REGLAMENTO USO DE RECURSOS INFORMATICOS

REGLAMENTO USO DE RECURSOS INFORMATICOS

CAPÍTULO I:

DISPOSICIONES GENERALES

ARTICULO 1. OBJETIVO

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

ARTICULO 2. AMBITO DE ACCION

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

ARTICULO 3. DEFINICIONES Y NOMENCLATURA

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

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

REGLAMENTO USO DE RECURSOS INFORMATICOS

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

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

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

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

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

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

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

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

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

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

REGLAMENTO USO DE RECURSOS INFORMATICOS

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

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

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

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

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

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

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

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

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

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

REGLAMENTO USO DE RECURSOS INFORMATICOS

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

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

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

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

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

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

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

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

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

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

REGLAMENTO USO DE RECURSOS INFORMATICOS

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

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

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

Módem: Dispositivo utilizado para la conexión a Internet.

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

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

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

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

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

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

REGLAMENTO USO DE RECURSOS INFORMATICOS

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

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

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

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

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

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

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

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

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

REGLAMENTO USO DE RECURSOS INFORMATICOS

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

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

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

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

SPAM: Correo electrónico no deseado.

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

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

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

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

USIT: Unidad de Servicios de Informática y Telemática

REGLAMENTO USO DE RECURSOS INFORMATICOS

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

UTEFOR: Unidad de Tecnología de la Formación

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

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

CAPITULO II
USO Y SEGURIDAD DE LOS RECURSOS INFORMATICOS

ARTICULO 4: Deberes y prohibiciones de los Usuarios

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

1. Utilizar los recursos informáticos atendiendo las disposiciones expresadas en este reglamento.
2. Hacer uso adecuado de todos los activos o recursos de Información.
3. Cumplir con los principios de la seguridad de la información: confidencialidad, integridad y disponibilidad.
4. Cumplir la política de seguridad de la información del INA.
5. Custodiar, resguardar, manipular y utilizar los recursos informáticos según lo establecido por la USIT.
6. Comportarse apegado a los más altos valores éticos y morales, a las buenas costumbres y estándares de conducta socialmente aceptados, de tal forma que no se dañe la integridad moral de un tercero, interno o externo al INA.
7. Solicitar la conexión de los equipos que se requieran en la red institucional por medio de la UO bajo el procedimiento establecido.

REGLAMENTO USO DE RECURSOS INFORMATICOS

8. Informar de los problemas que presenten los recursos informáticos institucionales por medio del procedimiento establecido por la USIT.
9. Custodiar los programas, manuales, cables y otros dispositivos del recurso informático que le sean asignados.
10. Conservar la integridad y buen funcionamiento de los equipos que conforman la infraestructura informática.
11. Acatar todas las disposiciones dictadas por la USIT sobre uso de los recursos informáticos.
12. Apagar los equipos tecnológicos al finalizar su jornada laboral, salvo casos en los que sea estrictamente necesario que permanezcan encendidos, lo cual deberá ser justificado debidamente por la jefatura inmediata.

Son prohibiciones de los usuarios en el uso y seguridad de los recursos informáticos:
1. Utilizar la red eléctrica conectada al sistema de respaldo de energía del INA para otros fines distintos a la conexión de computadoras portátiles o de escritorio autorizados por la USIT.
2. Utilizar software en los equipos que no haya sido instalado ni autorizado por la USIT.
3. Almacenar en el equipo asignado o en el disponible en la red, archivos de cualquier tipo ajenos a los fines e intereses de la institución.
4. Descargar, instalar, implementar o hacer uso de software no autorizado y/o sin licenciamiento.
5. Guardar, distribuir materiales, fotografías, música, videos, mensajes, documentos o cualquier otro tipo de archivo que no tengan relación con sus funciones dentro del INA.
6. Utilizar los recursos informáticos de la Institución para exhibir, copiar, mover, reproducir o manipular de cualquier otra forma material de contenido que atente contra la ética, la moral o las buenas costumbres.
7. Suprimir, modificar, borrar o alterar los medios de identificación de los equipos, o entorpecer de cualquier otra forma los controles establecidos para fines de inventario.
8. Utilizar los recursos informáticos de la institución para realizar actividades personales o con fines lucrativos.
9. Utilizar los recursos informáticos para la transferencia de información que afecte los derechos de autor o propiedad intelectual.

