **o una instancia superior a ésta, siempre y cuando se cumplan con los principios de seguridad de la información de dicha UO.**
Caracteres: Cualquier símbolo en una computadora. Pueden ser números, letras, puntuaciones, espacios, etc.	**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.	**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.	**Clave de usuario:** Contraseña compuesta por un conjunto finito de caracteres que **la persona usuaria** emplea para acceder a un servicio, sistema o programa.
Confidencialidad: Garantía que la información sea accesible sólo para aquellas personas autorizadas.	**Confidencialidad: Protección de la información sensible** contra acceso y divulgación no autorizada.
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.	**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 de **la persona 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 Electrónico:** servicio de red dentro y fuera del INA que permite a las **personas usuarias** enviar y recibir mensajes mediante sistemas de comunicación electrónicos.
Correo masivo: Envío de un mensaje a una gran cantidad de destinatarios.	**Correo masivo:** Envío de un mensaje a una gran cantidad de **personas destinatarias.**
Cuenta: Nombre único que identifica a cada usuario (conocido como login), se autentica mediante una contraseña	**Cuenta:** Nombre único que

(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	identifica a cada **persona usuaria** (conocido como login), se autentica mediante una contraseña (password) **Cuotas de disco:** Espacio de almacenamiento en disco asignado a una **persona usuaria.** **Decodificación:** Proceso inverso para obtener la información en su formato nativo. **Disponibilidad de la Información:** Se vincula con el hecho de que la información se encuentre disponible (v. gr. utilizable) cuando la necesite en un proceso de la organización en el presente y en el futuro. También se asocia con la protección de los recursos necesarios y las capacidades asociadas. Implica que se cuente con la información necesaria en el momento en que la organización la requiere. **Dispositivos Móviles**: son dispositivos de tamaño pequeño, con capacidad de procesamiento y de conexión a una red, con memoria limitada, diseñados específicamente para una función, pero que pueden llevar a cabo otras funciones más generales. **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 o imagen digitalizada:** Transformación o representación electrónica que se puede almacenar y acceder por medio de una computadora.

expresamente, o transmitida por un medio electrónico o informático.	**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.	**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 éstos.
Encriptación: Proceso para codificar la información a un formato más seguro.	**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.	**Firewall:** Elemento del sistema de seguridad de información que es 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.	**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, mediante el Service Desk
Hardware: Corresponde a todos los componentes físicos (tangibles) de una computadora y sus periféricos (impresoras, teclados, enrutadores, switches, etc.).	**<u>GTIC</u>: Gestión de Tecnologías de Información y Comunicación.** **Hardware:** Todos los componentes electrónicos, eléctricos y mecánicos que integren: computadoras, servidores, módems, routers, switches, cableado, cintas, discos, fuentes de poder, dispositivo de almacenamiento (SAN), UPS, en oposición a los programas que se escriben para ella y la controlan (software).
INA: Instituto Nacional de Aprendizaje	**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.	**Incidentes de Seguridad de la Información:** Eventos inesperados que amenazan la seguridad de la

Integridad de la Información: Exactitud y totalidad de la información y los métodos de procesamiento.	información de una organización y comprometen las operaciones de la misma.
Internet: Conjunto de servidores interconectados electrónicamente, integrado por las diferentes redes de cada país del mundo.	**Integridad:** Precisión y suficiencia de la información, así como su validez de acuerdo con los valores y expectativas del negocio.
Intranet (red Interna): Red privada que permite acceso a información institucional que se basa en las mismas tecnologías que Internet.	**Internet:** Conjunto de servidores interconectados electrónicamente, integrado por las diferentes redes de cada país del mundo.
Jefaturas: Funcionario de la administración activa responsable de una Unidad o Proceso, con autoridad para ordenar y tomar decisiones.	**Intranet (red Interna):** Red privada que permite acceso a información institucional que se basa en las mismas tecnologías que Internet.
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.	**Jefaturas: Persona funcionaria** de la administración activa responsable de una Unidad Organizacional, con autoridad para ordenar y tomar decisiones.
Medio de almacenamiento: Cualquier dispositivo en el cual se puede guardar información.	**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.
Módem: Dispositivo utilizado para la conexión a Internet.	**Medio de almacenamiento:** Cualquier dispositivo en el cual se puede guardar información.
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.	**Módem:** Dispositivo utilizado para la conexión a Internet.
Perfil: Conjunto de derechos y atribuciones que tienen los usuarios	**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 y lo establecido en la Ley de Control Interno en su artículo 16 relativo a los Sistemas de Información

de los recursos informáticos. **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. **Usuario o Usuario Final:** Todas aquellas personas que utilicen sistemas, software, equipos informáticos y los servicios de red provistos por el INA. **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,	**Perfil:** Conjunto de derechos y atribuciones que tienen las **personas usuaria**s de los recursos informáticos. **Personas usuarias externas:** Todas aquellas personas naturales o jurídicas, que no son **personas funcionarias** del INA pero prestan algún tipo de servicio profesional o técnico a la Institución. **Persona Usuaria Final:** Todas aquellas **terceras personas** que utilicen sistemas, software, equipos informáticos y los servicios de red provistos por el INA. **Privilegio:** Permiso para realizar una actividad dentro de los sistemas, equipos o servicios de la Institución. **Recursos de TI** **Menor privilegio:** Principio utilizado para la asignación de perfiles de usuario según el cual a éste se le deben asignar, por defecto, únicamente los permisos estrictamente necesarios para la realización de sus labores. **Necesidad de saber:** Principio utilizado para la definición de perfiles de usuario según el cual a éste se le deben asignar los permisos estrictamente necesarios para tener acceso a aquella información que resulte imprescindible para la realización del trabajo. **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

portátiles, faxes, impresoras, fotocopiadoras, teléfonos, etc.) dentro del INA.	la pantalla, generalmente ocultando el contenido con el que se está trabajando.
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.	**Recurso informático:** Cualquier equipo tecnológico (computadoras, portátiles, faxes, impresoras, fotocopiadoras, teléfonos, etc.) dentro del INA.
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**.**	**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.
Respaldos: Copia de seguridad de la información en un medio de almacenamiento externo.	**Reporte de navegación:** Informe emitido mediante un sistema o herramienta que permite mostrar los sitios de Internet que una **persona usuaria** ha accesado durante un periodo definido.
Rol: Conjunto de permisos que se asignan a un usuario que se autentican o accesa a un servicio, aplicación o sistema.	**Respaldos:** Copia de seguridad de la información en un medio de almacenamiento externo.
Seguridad de la Información: Conjunto de regulaciones, procedimientos y acciones dirigidas a preservar la confidencialidad, integridad y disponibilidad de la información institucional.	**Rol:** Conjunto de permisos que se asignan a una **persona usuaria** 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	**Seguridad informática:** La seguridad informática o seguridad de tecnologías de la información es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información

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	contenida o circulante; considera aspectos como Confiabilidad, Integridad y Disponibilidad de los datos. **Service Desk:** Gestiona eventos que causan o pueden causar una pérdida en la calidad de un servicio, mantiene proactivamente informados a las **personas usuarias** 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 las **personas usuarias**. **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 carácter institucional de las **personas usuarias** de cada unidad organizativa. **Sesión:** Período de tiempo que una persona usuaria 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

