Artículo 12.—**De los Acuerdos de la Comisión.** Los acuerdos tomados por los miembros de la Comisión de Recomendación de Adjudicaciones, se deberán consignar en el expediente electrónico de la contratación. La recomendación de esa comisión se tramitará a través del sistema digital unificado (SDU), a la persona u órgano competente para tomar la decisión final del procedimiento respectivo, utilizando para ello el módulo respectivo en SDU.

Artículo 13.—**Publicación.** De conformidad con lo dispuesto en los artículos 4 y 5 de la Ley No. 8220 "Protección al ciudadano del exceso de requisitos y trámites administrativos", la Dirección de Proveeduría Institucional y la Dirección de Tecnologías de la Información, deberán publicar - respectivamente- en La Gaceta, en Internet e Intranet el presente Reglamento Interno.

Artículo 14.—**Vigencia.** Rige a partir de la publicación el *La Gaceta*.

Proveeduría Institucional.—Irán Barquero Mena, Director.—1 vez.—O.C. N° 7219.—Solicitud N° 462724.—(IN2023814753).

INSTITUTO NACIONAL DE APRENDIZAJE

JUNTA DIRECTIVA

Se hace saber que la Junta Directiva del Instituto Nacional de Aprendizaje, mediante el acuerdo adoptado en el capítulo VI de la sesión ordinaria Nº 36-2023 celebrada el 11 de setiembre del 2023 (Acuerdo de Junta Directiva Nº JD-AC-302-2023-V2), aprobó la reforma integral al siguiente reglamento:

"REGLAMENTO DE USO
DE RECURSOS INFORMÁTICOS"

Por tanto:

La Junta Directiva del Instituto Nacional de Aprendizaje, mediante Acuerdo firme JD-AC-302-2023, tomado en la Sesión Ordinaria Nº 36-2023 del día 11 de setiembre del 2023, acordó aprobar el siguiente "Reglamento de uso de Recursos Informáticos", el cual dispone:

CAPÍTULO I

Disposiciones generales

Artículo 1º—**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.

Artículo 2º—**Ámbito de acción**. 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.

Artículo 3º—**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.

Antivirus: Aplicación o grupo de aplicaciones dedicadas a la prevención, búsqueda, detección, bloqueo, desinfección 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 Unidad Organizativa, o una instancia superior a ésta, siempre y cuando se cumplan con los principios de seguridad de la información de dicha Unidad Organizativa.

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

Certificado de Firma Digital: La firma digital es un instrumento tecnológico que da fe de la identidad del firmante. Para firmar de manera digital, el usuario requiere una tarjeta, que es un dispositivo similar a una tarjeta de crédito o débito, con un chip incorporado en el que se almacena el certificado digital, mediante el cual se da a los usuarios la capacidad de autenticarse y firmar.

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

Código Malicioso: Se llama Código Malicioso, programa malicioso, programa maligno, programa malintencionado, en inglés Malware (acortamiento de malicious software), badware o código maligno, a cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

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).

CGI: Comisión Gerencial de Informática.

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.

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, sistemas de alimentación ininterrumpida; 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.

Infraestructura tecnológica: La infraestructura tecnológica es el conjunto de computadoras, servidores, equipos de comunicación, equipos de almacenamiento, equipos periféricos, herramientas de gestión de los equipos, herramientas de seguridad informática y demás elementos físicos y lógicos que se integran para la funcionalidad de la red y las comunicaciones.

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.

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

Persona Administradora de Recursos Informáticos (ARI): Persona funcionaria en informática, designada por la jefatura para administrar los recursos informáticos en la GTIC y sus Unidades adscritas, así como en las Unidades Regionales.

Persona Administradora de Sistemas Institucionales (ASI): Persona funcionaria de la parte usuaria con amplio conocimiento administrativo y técnico del área que se encuentra automatizada o que se automatizará, quien por su perfil se ubica como asesor, colaborar estrecho y elemento STAFF de la jefatura, y por ende, de enlace y canal único de comunicación entre los usuarios del sistema de información y la parte técnica informática, en cuanto a capacitación, gestión y aprobación de cualquier necesidad de los usuarios de sistemas de información.

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.

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.

RDFD: Repositorio de documentos firmados digitalmente.

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 tecnológica 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: En español Mesa de Ayuda (en inglés: Help Desk, a veces traducido como 'Centro de ayuda'), o Centro de Servicio, es un conjunto de recursos tecnológicos y humanos, para prestar servicios con la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados con las TIC.

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.

Servicios de TIC: Servicios que se ofrecen en tecnología de la Información y Comunicación a nivel institucional.

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.

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

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.

CAPÍTULO II

Uso y seguridad de los recursos informáticos

Artículo 4º—**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 Unidad Organizativa bajo el procedimiento establecido.
8. Informar de los problemas o incidentes que presenten los recursos informáticos institucionales por medio del procedimiento establecido por la GTIC.
9. Custodiar los recursos informáticos que le sean asignados, además de los instaladores de programas y manuales asignados sea en formato físico o virtual.
10. Conservar la integridad y buen funcionamiento de los equipos que conforman la infraestructura tecnológica.
11. Acatar todas las disposiciones dictadas por la GTIC y sus Unidades adscritas 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 ante 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.
15. Garantizar que todo documento firmado digitalmente producto de sus funciones, sea almacenado en el RDFD.
16. Almacenar información de carácter laboral mediante las herramientas oficiales provistas por el INA.

