SERVICIO NACIONAL DE AGUAS SUBTERRANEAS RIEGO Y AVENAMIENTO

SENARA

MANUAL DE POLÍTICAS DE TECNOLOGÍAS DE INFORMACIÓN

2019

Contenido

Presentación

Como resultado del proyecto “Implementación de las normas técnicas para la gestión y el control de las tecnologías de la información (TI) emitidas por la Contraloría General de la República (NTCGR)” liderado por la Subgerencia General (Comisión de TI) y la Unidad de Tecnologías de la Información del Senara, se crearon las políticas que conforman este documento.

Marco Jurídico

La Contraloría General de la República ha emitido leyes y normativas para el control y administración en materia de tecnologías de información y comunicación, así como la Ley General de Control Interno y otras normativas relacionadas sobre este tema.

En el año 2007 el ente contralor emite las "Normas técnicas para la gestión y el control de las tecnologías de información" las cuales fueron publicadas en el Diario Oficial La Gaceta No 119 del Jueves 21 de junio de ese mismo año y en su Capítulo I, Artículo 1.1 se establece la necesidad que en cada Institución exista un marco estratégico de Tecnologías de Información, constituido por políticas organizacionales que el personal comprenda y con las que esté comprometido.

Por lo tanto, en todas las instituciones del Estado deben existir manuales de políticas internas relativas a la administración de Tecnologías de Información. Para su cumplimiento, se definen en este documento las políticas que en esta materia, las cuales deben aplicarse para el Servicio Nacional de Aguas Subterráneas, Riego y Avenamiento.

Ámbito de aplicación

Las políticas definidas en este documento son de aplicación para todo el Servicio Nacional de Aguas Subterráneas, Riego y Avenamiento (SENARA), incluyendo el Distrito de Riego Arenal Tempisque (en adelante denominado DRAT) y las Oficinas Regionales, cuyas actividades se apoyan en instrumentos informáticos.

Actualizaciones de este manual

Este instrumento rige una vez que la Junta Directiva lo apruebe y haya ordenado su puesta en marcha de manera oficial.

Deberá ser revisado y actualizado formalmente por lo menos una vez cada año, siendo responsabilidad de la Comisión de Tecnologías de Información en conjunto con la Unidad de Gestión Informática, en adelante denominado UGI, realizar este proceso.

Durante el proceso de implementación cualquier usuario podrá hacer observaciones, con el objetivo de mejorar y/o modificar cláusulas o políticas, las cuales se harán llegar a la jefatura del Unidad de Gestión Informática.

Objetivos

Objetivo General

Establecer el marco estratégico en materia de tecnologías de información, así como facilitar el mejor aprovechamiento de los recursos informáticos y las telecomunicaciones, que son propiedad o se encuentran a disposición del Servicio Nacional de Aguas Subterráneas, Riego y Avenamiento, para alcanzar la misión institucional.

Objetivos Específicos:

- ✓ Utilizar los recursos tecnológicos de información y comunicación en forma responsable y apropiada, de conformidad con las disposiciones dadas en este manual y otras de carácter institucional, legal o emitido por otros órganos del Estado Costarricense, que guarden relación con normativas aplicables a la materia.
- ✓ Minimizar las interrupciones de los servicios asociadas a los sistemas informáticos y comunicaciones, ocasionados por uso inapropiado o por daños causados en forma accidental o intencional.
- ✓ Ordenar el desarrollo y mantenimiento de aplicaciones acordes con un modelo integral de información institucional e interinstitucional, para el intercambio de información de gran utilidad para la institución.
- ✓ Adquirir tecnología acorde a las necesidades institucionales aprovechando al máximo las capacidades de los funcionarios y el presupuesto asignado para esta materia.

Supervisión de las políticas

La supervisión del cumplimiento de las "Políticas Generales sobre Tecnologías de Información", queda a cargo de la Unidad de Gestión Informática; razón por la cual está facultada para verificar en cualquier momento el cumplimiento de estas políticas y de las normativas vigentes en materias de tecnologías de información y comunicación.

Violación a las políticas

La infracción o incumplimiento de las políticas sobre tecnologías de información y comunicación, será notificado a la jefatura correspondiente a fin de que ésta proceda según corresponda. Durante el proceso de implementación se estará revisando el tema de cumplimiento y sanción con la Unidad de Recursos Humanos.