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. **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 **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.	las consultas y eventos que pueden causar o no una interrupción o una reducción de la calidad del servicio y reportadas por las **personas usuarias**. **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. **UAP:** Unidad de Administración de proyectos **Unidad Organizativa (UO):** Elemento que reside en el organigrama institucional hace referencia a cualquier unidad. **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. **USEVI:** Unidad de Servicios Virtuales. **USST:** Unidad de Soporte a Servicios Tecnológicos. **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**	**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	**ARTICULO 4: Deberes y prohibiciones de las personas usuarias** Son deberes de las **personas usuarias** 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 **GTIC.** 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

USIT.	procedimiento establecido por la **GTIC**.
9. Custodiar los programas, manuales, cables y otros dispositivos del recurso informático que le sean asignados.	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.	10. Conservar la integridad y buen funcionamiento de los equipos que conforman la infraestructura informática. 11. Acatar todas las disposiciones dictadas por la **GTIC** 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. 13. Todo incidente o cambio en el uso de los recursos informáticos, debe ser reportado a la GTIC mediante el Service Desk. 14. Conectarse a la red del INA desde sitios externos, con el objetivo de utilizar los sistemas o servicios de TI definidos por la **GTIC**, en apego al procedimiento establecido para tal fin.
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.	Son prohibiciones de las **personas usuarias** 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 **GTIC.** 2. Utilizar software en los equipos que no haya sido autorizado por la **GTIC** e instalado por la USST.

4. Descargar, instalar, implementar o hacer uso de software no autorizado y/o sin licenciamiento.	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.
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.	4. Descargar, instalar, implementar o hacer uso de software no autorizado y/o sin licenciamiento.
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.	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.
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.	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.
8. Utilizar los recursos informáticos de la institución para realizar actividades personales o con fines lucrativos.	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.
9. Utilizar los recursos informáticos para la transferencia de información que afecte los derechos de autor o propiedad intelectual.	8. Utilizar los recursos informáticos de la institución para realizar actividades personales o con fines lucrativos.
10. Realizar acciones para dañar o alterar los recursos informáticos o la seguridad de la red.	9. Utilizar los recursos informáticos para la transferencia de información que afecte los derechos de autor o propiedad intelectual.
11. Realizar modificaciones en el equipo (remover, cambiar o intercambiar los componentes internos), instalar conexiones y otros dispositivos de comunicación del INA.	10. Realizar acciones para dañar o alterar los recursos informáticos o la seguridad de la red.
12. Utilizar telefonía convencional o móvil como módem para el acceso a	11. Realizar modificaciones en el equipo (remover, cambiar o

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.	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, a menos de que sean autorizados por la USIT. 13. Cambiar la configuración de los recursos informáticos establecidos por la **USST**. 14. Conectar recursos informáticos a la red de computadoras, sin que su configuración sea la aprobada por la **GTIC**. 15. Utilizar herramientas espías para la recolección de datos que puedan interferir la privacidad de las **personas usuarias.**		
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 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 **GTIC** 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.	Ajuste a la estructura	
ARTICULO 6: Deberes de la USIT Son deberes de la USIT en el en el uso y seguridad de los recursos	**ARTICULO 6: Deberes de la GTIC** Son deberes de la GTIC y las unidades adscritas en el uso y seguridad de los recursos	Lenguaje incluyente y ajuste a la estructura	

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.	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 **terceras personas**, las cláusulas referentes a temas de seguridad de la información. 6. Realizar una evaluación periódica del servicio, con el fin de renovar la respectiva autorización para el uso de los recursos informáticos de **terceras personas.** 7. Dar solución pronta y efectiva a las personas usuarias a los problemas que suscite el uso de los recursos informáticos institucionales, la cual puede ser remota o en sitio. 8. Acatar las directrices establecidas por la CGI en cuanto a los lineamientos y políticas y sobre el uso de los recursos informáticos.	actual Se incluye: y de las Unidades adscritas Lenguaje incluyente	

		Se ajusta según observaciones de Auditoría. AI-00199-2013 Lenguaje incluyente	
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	**ARTICULO 7: Deberes de la persona ARI** Son deberes de la persona ARI en el uso y seguridad de los recursos informáticos: 1. Verificar el estado de los equipos previa asignación a las personas funcionarias. 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 todas las personas usuarias, los estándares y procedimientos para el uso de recursos informáticos, de acuerdo con los lineamientos y políticas dictadas por la **GTIC** en el cumplimiento de su deber. 4. Asesorar de forma oportuna a las personas usuarias 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. 8. Acatar las directrices establecidas	Lenguaje incluyente y ajustes al organigrama. Se sustituye USIT por	

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.	por la CGI en cuanto a los lineamientos y políticas y sobre el uso de los recursos informáticos. 9. Garantizar la privacidad de los datos del INA y las **personas usuaria**	GTIC Se ajusta según observaciones de Auditoría. AI-00199-2013 Lenguaje incluyente	
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.	**CAPITULO III** **USO DE CONTRASEÑAS** **ARTICULO 8: Deberes y prohibiciones de las personas usuarias** Son deberes de las **personas usuarias** 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	Lenguaje incluyente	

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.	contraseña. 6. Utilizar los procedimientos que establezca la **GTIC** para solicitar cuentas de acceso a los sistemas o equipos del INA o cambios de las mismas. Son prohibiciones de las **personas usuarias** en el uso de las contraseñas: 1. Compartir entre **personas usuarias** 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 **terceras personas**. 4. Buscar palabras claves de otras personas usuarias 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	Se sustituye USIT por GTIC Lenguaje inluyente	

	ARTICULO 9: Deberes de la <u>USIT</u> Son deberes de las **personas funcionarias** de la **<u>USIT</u>** en el uso de las contraseñas: 1. Entregar a su propietario la cuenta de acceso y clave de la **persona usuaria** 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 la persona funcionaria para hacer entrega de la clave de usuario a los sistemas o equipos del INA. 3. Suspender todas las cuentas asociadas a la **persona funcionaria** cuando deja de laborar para la Institución. 4. Bloquear automáticamente después de un intervalo de tiempo de inactividad definido por la <u>GTIC</u>, toda computadora, estación de trabajo o terminal. 5. Conceder a las **personas usuarias**, acceso a los sistemas de información, previa solicitud de la Jefatura de la UO correspondiente.	Lenguaje incluyente y ajuste al organigrama	

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 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 una **persona funcionaria** para que procedan a la eliminación de los privilegios. 2. Informar de manera inmediata a la USIT cuando una **persona funcionaria** 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.	Lenguaje incluyente	
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 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 una **persona usuaria**. 1. Informar a la USIT los cambios en los privilegios otorgados a las **personas funcionarias** de su Unidad. 2. Notificar a la USIT acerca de la contratación de cualquier **persona funcionaria** en su área, debiendo enviar por escrito el nombre de la persona usuaria, fecha de ingreso, descripción de trabajo e información que necesita accesar para realizar sus labores, lo último. Todo lo anterior, mediante el Service Desk	Lenguaje incluyente	

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.	**ARTICULO 12: Deberes de la persona ARI** Son deberes de **la persona** ARI en el uso de las contraseñas: 1. Tramitar las solicitudes de apertura de las cuentas y cambios correspondientes a las **personas usuarias** de la Unidad, así como su eliminación o inhabilitación temporal por ausencia de la **persona funcionaria**. 2. Notificar a la USIT sobre cualquier cambio de perfil que se genere a una **persona usuaria**, así como la razón de ese cambio.	Lenguaje incluyente	
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	**CAPITULO IV USO DE INTERNET** **ARTICULO 13: Deberes y prohibiciones de las personas usuarias** Son deberes de las **personas usuarias** en el uso de internet: 1. Utilizar en todo momento la página establecida por la **GTIC,** como página de inicio en el navegador de Internet. 2. Justificar cuando se le solicite ante la **GTIC**, el uso de INTERNET que no esté considerado conforme a este reglamento. Son prohibiciones de las **personas usuarias** en el uso de internet: 1. Conectarse a Internet por medios no autorizados por la **GTIC**. 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 de la **persona funcionaria** 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	Lenguaje incluyente Se sustituye USIT por GTIC Se ajusta según observaciones de Auditoría. AI-00199-2013	