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. Instalar software en los equipos que no haya sido autorizado por la GTIC e instalado por un ARI.
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. Acceder a Internet utilizando medios no autorizados por la USIT (telefonía, redes externas, servicio celular u otros) mientras esté conectado a la red Institucional.
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.

Artículo 5º—**Deberes de la Unidad Organizativa**. Son deberes de la Unidad Organizativa en el uso y seguridad de los recursos informáticos:

1. Adquirir y custodiar las licencias de 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.

Artículo 6º—**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 tecnología informática.
2. Velar por las funciones de planeación, coordinación y administración de los servicios de seguridad de tecnología informática.
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 según la normativa institucional en seguridad informática, 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 (confidencialidad, integridad y disponibilidad) los cuales serán entre el INA y el contratista. Para el caso de terceras personas, será el contratista el responsable de llevar a cabo los acuerdos de confidencialidad que sean necesario para la ejecución del servicio, lo cual deberá quedar indicado en las contrataciones de servicios que requiera el INA.
6. Realizar al menos una revisión anual de los servicios contratados, 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, de acuerdo con los tiempos establecidos en el Catálogo de Servicios.
8. Acatar las directrices establecidas por la CGI en cuanto a los lineamientos y políticas y sobre el uso de los recursos informáticos.
9. Mantener un sitio para ser utilizado como RDFD que cumpla con lo estipulado en el Artículo 6º—"Gestión y conservación de documentos electrónicos", de la Ley N° 8454 "LEY DE CERTIFICADOS, FIRMAS DIGITALES Y DOCUMENTOS ELECTRÓNICOS".

Artículo 7º—**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 Unidad Organizativa 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 servicios.
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.

CAPÍTULO III

Uso de contraseñas

Artículo 8º—**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 servicios de TIC 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 servicios de TIC o cambios de las mismas.
7. Dar el mismo tratamiento y cuidado al pin de la firma digital, como se indica en este reglamento para las contraseñas.

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 servicios de TIC o cambios de las mismas vía telefónica o correo electrónico (salvo solicitud firmada 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.

Artículo 9º—**Deberes de las Unidades de la GTIC**. Son deberes de las personas funcionarias de la GTIC y sus unidades adscritas 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 servicios de TIC, 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 servicios de TIC.
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 Unidad Organizativa correspondiente.

Artículo 10.—**Deberes de la Unidad de Recursos Humanos**. Son deberes de la Unidad de Recursos Humanos 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 formal y oportuna a la USIT, cuando se deba inhabilitar el acceso a los recursos informáticos a un usuario por cualquiera de los lineamientos definidos por la Unidad de Recursos Humanos.
3. Comunicar inmediatamente a la USIT el traslado de una persona funcionaria para que procedan a la eliminación de los privilegios.
4. Comunicar a la USIT acerca de la contratación de cualquier persona funcionaria, debiendo enviar el nombre de la persona usuaria, fecha de ingreso, nombre del puesto, lugar de trabajo, para que se proceda con la creación del perfil de usuario.

Artículo 11.—**Deberes de la Unidad Organizativa**. Son deberes de la Unidad Organizativa en el uso de las contraseñas:

1. Solicitar al ASI respectivo el acceso a los sistemas de información que le concederá a una persona usuaria.
2. Solicitar a la USIT el cambio de los privilegios otorgados en los accesos a los servicios de TI ofrecidos por la USIT, a través de los procedimientos establecidos para tal fin.
3. Notificar al ASI acerca de la contratación, traslado, cese o cualquier otro motivo que requiera ajustes en los roles asignados en los sistemas de las personas funcionarias en su dependencia, mediante el Service Desk.

Artículo 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.

CAPÍTULO IV

Uso de internet

Artículo 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; 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.

Artículo 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.

CAPÍTULO V

Uso del servicio de correo electrónico

Artículo 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 en todo correo electrónico que sea enviado desde el Sistema de Correo Electrónico del INA, según el formato establecido por Asesoría de Comunicación.
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.

Artículo 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. Administrar la capacidad de almacenamiento de correo para cada persona usuaria.
3. Implementar y automatizar el aviso de confidencialidad suministrado por la Asesoría Legal.

CAPÍTULO VI

Control de virus y software malicioso

Artículo 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. Realizar un escaneo con la herramienta antivirus provista por el INA en busca y limpieza de posible malware antes de proceder a la lectura de la información obtenida de fuentes externas en cualquier medio de almacenamiento 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 de almacenamiento externo 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 Unidad Organizativa correspondiente y además estar claramente definidos los permisos de seguridad sobre lo que se comparte.
4. Modificar la frecuencia del escaneo automático del software.

Artículo 18.—**Deberes de la Unidad Organizativa**. Son deberes de la Unidad Organizativa 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.

Artículo 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.