1. Políticas Generales

1. La Unidad de Gestión Informática, será una Unidad administrativa funcionalmente independiente, que le permitirá la ejecución de procesos de planeación, coordinación, ejecución y supervisión estratégica de los proyectos e inversiones de tecnología de información a nivel institucional. Para ello tendrá una dependencia jerárquica adecuada a este propósito, asociada directamente a la Gerencia General de la institución.
2. Las políticas de tecnologías de información serán aprobadas por la Junta Directiva de SENARA y divulgadas por la Gerencia General a Directores Regionales y al DRAT. Todos los Directores, Jefes de Unidad y Directores Regionales, deberán divulgarlo a su personal. Además, para su divulgación, se utilizara el sitio web institucional. Estas políticas serán materia obligada en los procesos de inducción a los nuevos funcionarios.
3. Todos los funcionarios del SENARA, deberán conocer el Manual de Políticas de TI y regirse en su actuar por los principios consignados en ellos.
4. La Unidad de Gestión Informática será responsable por la definición y ejecución de los presupuestos que el SENARA asigne en materia de tecnología de información. Estos presupuestos incluye tanto presupuesto ordinario, extraordinario, donaciones o proyectos de cooperación, entre otros.
5. La Gerencia General tendrá la responsabilidad de la designación del coordinador de la Comisión de Tecnología de Información.
6. La Dirección Administrativa Financiera, las distintas Unidades y oficinas Regionales que conforman la institución, brindarán apoyo en el cumplimiento de las políticas de TI.
7. La Administración del SENARA, procurará recursos suficientes en los presupuestos ordinarios, extraordinarios o de proyectos de cooperación; para satisfacer los requerimientos que se deriven de la puesta en ejecución de implementación de sistemas digitales para SENARA.
8. La Comisión de Tecnologías de Información en conjunto con la Unidad de Gestión Informática, concientizaran a todos los funcionarios del SENARA, sobre su obligación de conocer y aplicar la normativa en materia de seguridad de TI, para lograr un cambio favorable en la cultura organizacional.

2. Políticas Administrativas

2.1. Políticas para el planeamiento y administración de actividades

1. La Unidad de Gestión Informática contará con un Plan estratégico en tecnologías de información y comunicación (PETIC) con el cual se orientarán las actividades.
2. En los proyectos relacionados con desarrollo de aplicaciones, deberá aplicarse una metodología formal basada en los enfoques de ciclo de vida de sistemas y orientación a objetos mediante proceso unificado, para asegurar la adecuada administración y desarrollo.

2.2. Políticas sobre los servicios que ofrece la Unidad de Gestión Informática

1. La Unidad de Gestión Informática creará un registro de los servicios que ofrece a las dependencias del SENARA y los informará a través de la web.
2. Los servicios ofrecidos por la Unidad de Gestión Informática, se solicitarán formalmente y siguiendo los procedimientos que se emitan para ese fin.

2.3. Políticas para el acceso físico a las oficinas de TI

1 El área de servidores de Red, es de acceso restringido, dadas las características del trabajo que se desarrolla en sus instalaciones.

2 Los funcionarios de las diferentes dependencias podrán ingresar a la oficina del Gestor Informático para efectos de solicitar servicios o consultas, siempre que haya un funcionario de la Unidad de Gestión Informática que los atienda personalmente.

2.4. Políticas para la documentación y mantenimiento de manuales de la Unidad de Gestión Informática

1. La Unidad de Gestión Informática, documentará formalmente todas las actividades que realice en el desarrollo de los servicios que brinda a la Institución.

2.5. Políticas para la adquisición de nuevas tecnologías

1. Todos los procesos institucionales de adquisición de recursos informáticos, deberán ser valorados y aprobados previamente por el Unidad de Gestión Informática.

2. Para la adquisición de nuevos recursos de hardware, software y otros dispositivos tecnológicos, la Unidad de Gestión Informática recomendará aquellos que ofrezcan calidad comprobada y sean referentes en el mercado nacional.

3. Para el trámite de adquisición de nuevos recursos informáticos, la Unidad de Gestión Informática asesorará y apoyará a la Unidad de Servicios Administrativos, en la definición de las características tecnológicas y evaluación de ofertas mediante recomendaciones técnicas.
4. Para la adquisición de nuevos recursos, la Unidad de Gestión Informática se fundamentará en los reglamentos y normativas de compras definidos para la Institución o proyecto de cooperación según sea el caso.
5. La Unidad de Gestión Informática y la Unidad de Servicios Administrativos velarán porque los recursos informáticos adquiridos sean enviados a y utilizados por la misma Dirección en que surgió la necesidad de compra.

2.6. Políticas sobre inventario de equipo

1. La Unidad de Gestión Informática mantendrá un inventario de equipo con las características de cada uno de ellos, tanto de la sede central como de las oficinas regionales.
2. La Unidad de Gestión Informática deberá revisar el inventario del equipo por lo menos una vez al año, realizando los cambios que sean necesarios. Hará un informe a la Dirección Administrativa Financiera con copia a la Gerencia General sobre las diferencias y/o deficiencias encontradas.