10. Realizar acciones para dañar o alterar los recursos informáticos o la seguridad de la red.
11. Realizar modificaciones en el equipo (remover, cambiar o intercambiar los componentes internos), instalar conexiones y otros dispositivos de comunicación del INA.
12. Utilizar telefonía convencional o móvil como módem para el acceso a Internet.
13. Cambiar la configuración de los recursos informáticos establecidos por la USIT.
14. Conectar recursos informáticos a la red de computadoras, sin que su configuración sea la aprobada por la USIT.
15. Utilizar herramientas espías para la recolección de datos que puedan interferir la privacidad de los usuarios.

ARTICULO 5: Deberes de la UO

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

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

ARTICULO 6: Deberes de la USIT

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

1. Administrar la seguridad de la información.
2. Velar por las funciones de planeación, coordinación y administración de los servicios de seguridad de la información.
3. Garantizar la seguridad en las operaciones realizadas, a través del control de procesos, normativas, reglas, políticas y estándares.
4. Asegurar una adecuada protección de los recursos informáticos, velando por la confidencialidad, integridad y disponibilidad de la información del INA.
5. Incorporar en las contrataciones de servicios informáticos a realizar con terceros, las cláusulas referentes a temas de seguridad de la información.

REGLAMENTO USO DE RECURSOS INFORMATICOS

6. Renovar cada 6 meses, la respectiva autorización para el uso de los recursos informáticos de los terceros.

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

ARTICULO 7: Deberes del ARI

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

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

CAPITULO III

USO DE CONTRASEÑAS

ARTICULO 8: Deberes y prohibiciones de los Usuarios

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

1. Ingresar a los sistemas o equipos del INA mediante una cuenta de acceso propia.
2. Tratar todas las contraseñas como información confidencial.

3. Cambiar la contraseña que le ha sido asignada tal y como el sistema se lo solicita.
4. Velar por que su clave de usuario, sea lo más segura posible respetando los procedimientos establecidos para tal fin.
5. Velar por las acciones que se reporten y ejecuten con su contraseña.
6. Utilizar los procedimientos que establezca la USIT para solicitar cuentas de acceso a los sistemas o equipos del INA o cambios de las mismas.

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

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

ARTICULO 9: Deberes de la USIT

Son deberes de la USIT en el uso de las contraseñas:

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

REGLAMENTO USO DE RECURSOS INFORMATICOS

ARTICULO 10: Deberes de la URH

Son deberes de la URH en el uso de las contraseñas:

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

ARTICULO 11: Deberes de la UO

Son deberes de la UO en el uso de las contraseñas:

1. Solicitar a la USIT el acceso a los sistemas de información que le concederá a un usuario.
2. Informar a la USIT los cambios en los privilegios otorgados a los funcionarios de su Unidad.
3. Notificar a la USIT acerca de la contratación de cualquier funcionario en su área, debiendo enviar por escrito el nombre del usuario, fecha de ingreso, descripción de trabajo e información que necesita accesar para realizar sus labores, lo último, utilizando los formularios establecidos para este fin.

ARTICULO 12: Deberes del ARI

Son deberes del ARI en el uso de las contraseñas:

1. Tramitar las solicitudes de apertura de las cuentas y cambios correspondientes a los usuarios de la Unidad, así como su eliminación o inhabilitación temporal por ausencia del funcionario.
2. Notificar a la USIT sobre cualquier cambio de perfil que se genere a un usuario, así como la razón de ese cambio.

CAPITULO IV
USO DE INTERNET

ARTICULO 13: Deberes y prohibiciones de los Usuarios

Son deberes de los usuarios en el uso de internet:

REGLAMENTO USO DE RECURSOS INFORMATICOS

1. Utilizar en todo momento la página establecida por la USIT, como página de inicio en el navegador de Internet.
2. Justificar cuando se le solicite, el uso de INTERNET que no esté considerado conforme a este reglamento.