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.	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 **GTIC**. 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. Se prohíbe navegar en internet desde un equipo que tenga software no autorizados por la **GTIC**.	Se sustituye USIT por GTIC Se sustituye USIT por	

		GTIC Se sustituye USIT por GTIC Se ajusta según observaciones de Auditoría. AI-00199-2013	
ARTICULO 14: Deberes de la USIT Son deberes de la USIT en el uso de internet: 1. Registrar en bitácora todo sitio	**ARTICULO 14: Deberes de la <u>GTIC</u>** Son deberes de la **<u>GTIC</u>** en el uso de internet: 1. Registrar en bitácora todo sitio	Se sustituye USIT por GTIC	

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.	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 una **persona usuaria** que esté haciendo mal uso del servicio de Internet, así como cancelar el servicio; todo lo anterior respetando el derecho a privacidad de la información de la **persona funcionaria**.	Lenguaje incluyente Se ajusta según observaciones de Auditoría. AI-00199-2013	
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	**CAPITULO V USO DEL SERVICIO DE CORREO ELECTRÓNICO** **ARTICULO 15: Deberes y prohibiciones de las personas usuarias** Son deberes de las **personas usuarias** 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;	Lenguaje incluyente	

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	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" 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 de la **persona usuaria.** -Unidad, Proceso o Núcleo, para el cual trabaja. -Correo electrónico de la **persona funcionaria o usuaria**. -Número de teléfono o teléfonos de contacto de la **persona funcionaria o usuaria**. -Aviso de confidencialidad. 5. Reportar inmediatamente, a su jefe o a la **GTIC**, 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 las **personas usuarias** en el servicio de correo electrónico: 1. Utilizar algún tipo de fondo que no sea el autorizado o definido por la **Asesoría de la Comunicación** 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		

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.	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 otras **personas usuarias**. 5. Permitir a otras **personas usuarias** utilizar su cuenta de correo institucional. 6. Dejar sesiones abiertas sin control alguno. 7. Ver, copiar, alterar o destruir el contenido del correo de otra **persona usuaria** 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 **terceras personas**; identificarse como una persona ficticia o simplemente no identificarse. 12. Violentar las medidas de seguridad que soportan el entorno del servicio de correo electrónico.	Se sustituye USIT por GTIC Lenguaje incluyente Se sustituye USIT por **Asesoría de la Comunicación**	

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.	**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 **persona usuaria**. 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 de la persona usuaria. -Unidad, Proceso o Núcleo, para el cual trabaja. -Correo electrónico de la persona funcionaria o usuaria. -Número de teléfono o teléfonos de contacto de la **persona funcionaria o usuario**. -Aviso de confidencialidad. 4. Elaborar el aviso de confidencialidad.	Lenguaje incluyente	.
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	**CAPITULO VI CONTROL DE VIRUS Y SOFTWARE MALICIOSO** **ARTICULO 17: Deberes y prohibiciones de** las **personas usuarias finales** Son deberes de las **personas usuarias finales** en el control de virus y software malicioso: 1. Reportar oportunamente cualquier mal funcionamiento de la herramienta antivirus a la **USST**.	Lenguaje incluyente	

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.	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 **GTIC** 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 las **personas usuarias finales** 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.	Se sustituye USIT por USST Se ajusta según observaciones de Auditoría. AI-00199-2013 Se sustituye USIT por GTIC	

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 18: Deberes de la UO** Son deberes de la UO en el control de virus y software malicioso: 1. Solicitar a la **GTIC** la revisión y autorización de la herramienta de antivirus instalada en los equipos pertenecientes a **terceras personas**, con el fin de que puedan realizar algún tipo de labor en los recursos informáticos. 2. Autorizar a las **personas usuarias** a utilizar directorios, carpetas o unidades de disco compartido y definir los permisos de seguridad sobre lo que se comparte.	Lenguaje incluyente Se sustituye USIT por GTIC	
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 19: Deberes de la GTIC** Son deberes de la **GTIC** 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.	Se sustituye USIT por GTIC	
ARTICULO 20: Deberes del ARI Son deberes del ARI en el control de	**ARTICULO 20: Deberes de la persona ARI** Son deberes de **la persona** ARI en	Lenguaje incluyente	

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.	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 **GTIC** y la UO correspondiente. 3. Comunicar los cambios realizados en las políticas, estándares, configuración y mantenimiento de equipos para mantener la seguridad informática.	Se sustituye USIT por GTIC	
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.	**CAPITULO VII** **ESCRITORIO Y PANTALLA LIMPIA** **ARTICULO 21: Deberes y prohibiciones de** las **personas usuarias** Son deberes de la **persona usuaria** 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 **Asesoría de la Comunicación**. **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 las personas funcionarias. 4. Bloquear o proteger con el protector de pantalla autorizado por la **Asesoría de la Comunicación**, las computadoras cuando están desatendidas, para evitar el acceso	Lenguaje incluyente Se sustituye USIT por Asesoría de la Comunicación	

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.	no autorizado. Son prohibiciones de la persona usuaria en el uso del escritorio y pantalla limpia: **1.** Desactivar o modificar la configuración del protector de pantalla establecido por la **Asesoría de la Comunicación** **2.** Cambiar el fondo de pantalla institucional autorizado por la **Asesoría de la Comunicación** **3.** 4. 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.	Se sustituye USIT por Asesoría de la Comunicación Se sustituye USIT por Asesoría de la Comunicación Se sustituye USIT por Asesoría de la Comunicación	
CAPITULO VIII PRIVACIDAD Y PROTECCIÓN DE LA	**CAPITULO VIII PRIVACIDAD Y PROTECCIÓN DE LA**	Lenguaje incluyente	

INFORMACIÓN	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 22: Deberes y prohibiciones de** las **personas usuarias** Son deberes de la **persona usuaria** para resguardar la privacidad y protección de la información: 1. Ingresar o extraer **información** 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. 2. 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 de la **persona usuaria** 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.	Eliminar por cuanto es una obligación de cada trabajador y no le da ningún valor agregado. Se agrega el término información Lenguaje incluyente	

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.	**ARTICULO 23: Deberes de la persona ARI** Es deber de **la persona** ARI guardar la debida confidencialidad, cuando por razones de trabajo se tenga acceso incidental a información no autorizada por las **personas usuarias**.	Lenguaje incluyente	
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	**CAPITULO IX SEGURIDAD FÍSICA Y AMBIENTAL** **ARTICULO 24: Deberes y prohibiciones de las personas usuarias de la GTIC** Son deberes de la **persona usuaria** 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 de la **persona usuaria** 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 una **persona funcionaria** a cualquier área, utilizando el carné o credenciales de otra persona funcionaria. 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	Lenguaje incluyente	

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.	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 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 toda **persona funcionaria** 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.	Lenguaje incluyente	
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,	**ARTICULO 26: Deberes de la persona ARI** Son deberes de **la persona** ARI para garantizar la seguridad física y ambiental: 1. Notificar, al momento de detectar cualquier anomalía de seguridad detectada, a la **GTIC** y la UO correspondiente.	Lenguaje incluyente	