Artículo 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, a la GTIC y a la Unidad Organizativa correspondiente.
3. Instalar el software antivirus autorizado por la USIT en todo dispositivo institucional que lo permita.

CAPÍTULO VII

Escritorio y pantalla limpia

Artículo 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 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.

CAPÍTULO VIII

Privacidad y protección de la información

Artículo 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 o ceder información que no sea clasificada del tipo “Información Pública” 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.

Artículo 23.—**Deberes del personal de la GTIC, unidades adscritas y personal ARI**. Es deber del personal indicado guardar la debida confidencialidad, cuando por razones de trabajo se tenga acceso a información confidencial o que contienen datos personales sensibles o de acceso restringido.

CAPÍTULO IX

Seguridad física y ambiental

Artículo 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. El ingreso de personas no autorizadas a las áreas restringidas.
2. Almacenar en los cuartos de servidores, cuartos de comunicación o gabinetes, 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 tecnológica.
5. Trasladar a otras dependencias, sin la debida autorización, cualquier elemento físico de la instalación informática o de la infraestructura tecnológica.

Artículo 25.—**Deberes de la Unidad Organizativa**. Son deberes de la Unidad Organizativa 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 Unidad Organizativa correspondiente.

Artículo 26.—**Deberes de la persona ARI**. Son deberes de la persona ARI para garantizar la seguridad física y ambiental:

1. Notificar a la GTIC y la Unidad Organizativa correspondiente al momento de detectar cualquier anomalía de seguridad informática.
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.

CAPÍTULO X

Respaldos y recuperación

Artículo 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.

Artículo 28.—**Deberes de la persona ARI**.

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

CAPÍTULO XI

Manipulación y destrucción de datos

Artículo 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, sin acatar lo dispuesto en los procedimientos, manuales, u otras directrices emitidas por la Unidad de Archivo Central Institucional.
2. Usar o distribuir información institucional para fines ilícitos (propios o para terceras personas).

CAPÍTULO XII

De las solicitudes de servicio

Artículo 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.

Artículo 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.

CAPÍTULO 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. Cuyo debido proceso seguirá las regulaciones contenidas en el 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, específicamente el incumplimiento de los artículos 4, inciso 1, 2, 3, 4, 5, 12, 13, artículo 13, incisos 1 y 7, artículo 15, incisos 1 y 2, artículo 17, incisos 1, 2, 3, 4, artículos 21, incisos 1, 2, 3, Artículo 22, inciso 1, artículo 24, inciso 1, y el artículo 29, inciso 1 del presente reglamento.

Las faltas leves se sancionarán de la siguiente forma:

a) Por la primera, con amonestación escrita si a juicio de la jefatura no resulta aplicable el apercibimiento verbal.
b) Por la segunda, con una suspensión sin goce de salario de uno a cinco días.
c) Por la tercera, con una suspensión sin goce de salario de seis a diez días.
d) Por la cuarta, con una suspensión sin goce de salario de once a quince días.
e) Por las demás, con el despido sin responsabilidad patronal.
f) Esas sanciones se aplicarán sin perjuicio de que, si las faltas lo ameriten, se imponga una sanción mayor.

Artículo 33.—**Faltas graves**. Se considera falta grave el incumplimiento a cualquier obligación, deber y/o responsabilidad dispuesta en el presente reglamento, específicamente el incumplimiento de los artículos 4, incisos 6, 7, 8, 9, 10, 11, 14 y 15, artículo 8, incisos 1, 2, 3, 4, artículo 13, incisos 2, 3, 4, 5, 6, artículo 15, incisos 3, 4, 5, 6, 7, 8, 9, 10, 11 y 12, artículo 22, incisos 1, 2, 3, artículo 24, incisos 1, 2, 3, 4, artículo29, incisos 1 y 2, artículo 31, incisos 1 y 2 del presente reglamento.

Las faltas graves se sancionarán de la siguiente forma:

a) Por una, con suspensión sin goce de salario de uno a cinco días.
b) Por dos, con suspensión sin goce de salario de seis a diez días.
c) Por tres, con suspensión de goce de salario de once a quince días.
d) Por cuatro, despido sin responsabilidad patronal.
e) Esas sanciones se aplicarán sin perjuicio de que, si las faltas lo ameriten, se imponga una sanción mayor.

CAPÍTULO XIV

Disposiciones finales

Artículo 34.—**Vigencia**. Este Reglamento rige a partir del día hábil siguiente a su publicación en el Diario Oficial *La Gaceta*.

Firmado digitalmente.—Unidad de Compras Institucionales.—Lic. Allan Altamirano Díaz, Jefe.—1 vez.—O.C. N° 01-M557-2023.—Solicitud N° 462804.—(IN2023814738).

JUNTA DE PENSIONES Y JUBILACIONES DEL MAGISTERIO NACIONAL

REGLAMENTO DE CRÉDITO
DEL FONDO ESPECIAL ADMINISTRATIVO

Según el acuerdo adoptado por la Junta Directiva de la Junta de Pensiones y Jubilaciones del Magisterio Nacional, en la Sesión Ordinaria: 0101-2023 del