2.7. Políticas sobre reparación de equipos

1. Todos los usuarios deberán acatar el procedimiento que la Unidad de Gestión Informática implemente para controlar los servicios de reparación y la calidad de los mismos.
2. La obtención de fondos presupuestarios para la adquisición de repuestos y accesorios será gestionada a través de la Unidad de Gestión Informática, quedando condicionado a la factibilidad técnica y presupuestaria.
3. La Unidad de Gestión Informática en coordinación con la Unidad de Servicios Administrativos tendrá un control de las garantías de los equipos adquiridos para hacer cumplir los compromisos contractuales. Los equipos no cubiertos procederán a ser reparados en el sitio mismo o en el taller. Podrá además ser enviado a talleres externos especializados y el costo será gestionada a través de la

Unidad de Gestión Informática, quedando también condicionado a la factibilidad técnica y presupuestaria.

3. Políticas relativas a sistemas de Información

3.1. Políticas generales para el desarrollo de sistemas de información

1. La Unidad de Gestión Informática podrá recurrir al desarrollo sistemas de información por "outsourcing", cuando no cuente con el recurso humano y/o tecnológico necesario, para llevar a cabo los desarrollos de forma interna, además cuando otros factores como el tiempo no lo permitan.

2. En general para el desarrollo de sistemas "outsourcing", se regirá por las disposiciones establecidas en las leyes, reglamentos, manuales y procedimientos que les aplique.
3. El desarrollo de sistemas de información se hará mediante proyectos debidamente formalizados, administrados y de acuerdo con la metodología y estándares de la Unidad de Gestión Informática, los cuales estarán establecidos en su respectivo manual.
4. Las solicitudes de nuevos sistemas de información a desarrollar, deberán ser formalmente presentadas por las Jefaturas, con el formato y los requerimientos que la Unidad de Gestión Informática defina.
5. Las solicitudes de nuevos sistemas de información, promovidas por las diferentes dependencias de SENARA, serán evaluadas y aprobadas por la Comisión de Tecnologías de Información en conjunto con la Unidad de Gestión Informática de acuerdo a las prioridades establecidas en el PETIC.

6. El control y monitoreo del avance de proyectos de sistemas de información por "outsourcing" estará a cargo de la Unidad de Gestión Informática.
7. La Unidad de Gestión Informática estará pendiente que las empresas contratadas para el desarrollo de sistemas de información, brinden la capacitación a sus funcionarios en administración, uso y mantenimiento del nuevo sistema de información.

3.2. Políticas sobre mantenimiento de sistemas de información

1. Será considerado como mantenimiento de sistemas de información todas las acciones que impliquen modificaciones, correcciones, mejoras o adiciones a los sistemas de información, que soliciten los usuarios de cualquier dependencia del SENARA.

2. La Unidad de Gestión Informática definirá el procedimiento y las formalidades necesarias que orienten la forma en que serán desarrolladas las actividades de mantenimiento de sistemas de información.

3. En caso de requerirse mantenimiento de sistemas de información tipo "outsourcing", se aplicará las políticas anteriores "Políticas para el desarrollo externo ("outsourcing") de sistemas de información".

4. Políticas relativas a bases de datos.

4.1. Políticas para la creación de bases de datos

1. La Unidad de Gestión Informática permitirá la creación de bases de datos a empresas contratadas para este fin o para el desarrollo de sistemas de información, siempre que se desarrollen según los estándares definidos por la administración, y que entreguen la documentación técnica especificada mediante un manual.
2. En la creación de nuevas bases de datos se deberá generar la documentación necesaria y suficiente, que permita comprender su estructura física y lógica, así como su contenido.
3. En la definición de nomenclatura para las bases de datos, deberá respetarse el Manual de Estándares correspondiente elaborado por la Unidad de Gestión Informática.

4.2. Políticas para la migración de información de bases de datos

1. Toda migración de base de datos deberá ser realizada por personal técnico capacitado interno o personal externo, el cual deberá ser supervisado por un profesional de la Unidad de Gestión Informática.
2. Antes de cualquier proceso de migración se deberán realizar los respaldos respectivos, así como realizar previamente una prueba de la migración en un servidor de pruebas, para garantizar que el proceso de migración funciona correctamente.
3. En las actividades de migración de información a bases de datos, se deberá seguir el procedimiento definido por la Unidad de Gestión Informática para evitar atrasos y complicaciones, así como dejar documentado en una bitácora todo lo realizado para futuras migraciones.

4.3. Políticas sobre instalación de bases de datos

1. Toda instalación de base de datos deberá ser realizada por el personal técnico capacitado de la Unidad de Gestión Informática, o en su defecto por personal de empresas contratadas para estos efectos, bajo la supervisión de la Unidad de Gestión Informática.
2. Antes de cualquier instalación deberán realizarse los respaldos respectivos para evitar accidentes y garantizar la recuperación de la base de datos.
3. Para la instalación de bases de datos se deberá seguir el procedimiento definido por la Unidad de Gestión Informática para prevenir que se den atrasos o complicaciones, así como dejar documentado en una bitácora todo lo realizado.