Son prohibiciones de los usuarios en el uso de internet:

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

REGLAMENTO USO DE RECURSOS INFORMATICOS

ARTICULO 14: Deberes de la USIT

Son deberes de la USIT en el uso de internet:

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

CAPITULO V
USO DEL SERVICIO DE CORREO ELECTRÓNICO

ARTICULO 15: Deberes y prohibiciones de los Usuarios

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

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

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

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

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

REGLAMENTO USO DE RECURSOS INFORMATICOS

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

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

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

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

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

3. Enviar copias no autorizadas de programas informáticos.

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

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

6. Dejar sesiones abiertas sin control alguno.

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

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

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

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

REGLAMENTO USO DE RECURSOS INFORMATICOS

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

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

ARTICULO 16: Deberes de la USIT

Son deberes de la USIT en el servicio de correo electrónico:

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

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

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

4. Elaborar el aviso de confidencialidad.

CAPITULO VI

CONTROL DE VIRUS Y SOFTWARE MALICIOSO

ARTICULO 17: Deberes y prohibiciones de los Usuarios

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

1. Velar por el correcto funcionamiento de la herramienta antivirus y reportarlo a la USIT cuando se encuentra deshabilitado.

2. Seguir un proceso de verificación de virus antes de proceder a la lectura de la información obtenida de fuentes externas en cualquier medio de almacenamiento (discos flexibles, CD´s, DVD´s, Cintas o cualquier otro similar.) o correo electrónico.

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

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

ARTICULO 18: Deberes de la UO

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

ARTICULO 19: Deberes de la USIT

Son deberes de la USIT en el control de virus y software malicioso:
1. Velar por que todo equipo de cómputo propiedad de la Institución cuente con el software oficial de antivirus del INA, el cual debe ser actualizado de forma periódica.
2. Habilitar o deshabilitar los servicios relacionados con el software de antivirus o aplicaciones instaladas para combatir el software malicioso, tanto a nivel de servidor como de los demás dispositivos.

REGLAMENTO USO DE RECURSOS INFORMATICOS

ARTICULO 20: Deberes del ARI

Son deberes del ARI en el control de virus y software malicioso:

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

CAPITULO VII
ESCRITORIO Y PANTALLA LIMPIA

ARTICULO 21: Deberes y prohibiciones de los Usuarios

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

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

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

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

REGLAMENTO USO DE RECURSOS INFORMATICOS

CAPITULO VIII

PRIVACIDAD Y PROTECCIÓN DE LA INFORMACIÓN

ARTICULO 22: Deberes y prohibiciones de los Usuarios

Son deberes del usuario para resguardar la privacidad y protección de la información

1. Firmar un contrato de confidencialidad de conformidad a lo que establece la Política de Seguridad de la Información.
2. Ingresar o extraer de las bases de datos del INA, a través de los procedimientos establecidos para tal fin, los cuales deben contar con los mecanismos de seguridad adecuados.
3. Utilizar la información del INA de acuerdo con los derechos que se les asignen de conformidad con sus funciones, así como conocer y cumplir las regulaciones en materia de seguridad de la información.

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

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

ARTICULO 23: Deberes del ARI

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

CAPITULO IX

SEGURIDAD FÍSICA Y AMBIENTAL

ARTICULO 24: Deberes y prohibiciones de los Usuarios

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

REGLAMENTO USO DE RECURSOS INFORMATICOS

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

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

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

ARTICULO 25: Deberes de la UO

Son deberes de la UO para garantizar la seguridad física y ambiental:

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

ARTICULO 26: Deberes del ARI

Son deberes del ARI para garantizar la seguridad física y ambiental:

1. Notificar, al momento de detectar cualquier anomalía de seguridad detectada, a la USIT y la UO correspondiente.
2. Comunicar los cambios realizados en las políticas, estándares, configuración y mantenimiento de equipos para mantener la seguridad informática.

REGLAMENTO USO DE RECURSOS INFORMATICOS

3. Indicar a la USIT, sobre remodelaciones en el área física que alteren la disposición del cableado de la red de datos.

CAPITULO X
RESPALDOS Y RECUPERACIÓN

ARTICULO 27: Deberes de los Usuarios

Son deberes del usuario en el respaldo y recuperación de la información:

1. Almacenar la información de carácter institucional incluyendo los registros vitales en una localidad definida, de acuerdo al procedimiento establecido para estos fines.
2. Realizar los debidos respaldos de la información contenida en sus computadoras.