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.	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.	Se sustituye USIT por GTIC	
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.	**CAPITULO X** **RESPALDOS Y RECUPERACIÓN** **ARTICULO 27: Deberes de las personas usuarias** Son deberes de la **persona usuaria** 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.	Lenguaje incluyente	
ARTICULO 28: Deberes del ARI Es deber del ARI instruir a solicitud de los usuarios, acerca de la elaboración y recuperación de respaldos.	**ARTICULO 28: Deberes de la persona ARI** Es deber de **la persona** ARI instruir a solicitud de las **personas usuarias**, acerca de la ejecución y recuperación de respaldos.	Lenguaje incluyente	
CAPITULO XI MANIPULACIÓN Y	**CAPITULO XI MANIPULACIÓN Y**	Lenguaje incluyente	

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).	**DESTRUCCIÓN DE DATOS** **ARTICULO 29: Deberes y prohibiciones de las personas usuarias** Son deberes de la **persona usuaria** considerar lo siguiente, cuando requiera destruir información: 1. Eliminar los documentos textuales, electrónicos y digitalizados en una forma precisa y transformada en material no legible, 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 de la **persona usuaria** 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 **terceras personas**).	Se ajusta según observaciones de Auditoría. AI-00199-2013 Se modifica para no encasillar al INA en determinados métodos de destrucción de documentos que podrían quedar obsoletos con el avance tecnológico.	
CAPITULO XII DE LAS SOLICITUDES DE SERVICIO. **ARTICULO 30: Deberes de los Usuarios**	**CAPITULO XII DE LAS SOLICITUDES DE SERVICIO.** **ARTICULO 30: Deberes de las personas usuarias**	Lenguaje incluyente	

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.	Son deberes de la **persona usuaria** en las solicitudes de servicio 1. Realizar las solicitudes de servicios a través del procedimiento establecido por la **GTIC**. 2. Autorizar la atención a la solicitud de servicio vía control remoto para que este sea ejecutado por **la persona** ARI. 3. Permitir la revisión del equipo asignado por parte de **la persona** 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.	Se sustituye USIT por GTIC	
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.	**ARTICULO 31: Prohibiciones de la persona ARI** Son prohibiciones de **la persona** ARI en las solicitudes de servicio 1. Accesar de forma remota sin previa autorización de la persona usuaria. 2. Accesar a información confidencial sin previa autorización de la **persona usuaria.**	Lenguaje incluyente	
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.	**CAPITULO XIII RÉGIMEN DISCIPLINARIO** El presente reglamento concuerda con las leyes vigentes de la república de Costa Rica, sancionará a toda aquella **persona usuaria** 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.	Lenguaje incluyente	
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	**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		

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	estipulado en el artículo 48 del Reglamento Autónomo de Servicios del Instituto Nacional de Aprendizaje. • Artículo 4: prohibiciones de las **personas usuarias** en el uso y seguridad de los recursos informáticos, incisos 1, 2, 3, 4 y 5. • Artículo 13: prohibiciones de las **personas usuarias** en el uso de internet, inciso 1. • Artículo 15: prohibiciones de las personas usuarias en el servicio de correo electrónico, incisos 1, 2,3 y 4. • Artículo 17: prohibiciones de las **personas usuarias** en el control de virus y software malicioso, incisos 1, 2 y3. • Artículo 21: prohibiciones de la **persona usuaria** en el uso del escritorio y pantalla limpia, incisos 1, 2 y 3. • Artículo 22: prohibiciones de la **persona usuaria** en la privacidad y protección de la información, inciso 1. • Artículo 24: prohibiciones de la **persona usuaria** para garantizar la seguridad física y ambiental, inciso 1. • Artículo 29: prohibiciones de la **persona usuaria** en la manipulación y destrucción de datos, inciso 1.

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. 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	**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: prohibiciones de las **personas usuarias** en el uso y seguridad de

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.	los recursos informáticos, incisos 1, 2, 3, 4, 5, 6, 7, 8, 9 y 10. • Artículo 8: prohibiciones de las **personas usuarias** en el uso de las contraseñas, incisos 1, 2, 3 y 4. • Artículo 13: prohibiciones de las **personas usuarias** en el uso de internet, incisos 1, 2, 3, 4, 5 y 6. • Artículo 15: prohibiciones de las **personas usuarias** en el servicio de correo electrónico, incisos 1, 2, 3, 4, 5, 6, 7 y 8. • Artículo 17: prohibiciones de las **personas usuarias** en el control de virus y software malicioso, inciso 1. • Artículo 22: prohibiciones de la **persona usuaria** en la privacidad y protección de la información, incisos 1 y 2. • Artículo 24: prohibiciones de la **persona usuaria** para garantizar la seguridad física y ambiental, incisos 1, 2, 3 y 4. • Artículo 29: prohibiciones de la **persona usuaria** en la manipulación y destrucción de datos, inciso 1. • Artículo 31: prohibiciones del ARI en las solicitudes de servicio, incisos 1 y 2.

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.	**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.	**ARTÍCULO 35: TRANSITORIO** La **GTIC** deberá en un plazo no mayor a dos meses posteriores a su publicación adaptar los procedimientos de su competencia con relación a este documento.	Se cambia USIT por GTIC	

5.- Que los miembros de la Junta Directiva realizaron sus consultas y comentarios sobre la propuesta presentada, y después de una amplia discusión y análisis manifestaron su anuencia a la aprobación de la misma.

POR TANTO: POR UNANIMIDAD DE LOS MIEMBROS PRESENTES SE ACUERDA:

PRIMERO: APROBAR LA PROPUESTA DE REFORMAS AL REGLAMENTO USO DE RECURSOS INFORMÁTICOS, SOLICITADOS POR LA SUBGERENCIA ADMINISTRATIVA, SEGÚN OFICIO SGA-284-2014 Y COMO CONSTA EN ACTAS.

SEGUNDO: QUE EN VIRTUD DE DICHA APROBACIÓN, EL REGLAMENTO SUPRACITADO TEXTUALMENTE SE LEERÁ DE LA SIGUIENTE MANERA:

REGLAMENTO USO DE RECURSOS INFORMATICOS

CAPÍTULO I:

DISPOSICIONES GENERALES

ARTICULO 1. OBJETIVO

El presente reglamento tiene como finalidad normar el uso de los recursos, de los servicios informáticos y los servicios de red, que está a disposición de las personas funcionarias para su utilización en actividades adjetivas y sustantivas.

ARTICULO 2. AMBITO DE ACCION

Lo enunciado en el presente reglamento es aplicable tanto para las personas usuarias finales, como para las personas técnicas informáticas, así como de las personas proveedoras de los recursos y servicios informáticos. Será responsabilidad de las personas citadas anteriormente, 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: Acceder 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: Convenio entre empresas y/o contrato entre las personas funcionarias que tengan acceso a consulta y/o modificación (crear, actualizar y eliminar) de datos de los servicios informáticos, o bien, entre instituciones que comparten datos o sistemas, para garantizar el manejo discreto de la información. También se utiliza el concepto "cláusulas de confidencialidad", que son aquellas que imponen una obligación negativa: de no hacer o de abstenerse; es decir, de no utilizar la información recibida con fines distintos a los estipulados (véanse los artículos 71 del Código de Trabajo)

Acuerdo de licenciamiento: Contrato entre persona proveedora debidamente autorizado o entre el fabricante y la institución, para utilizar éste en una forma determinada y de conformidad con las condiciones convenidas.

Administrador de Recursos Informáticos (ARI): Persona funcionaria técnico informática, designada por la jefatura para administrar los recursos informáticos tanto en la GTIC como en Unidades Regionales.

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

Autenticación: Acto de establecimiento o confirmación de la identidad de una persona usuaria 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, o una instancia superior a ésta, siempre y cuando se cumplan con los principios de seguridad de la información de dicha 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 la persona usuaria emplea para acceder a un servicio, sistema o programa.

Confidencialidad: Protección de la información sensible contra acceso y divulgación no autorizada.

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 de la persona soportista.

Correo Electrónico: servicio de red dentro y fuera del INA que permite a las personas usuarias enviar y recibir mensajes mediante sistemas de comunicación electrónicos.

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

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

Cuotas de disco: Espacio de almacenamiento en disco asignado a una persona usuaria.

Decodificación: Proceso inverso para obtener la información en su formato nativo.

Disponibilidad de la Información: Se vincula con el hecho de que la información se encuentre disponible (v. gr. utilizable) cuando la necesite en un proceso de la organización en el presente y en el futuro. También se asocia con la protección de los recursos necesarios y las capacidades asociadas. Implica que se cuente con la información necesaria en el momento en que la organización la requiere.

Dispositivos Móviles: son dispositivos de tamaño pequeño, con capacidad de procesamiento y de conexión a una red, con memoria limitada, diseñados específicamente para una función, pero que pueden llevar a cabo otras funciones más generales.

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 o imagen digitalizada: 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 éstos.

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

Firewall: Elemento del sistema de seguridad de información que es 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, mediante el Service Desk.

GTIC: Gestión de Tecnologías de Información y Comunicación.

Hardware: Todos los componentes electrónicos, eléctricos y mecánicos que integren: computadoras, servidores, módems, routers, switches, cableado, cintas, discos, fuentes de poder, dispositivo de almacenamiento (SAN), UPS, en oposición a los programas que se escriben para ella y la controlan (software).

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: Precisión y suficiencia de la información, así como su validez de acuerdo con los valores y expectativas del negocio.

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: Persona funcionaria de la administración activa responsable de una Unidad Organizacional, 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 y lo establecido en la Ley de Control Interno en su artículo 16 relativo a los Sistemas de Información.

Perfil: Conjunto de derechos y atribuciones que tienen las personas usuarias de los recursos informáticos.

Personas usuarias externas: Todas aquellas personas naturales o jurídicas, que no son personas funcionarias del INA pero que utilizan algún tipo de servicio profesional o técnico a la Institución.

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

Privilegio: Permiso para realizar una actividad dentro de los sistemas, equipos o servicios de TIC de la Institución. Se otorga mediante una autorización.

Recursos de TI

Menor privilegio: Principio utilizado para la asignación de perfiles de usuario según el cual a éste se le deben asignar, por defecto, únicamente los permisos estrictamente necesarios para la realización de sus labores.

Necesidad de saber: Principio utilizado para la definición de perfiles de usuario según el cual a éste se le deben asignar los permisos estrictamente necesarios para tener acceso a aquella información que resulte imprescindible para la realización del trabajo.

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 una persona usuaria 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 una persona usuaria 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.

Seguridad informática: La seguridad informática o seguridad de tecnologías de la información es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante; considera aspectos como Confiabilidad, Integridad y Disponibilidad de los datos.

Service Desk: Gestiona eventos que causan o pueden causar una pérdida en la calidad de un servicio, mantiene proactivamente informados a las personas usuarias 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 las personas usuarias.

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 carácter institucional de las personas usuarias de cada unidad organizativa.

Sesión: Período de tiempo que una persona usuaria 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 las personas usuarias.

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.

UAP: Unidad de Administración de proyectos

Unidad Organizativa (UO): Elemento que reside en el organigrama institucional hace referencia a cualquier unidad.

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.

USEVI: Unidad de Servicios Virtuales.

USST: Unidad de Soporte a Servicios Tecnológicos.

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 las personas usuarias

Son deberes de las personas usuarias 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 GTIC.

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 GTIC

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 GTIC 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.

13. Todo incidente o cambio en el uso de los recursos informáticos, debe ser reportado a la GTIC mediante el Service Desk.

14. Conectarse a la red del INA desde sitios externos, con el objetivo de utilizar los sistemas o servicios de TI definidos por la GTIC, en apego al procedimiento establecido para tal fin.

Son prohibiciones de las personas usuarias 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 GTIC.

2. Utilizar software en los equipos que no haya sido autorizado por la GTIC e instalado por la USST.

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, a menos de que sean autorizados por la USIT.

13. Cambiar la configuración de los recursos informáticos establecidos por la USST.

14. Conectar recursos informáticos a la red de computadoras, sin que su configuración sea la aprobada por la GTIC.

15. Utilizar herramientas espías para la recolección de datos que puedan interferir la privacidad de las personas usuarias.

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 GTIC 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 GTIC

Son deberes de la GTIC y sus unidades adscritas 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 terceras personas, las cláusulas referentes a temas de seguridad de la información.

6. Realizar una evaluación periódica del servicio, con el fin de renovar la respectiva autorización para el uso de los recursos informáticos de terceras personas.

7. Dar solución pronta y efectiva a las personas usuarias a los problemas que suscite el uso de los recursos informáticos institucionales, la cual puede ser remota o en sitio.

8. Acatar las directrices establecidas por la CGI en cuanto a los lineamientos y políticas y sobre el uso de los recursos informáticos.

ARTICULO 7: Deberes de la persona ARI

Son deberes de la persona ARI en el uso y seguridad de los recursos informáticos:

1. Verificar el estado de los equipos previa asignación a las personas funcionarias.

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 todas las personas usuarias, los estándares y procedimientos para el uso de recursos informáticos, de acuerdo con los lineamientos y políticas dictadas por la GTIC en el cumplimiento de su deber.

4. Asesorar de forma oportuna a las personas usuarias 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.

8. Acatar las directrices establecidas por la CGI en cuanto a los lineamientos y políticas y sobre el uso de los recursos informáticos.

9. Garantizar la privacidad de los datos del INA y las personas usuarias.

CAPITULO III

USO DE CONTRASEÑAS

ARTICULO 8: Deberes y prohibiciones de las personas usuarias

Son deberes de las personas usuarias 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 GTIC para solicitar cuentas de acceso a los sistemas o equipos del INA o cambios de las mismas.

Son prohibiciones de las personas usuarias en el uso de las contraseñas:

1. Compartir entre personas usuarias 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 terceras personas.

4. Buscar palabras claves de otras personas usuarias 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 las personas funcionarias de la USIT en el uso de las contraseñas:

1. Entregar a su propietario la cuenta de acceso y clave de la persona usuaria 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 la persona funcionaria para hacer entrega de la clave de usuario a los sistemas o equipos del INA.

3. Suspender todas las cuentas asociadas a la persona funcionaria cuando deja de laborar para la Institución.

4. Bloquear automáticamente después de un intervalo de tiempo de inactividad definido por la GTIC, toda computadora, estación de trabajo o terminal.

5. Conceder a las personas usuarias, acceso a los sistemas de información, previa solicitud de la Jefatura 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 una persona funcionaria para que procedan a la eliminación de los privilegios.

2. Informar de manera inmediata a la USIT cuando una persona funcionaria 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 una persona usuaria.

1. Informar a la USIT los cambios en los privilegios otorgados a las personas funcionarias de su Unidad.

2. Notificar a la USIT acerca de la contratación de cualquier persona funcionaria en su área, debiendo enviar por escrito el nombre de la persona usuaria, fecha de ingreso,

descripción de trabajo e información que necesita acceder para realizar sus labores, lo último.