ARTICULO 28: Deberes del ARI

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

CAPITULO XI
MANIPULACIÓN Y DESTRUCCIÓN DE DATOS

ARTICULO 29: Deberes y prohibiciones de los Usuarios

Son deberes del usuario en la manipulación y destrucción de datos

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

Son prohibiciones del usuario en la manipulación y destrucción de datos

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

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

CAPITULO XII
DE LAS SOLICITUDES DE SERVICIO.

ARTICULO 30: Deberes de los Usuarios

Son deberes del usuario en las solicitudes de servicio

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

ARTICULO 31: Prohibiciones del ARI

Son prohibiciones del ARI en las solicitudes de servicio

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

CAPITULO XIII
RÉGIMEN DISCIPLINARIO

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

REGLAMENTO USO DE RECURSOS INFORMATICOS

ARTÍCULO 32. FALTAS LEVES

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

- **Artículo 4**

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

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

- **Artículo 13**

Son prohibiciones de los usuarios en el uso de internet:

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

- **Artículo 15**

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

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

REGLAMENTO USO DE RECURSOS INFORMATICOS

2. Abrir correos de dudosa procedencia, los cuales no han sido solicitados explícitamente, o que provengan de un remitente desconocido. Tampoco aquellos que no tengan un asunto o "Subject" específico, o que en suinterior contengan un archivo adjunto no solicitado con una extensión considerada como peligrosa, por ejemplo: .com, .exe, .src, .bat, .cpl, .hta, .vbs, .cmd, .pif, .bmp, .gif; .hlp. El correo debe ser eliminado en caso de existir duda.
3. Utilizar los recursos del servicio de correo electrónico del INA para actividades o el envío de cualquier tipo de cadenas de mensajes, así como la distribución de este tipo de información; además del envío de correo tipo "SPAM", es decir "correo basura no solicitado"
4. Enviar correos masivos a todas aquellas personas que no estén explícitamente autorizados para dicha labor. Se podrá hacer uso de este recurso salvo autorización explícita de las autoridades superiores.

- **Artículo 17**

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

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

- **Artículo 21**

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

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

REGLAMENTO USO DE RECURSOS INFORMATICOS

2. Cambiar el fondo de pantalla institucional autorizado por la USIT.

3.Desplegar en los monitores de las computadoras información institucional a la vista de otras personas, que no sean las autorizadas para tener acceso a esa información.

- **Artículo 22**

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

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

- **Artículo 24**

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

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

- **Artículo 29**

Son prohibiciones del usuario en la manipulación y destrucción de datos

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

ARTÍCULO 33. FALTAS GRAVES

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

- **Artículo 4**

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

1. Utilizar software en los equipos que no haya sido instalado ni autorizado por la USIT.

REGLAMENTO USO DE RECURSOS INFORMATICOS

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

- **Artículo 8**

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

1. Compartir entre usuarios las contraseñas de acceso a los recursos informáticos.
2. Solicitar cuentas de acceso a los sistemas o equipos del INA o cambios de las mismas vía telefónica o correo electrónico (salvo correo electrónico firmado digitalmente).

3. Dejar contraseñas escritas en medios, lugares físicos o electrónicos donde puedan ser accesados por terceros.
4. Buscar palabras claves de otros usuarios o cualquier intento de encontrar y aprovechar agujeros en la seguridad de los sistemas informáticos del INA o del exterior, o hacer uso de programas para acceder cualquier sistema informático.

- **Artículo 13**

Son prohibiciones de los usuarios en el uso de internet:

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

REGLAMENTO USO DE RECURSOS INFORMATICOS

- **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:

REGLAMENTO USO DE RECURSOS INFORMATICOS

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

- **Artículo 29**

Son prohibiciones del usuario en la manipulación y destrucción de datos

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

- **Artículo 31**

Son prohibiciones del ARI en las solicitudes de servicio

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

CAPITULO XIV:
DISPOSICIONES FINALES

ARTÍCULO 34: VIGENCIA.

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

ARTÍCULO 35: TRANSITORIO

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