Todo lo anterior, mediante el Service Desk

ARTICULO 12: Deberes de la persona ARI

Son deberes de la persona ARI en el uso de las contraseñas:

1. Tramitar las solicitudes de apertura de las cuentas y cambios correspondientes a las personas usuarias de la Unidad, así como su eliminación o inhabilitación temporal por ausencia de la persona funcionaria.

2. Notificar a la USIT sobre cualquier cambio de perfil que se genere a una persona usuaria, así como la razón de ese cambio.

CAPITULO IV USO DE INTERNET

ARTICULO 13: Deberes y prohibiciones de las personas usuarias

Son deberes de las personas usuarias en el uso de internet:

1. Utilizar en todo momento la página establecida por la GTIC, como página de inicio en el navegador de Internet.

2. Justificar cuando se le solicite ante la GTIC, el uso de INTERNET que no esté considerado conforme a este reglamento.

Son prohibiciones de las personas usuarias en el uso de internet:

1. Conectarse a Internet por medios no autorizados por la GTIC.

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 de la persona funcionaria 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 GTIC.

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. Se prohíbe navegar en internet desde un equipo que tenga software no autorizados por la GTIC.

ARTICULO 14: Deberes de la GTIC

Son deberes de la GTIC 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 una persona usuaria que esté haciendo mal uso del servicio de Internet, así como cancelar el servicio; todo lo anterior respetando el derecho a privacidad de la información de la persona funcionaria.

CAPITULO V USO DEL SERVICIO DE CORREO ELECTRÓNICO

ARTICULO 15: Deberes y prohibiciones de las personas usuarias

Son deberes de las personas usuarias 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" 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 de la persona usuaria. -Unidad, Proceso o Núcleo, para el cual trabaja. -Correo electrónico de la persona funcionaria o usuaria. -Número de teléfono o teléfonos de contacto de la persona funcionaria o usuaria. -Aviso de confidencialidad.

5. Reportar inmediatamente, a su jefe o a la GTIC, 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 las personas usuarias en el servicio de correo electrónico:

1. Utilizar algún tipo de fondo que no sea el autorizado o definido por la Asesoría de la Comunicación 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 otras personas usuarias.

5. Permitir a otras personas usuarias utilizar su cuenta de correo institucional.

6. Dejar sesiones abiertas sin control alguno.

7. Ver, copiar, alterar o destruir el contenido del correo de otra persona usuaria 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 terceras personas; 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 persona usuaria.

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 de la persona usuaria. -Unidad, Proceso o Núcleo, para el cual trabaja. -Correo electrónico de la persona funcionaria o usuaria. -Número de teléfono o teléfonos de contacto de la persona funcionaria 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 las personas usuarias finales

Son deberes de las personas usuarias finales en el control de virus y software malicioso:

1. Reportar oportunamente cualquier mal funcionamiento de la herramienta antivirus a la USST.

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 GTIC 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 las personas usuarias finales 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 GTIC la revisión y autorización de la herramienta de antivirus instalada en los equipos pertenecientes a terceras personas, con el fin de que puedan realizar algún tipo de labor en los recursos informáticos.

2. Autorizar a las personas usuarias 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 GTIC

Son deberes de la GTIC 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 de la persona ARI

Son deberes de la persona 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 GTIC 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 las personas usuarias

Son deberes de la persona usuaria 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 Asesoría de la Comunicación.

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 las personas funcionarias.

4. Bloquear o proteger con el protector de pantalla autorizado por la Asesoría de la Comunicación, las computadoras cuando están desatendidas, para evitar el acceso no autorizado.

Son prohibiciones de la persona usuaria en el uso del escritorio y pantalla limpia:

1. Desactivar o modificar la configuración del protector de pantalla establecido por la Asesoría de la Comunicación.

2. Cambiar el fondo de pantalla institucional autorizado por la Asesoría de la Comunicación.

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 las personas usuarias

Son deberes de la persona usuaria para resguardar la privacidad y protección de la información:

1. Ingresar o extraer información 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.

2. 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 de la persona usuaria 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 de la persona ARI

Es deber de la persona ARI guardar la debida confidencialidad, cuando por razones de trabajo se tenga acceso incidental a información no autorizada por las personas usuarias.

CAPITULO IX SEGURIDAD FÍSICA Y AMBIENTAL

ARTICULO 24: Deberes y prohibiciones de las personas usuarias de la GTIC

Son deberes de la persona usuaria 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 de la persona usuaria 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 una persona funcionaria a cualquier área, utilizando el carné o credenciales de otra persona funcionaria.

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 toda persona funcionaria 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 de la persona ARI

Son deberes de la persona ARI para garantizar la seguridad física y ambiental:

1. Notificar, al momento de detectar cualquier anomalía de seguridad detectada, a la GTIC 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 las personas usuarias

Son deberes de la persona usuaria 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 de la persona ARI

Es deber de la persona ARI instruir a solicitud de las personas usuarias, acerca de la ejecución y recuperación de respaldos.

CAPITULO XI MANIPULACIÓN Y DESTRUCCIÓN DE DATOS

ARTICULO 29: Deberes y prohibiciones de las personas usuarias

Son deberes de la persona usuaria considerar lo siguiente, cuando requiera destruir información:

1. Eliminar los documentos textuales, electrónicos y digitalizados en una forma precisa y transformada en material no legible, 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 de la persona usuaria 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 terceras personas).

CAPITULO XII DE LAS SOLICITUDES DE SERVICIO.

ARTICULO 30: Deberes de las personas usuarias

Son deberes de la persona usuaria en las solicitudes de servicio

1. Realizar las solicitudes de servicios a través del procedimiento establecido por la GTIC.

2. Autorizar la atención a la solicitud de servicio vía control remoto para que este sea ejecutado por la persona ARI.

3. Permitir la revisión del equipo asignado por parte de la persona 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 de la persona ARI

Son prohibiciones de la persona ARI en las solicitudes de servicio

1. Accesar de forma remota sin previa autorización de la persona usuaria.

2. Accesar a información confidencial sin previa autorización de la persona usuaria.

CAPITULO XIII RÉGIMEN DISCIPLINARIO

El presente reglamento concuerda con las leyes vigentes de la república de Costa Rica, sancionará a toda aquella persona usuaria 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:** prohibiciones de las personas usuarias en el uso y seguridad de los recursos informáticos, incisos 1, 2, 3, 4 y 5.
- **Artículo 13:** prohibiciones de las personas usuarias en el uso de internet, inciso 1.
- **Artículo 15:** prohibiciones de las personas usuarias en el servicio de correo electrónico, incisos 1, 2,3 y 4.
- **Artículo 17:** prohibiciones de las personas usuarias en el control de virus y software malicioso, incisos 1, 2 y3.

- **Artículo 21:** prohibiciones de la persona usuaria en el uso del escritorio y pantalla limpia, incisos 1, 2 y 3.
- **Artículo 22:** prohibiciones de la persona usuaria en la privacidad y protección de la información, inciso 1.
- **Artículo 24:** prohibiciones de la persona usuaria para garantizar la seguridad física y ambiental, inciso 1.
- **Artículo 29:** prohibiciones de la persona usuaria en la manipulación y destrucción de datos, inciso 1.

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:** prohibiciones de las personas usuarias en el uso y seguridad de los recursos informáticos, incisos 1, 2, 3, 4, 5, 6, 7, 8, 9 y 10.
- **Artículo 8:** prohibiciones de las personas usuarias en el uso de las contraseñas, incisos 1, 2, 3 y 4.
- **Artículo 13:** prohibiciones de las personas usuarias en el uso de internet, incisos 1, 2, 3, 4, 5 y 6.
- **Artículo 15:** prohibiciones de las personas usuarias en el servicio de correo electrónico, incisos 1, 2, 3, 4, 5, 6, 7 y 8.
- **Artículo 17:** prohibiciones de las personas usuarias en el control de virus y software malicioso, inciso 1.
- **Artículo 22:** prohibiciones de la persona usuaria en la privacidad y protección de la información, incisos 1 y 2.
- **Artículo 24:** prohibiciones de la persona usuaria para garantizar la seguridad física y ambiental, incisos 1, 2, 3 y 4.
- **Artículo 29:** prohibiciones de la persona usuaria en la manipulación y destrucción de datos, inciso 1.
- **Artículo 31:** prohibiciones del ARI en las solicitudes de servicio, incisos 1 y 2.

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

ARTÍCULO NOVENO:

Gerencia General. Oficio GG-526-2014. Información complementaria sobre el Manual de Puestos, solicitada mediante Acuerdos Número 081-2014-JD y 092-2014-JD.

El señor Presidente, solicita al señor Gerente General que se refiera al tema.

El señor Gerente General, indica que el tema será expuesto por el señor Carlos Chacón, Jefe de la Unidad de Recursos Humanos y por la señora Eva Jiménez, funcionaria de la misma dependencia

El señor Esna Montero, señala que lo que les enviaron, fue por una solicitud del señor Director Muñoz Araya, sobre el tema del 0.43, y el documento viene sumamente borroso y en la última parte, donde se consignan las clases, salarios, está borroso y no se puede observar nada y es una imagen e imagina que estaba en colores y al sacar fotocopias, no se puede observar, incluso en la reunión previa, solicitaron que se les imprimiera, pero tampoco se pudo ver.

Trae el tema a colación, porque las primeras hojas sí se pueden leer, pero las últimas 6 o 7 hojas, que es donde viene la parte sustancial, donde vienen las tablas realmente no se pueden ver.

El señor Presidente, consulta al señor Secretario Técnico si cuando se distribuye el material, se verifica que sea legible.

El señor Secretario Técnico, responde que el material es enviado vía correo electrónico, ciertamente se observó que podían tener problemas con algunas láminas, en ese sentido desea aclarar que no se envían fotocopias a los señores Directores.

El señor Presidente, sugiere que para lo sucesivo es importante que el señor Secretario Técnico, solicite a la fuente que envíe el documento más claro.

El señor Director Solano Cerdas, indica que le llamó la atención cuando trataron de ver el material que estaba borroso, no se explica que la Administración manda cosas que son ilegibles. En ese sentido, si hubiera estado el señor Gustavo Ramírez, le hubiera preguntado, qué cree que podría hacer con su tecnología para mejorarlo.

El señor Director Esna Montero, acota que cuando les envían esta información, es para se pueda estudiar y tomar la decisión, en su caso particular, debe decir que no va a tomar una decisión, ya que no pudo estudiar las últimas láminas, incluso pueden hacer la presentación, pero no va a tomar una decisión, porque no lo pudo estudiar todo.

El señor Vicepresidente Lizama Hernandez, acota que trató de leer el documento en la computadora, pero fue imposible, porque además de que los cuadros son incómodos de leer, las letras de las páginas son de diferentes tamaños.

En ese sentido, prefiere no recibir el informe y que les envíen un documento legible y se pone en agenda en el momento que se tenga la información.

El señor Director Muñoz Araya, indica que envió una nota en donde mencionó que las páginas 3, 4 y 5 no se entienden bien, porque están borrosas algunas columnas, y además pidió que se anotara el 0.43, complementario a lo que venía en el Manual de Clases y la información que viene en el documento, es importante ya que cuando vieron el Manual de Clases, venía con un incremento muy sustancioso, desde un 45% a un 0.62% en las clases más bajas, eso implicaba alrededor del 10% del presupuesto del INA, y el aumento promedio era alrededor de los cien mil colones, cuando a nivel del país, se estaba peleando por el 0.43% de aumento por parte de los sindicatos, y en la Institución lo que se estaba pidiendo, estaba con una oscilación tan grande, entre 45% a un 0.62%, que representaba menos del 1% en las clases más bajas.

Menciona que el Presidente Ejecutivo en ese momento, pidió que se realizara un estudio completo y el que les presentan no lo es, porque no se toma en cuenta lo que dijo en ese momento el Asesor Legal, que se debía hacer un estudio de las condiciones fiscales que se dan en el momento en el país y el costo de vida, así como los salarios del sector privado, en los mismos puestos, en las mismas ejecuciones.

Indica que en los estudios que realiza el INEC, se puede ver claramente y aunque no se cita ninguna referencia con el sector privado, pero se puede ver cómo el sector privado está un 50% para abajo de los salarios del Gobierno Central y el resto del sector público y esto lo publica la Academia Centroamericana, en el estudio que presentó la semana pasada y publica un serie de comparaciones de los sectores privados y en este estudio no se toman en cuenta, es decir hay información disponible que no contempla y les deja ayunos en esa comparación de los mismos puestos en el sector privado.

En ese aspecto, con el estudio es muy ligero y difícilmente con esa información pueden tomar un acuerdo, que podría ser de trascendencia para el INA y que se puede creer, que están de acuerdo con la aprobación de un Manual de Clases.

Cree que con la información que se les da, aparte de que venía borrosa, es incompleta.

El señor Presidente, solicita que ingresen la señora Eva Jiménez y el señor Carlos Chacón.

La señora Eva Jimenez, les indica a los señores de Junta Directiva que no trae la presentación.

El señor Presidente, comenta que los señores miembros de la Junta Directiva iban a pedir un espacio de unos días más, ya que el documento que les llegó no venía muy claro y es complemento de la exposición.

En ese aspecto, sugiere que la presentación la reenvíen al señor Secretario Técnico, para la posterior remisión a los miembros de Junta Directiva, por lo que el tema se pospone el punto para ser visto en una próxima Sesión.

Agradece a los funcionarios. Se retiran del Salón de Sesiones.

ARTÍCULO DÉCIMO:

Asesoría Legal. Oficio ALCA-285-2014. Proyecto de resolución en Recurso de Apelación contra acto administrativo del Proceso de Adquisiciones, originado en licitación pública 2010LN-000010-01 para la "Contratación de

Servicios Profesionales de Abogados para el Cobro Judicial del Tributo creado mediante la Ley 6868 del INA".

El señor Presidente, solicita al señor Asesor Legal que se refiera a este punto.

El señor Asesor Legal, indica que para contextualizar a los nuevos integrantes de la Junta Directiva, debe mencionar que el INA se financia con un tributo especial fijado por su propia Ley, que es sobre el monto total de la planilla de salarios con cinco o más empleados se cancela un 1.5% y se recauda a través de la CCSS.

Agrega que el Sector Agropecuario paga un 0.5%, el Estado está exento junto con las Municipalidades y eventualmente instituciones que no tengan ánimo de lucro.

Señala que para la recaudación de ese tributo que la CCSS recauda, en primer instancia esa Institución recauda hasta tres meses, el patrono tiene la posibilidad de pagar y decir que paga Caja, es decir invalidez, vejez y muerte, enfermedad y maternidad y que no paga INA, por lo que se ahorran esa parte.

El señor Presidente, consulta si se está refiriendo a los patrones morosos,

El señor Asesor Legal, responde que sí.

En ese aspecto, el INA tiene que recuperar ese tributo. Para esto, existe lo que se llama el PIC, Proceso de Inspección y Cobros del INA. Anteriormente el Departamento Legal llevaba el cobro judicial, pero en realidad éste es bastante amplio, no significativamente alto en monto, pero si en cantidad de casos, porque se habla de que la misma morosidad y un poco más que puede tener la CCSS, en cantidad de casos, no en montos, porque obviamente la CCSS es mucho mayor, por lo se maneja en el INA.

EN ese sentido, existe una contratación de abogados externos, que son los que se encargan de recuperar en cobro judicial esos tributos. Esto se hizo mediante la Licitación 2010-10-01, donde se contrató un Staff de abogados externos, que fiscaliza el Proceso de Inspección y Cobros, además es un contrato anual prorrogable año a año.

Indica que las prórrogas no son facultativas, es decir en materia de contrataci8ón administrativa, a veces se comete el error de decir que el contrato ya está prorrogado en forma automática, y no es así, porque las prórrogas son facultad de la Administración, el hacerlo o no.

Añade que en los contratos que se firmaron con estos abogados externos, está claramente establecido que para hacer la prórroga, se requiere una evaluación, esto es muy usual en el INA, para cualquier servicio, ya sea de capacitación, aseo y limpieza, mantenimiento de zonas verdes, seguridad y vigilancia, es decir siempre se hace una evaluación de parte de los encargados, en este caso el Proceso de Adquisiciones, con base en los insumos que le da el PIC.

Señala que el señor Guillermo Angulo Álvarez, no pasó esa evaluación, porque tuvo problemas de que cuando lo llamaban no estaba, no presentaba los informes a tiempo o no los presentaba, es decir parece que se desentendió, porque existen toda una serie de controles, de informes que deben estar presentando al PIC, en este caso, el señor no lo ejecutó, en el expediente consta la evaluación que le dieron, y fue de un 60% en la calidad del servicio, lo cual es muy bajo, tomando en cuenta que se dedica a recuperar los tributos de la Institución.

Acota que en virtud de ello, se le procedió a comunicar que no se le iba a prorrogar el contrato, por lo que el señor interpone un Recurso de Apelación, en contra del oficio en que se le señala que no se le va a prorrogar el contrato.

Indica que este Recurso de Apelación, lo conoce la Junta Directiva y se basa en la Ley General de Administración Pública y no en la Ley de Contratación Administrativa, que regula por lo general lo que es la tramitología hasta la adjudicación y ciertos detalles en la ejecución, por lo que si hay apelaciones dentro de la ejecución de un contrato, se rige por Ley General de Administración Pública y en este caso, es simplemente que el señor presentó la Revocatoria en el lapso de tres días, con Apelación en Subsidio, se le rechaza la misma y la Apelación la conoce la Junta Directiva.

Agrega que básicamente los fundamentos son rechazarla también, en virtud de lo que ha señalado, porque las prórrogas son facultativas y la evaluación que hizo el técnico competente, arroja un resultado de un 60% en la calificación, es decir ni siquiera llega al 70%, de allí que la recomendación de la Asesoría Legal en esta Resolución es que se declare sin lugar el Recurso interpuesto por el señor

Guillermo Ángulo Álvarez y dar por agotada la Vía Administrativa. En ese caso, si el señor lo considera, continuará en los órganos judiciales correspondientes.

Asimismo, ofrece las disculpas porque este es un Recurso viejo que se envió, por lo que se ve que en el machote todavía aparece la figura del señor Francisco Marín, Expresidente Ejecutivo, pero fue porque se dio mucho antes de esta situación.

El señor Presidente, somete a votación dejar pendiente para resolver en una próxima Sesión, el contenido del Oficio ALCA-285-2014 sobre Proyecto de resolución en Recurso de Apelación, contra acto administrativo del Proceso de Adquisiciones, originado en licitación pública 2010LN-000010-01, para la Contratación de Servicios Profesionales de Abogados para el Cobro Judicial del Tributo, creado mediante la Ley 6868 del INA.

COMUNICACIÓN DE ACUERDO AC-151-2014-JD

CONSIDERANDO:

1. Que mediante oficio ALCA-285-2014, la Asesoría Legal remite para conocimiento y eventual aprobación de la Junta Directiva el proyecto de resolución del Recurso de Apelación en contra del acto administrativo del Proceso de Adquisiciones, originado en Licitación Pública 2010LN-000010-01 para la **"CONTRATACION DE SERVICIOS PROFESIONALES DE ABOGADOS PARA EL COBRO JUDICIAL DEL TRIBUTO CREADO MEDIANTE LA LEY 6868 DEL INA".**

2. Que el Asesor Legal expone ampliamente ante los miembros de la Junta

Directiva sobre el recurso de apelación interpuesto por el Licenciado Guillermo Angulo Álvarez en contra del acto administrativo en el cual se le notificó la no prórroga de su contrato con el INA.

3. Que una vez discutido y analizado el mismo, los miembros de la Junta Directiva tomaron la decisión de volver a discutir dicho tema en próximas sesiones.

POR TANTO:

POR UNANIMIDAD DE LOS MIEMBROS PRESENTES SE ACUERDA:

ÚNICO: DEJAR PARA PARA UNA PRÓXIMA SESIÓN EL CONOCIMIENTO DEL PROYECTO DE RESOLUCIÓN EN RECURSO DE APELACIÓN CONTRA ACTA ADMINISTRATIVO EN LICITACIÓN PÚBLICA 2010-LN-000010-01 "CONTRATACIÓN DE SERVICIOS PROFESIONALES DE ABOGADOS PARA EL COBRO JUDICIAL DEL TRIBUTO CREADO MEDIANTE LA LEY 6868 DEL INA".

ACUERDO APROBADO EN FIRME POR UNANIMIDAD

ARTÍCULO DÉCIMO PRIMERO:

DOCUMENTOS DISTRIBUIDOS PARA SER VISTOS EN PRÓXIMA SESIÓN:

- **13.1 Proceso de Adquisiciones. Oficio UCI-PA-1681-2014. Informe de recomendación para la adjudicación de la Licitación Pública 2012LN-000002-04 para la contratación de servicios de capacitación y formación profesional en el subsector de informática según demanda y cuantía inestimada para La Unidad Regional Polivalente de Liberia.**

El señor Presidente, indica que estos documentos se distribuyen para ser conocidos en la próxima Sesión.

ARTÍCULO DÉCIMO SEGUNDO:

Asuntos de la Presidencia Ejecutiva

No hay Asuntos de la Presidencia Ejecutiva.

ARTÍCULO DÉCIMO TERCERO:

Varios

El señor Secretario Técnico, menciona que le parece conveniente retomar la observación que hizo el señor Asesor Legal y que tiene relación con un correo del señor Gerente General, en cuanto a la conveniencia de realizar una Sesión Extraordinaria el día 18 de junio, en ese sentido debe indicar que hay una serie de licitaciones adicionales que están pendientes y también el tema de la SBD, por lo

que desea saber si se va a tomar una decisión sobre esto o si se pospondrá para la próxima Sesión.

El señor Presidente, indica que considera importante sobre lo planteado por el señor Asesor Legal, en el sentido de solicitar una prórroga a la Asamblea Legislativa para el tema de la SBD, para lo cual se estaría encomendando al señor Secretario Técnico que la solicite formalmente.

Al ser las veinte horas con cincuenta y dos minutos, del mismo día y lugar, finaliza la Sesión.

APROBADA EN LA SESIÓN 4632