4.4. Políticas sobre administración y mantenimiento de bases de datos

1. Todo mantenimiento a las bases de datos deberá ser realizado por personal técnico capacitado interno o externo, quienes deberán ser supervisados por el profesional responsable de esa tarea de la Unidad de Gestión Informática.
2. Antes de cualquier proceso de mantenimiento a la base de datos, se deberán realizar los respaldos respectivos para estar prevenidos contra cualquier accidente que se pudiera presentar.
3. Todo cambio o ajuste hecho en el proceso de mantenimiento, se deberá dejar documentado en una bitácora para efectos de control y seguimiento.
4. La Unidad de Gestión Informática deberá garantizar la conservación permanente de toda la información almacenada en las bases de datos de los servidores, que esté directa o indirectamente relacionada con las actividades del SENARA.
5. La información deberá ser conservada durante el período que se defina en la tabla de plazos de conservación, labor en la cual tendrá concurso el Archivo Central Institucional.
6. Todo acceso a las bases de datos del SENARA deberá contar con los mecanismos adecuados y controlados, que garanticen su seguridad, su integridad y la confidencialidad de la información almacenada.
7. Toda transacción que se ejecute en las bases de datos, dejará las pistas adecuadas de auditoría, para poder ejercer un control adecuado, de todas las modificaciones que se hagan en éstas mediante el uso de bitácoras.
8. Deberán de mantenerse y aplicarse sistemas de respaldos para todas las bases de datos del SENARA, con el fin de garantizar su conservación.
9. Deberán existir planes de recuperación de la información de las bases de datos, para garantizar la continuidad del servicio que se presta por medio de los sistemas de información.

4.5. Políticas de seguridad en bases de datos

1. Todo acceso a las bases de datos del SENARA deberá contar con los mecanismos adecuados y controlados, que garanticen su seguridad, su integridad y la confidencialidad de la información almacenada.
2. Toda transacción que se ejecute en las bases de datos, dejará las pistas adecuadas de auditoría, para poder ejercer un control adecuado, de todas las modificaciones que se hagan en éstas mediante el uso de bitácoras.
3. Deberán de mantenerse y aplicarse sistemas de respaldos para todas las bases de datos del SENARA, con el fin de garantizar su conservación.

5. Políticas relativas a redes y telecomunicaciones

5.1. Políticas para el uso de las redes de datos

1. La Unidad de Gestión Informática será la dependencia responsable de la administración y uso de la red interna de datos.
2. La Unidad de Gestión Informática garantizará el acceso controlado en la red interna de datos a los funcionarios del SENARA que así lo requieran.
3. Los usuarios accederán a la red de datos por medio de un usuario y contraseña que les asignará el administrador de la red.
4. El usuario y contraseña que se asigne será único y exclusivo para cada usuario, el cual será responsable por su uso.
5. Todas las operaciones que se efectúen por medio de las redes internas serán responsabilidad única del usuario al que se le asignó el usuario y contraseña relacionado con las mismas.
6. La Unidad de Gestión Informática monitoreará periódicamente los accesos a la red interna mediante herramientas de seguridad y administración.
7. No es permitido a ningún funcionario, excepto a los técnicos de redes, manipular los componentes activos de la red (switches, routers, dispositivos inalámbricos, cableado, etc.).
8. No se permitirá la instalación de puntos de acceso de redes inalámbricas con conexión a la red del SENARA sin la debida información y autorización de la Unidad de Gestión Informática. En caso de detección de un punto de acceso no autorizado se procederá a su inmediata desconexión de la red Institucional.
9. No estará permitida la conexión de equipos con nombres o direcciones no registrados.

10. No se permitirá el empleo de mecanismos para la manipulación de direcciones de red o cualquier otro uso que pueda afectar a la topología o a la estructura lógica de la red.
11. La Unidad de Gestión Informática solamente prestará apoyo a los equipos conectados a la red institucional; a estos efectos, se consideran conectados a la red del SENARA los equipos que accedan a la misma de forma remota a través de los medios proporcionados por la Unidad de Gestión Informática.
12. Los equipos electrónicos de gestión e infraestructura de la red del SENARA serán instalados, configurados y mantenidos exclusivamente por la Unidad de Gestión Informática.
13. Ningún usuario está autorizado a utilizar analizadores del tráfico que circula por la red del SENARA. Igualmente está prohibido utilizar herramientas de rastreo de puertos o que permitan detectar vulnerabilidades. El uso de estas herramientas sólo está permitido a los administradores de la red y bajo situaciones especiales (incidentes de seguridad, denuncias de usuarios, etc.) que lo justifiquen.
14. La Unidad de Gestión Informática pondrá en funcionamiento herramientas de control que posibiliten detectar, analizar y bloquear accesos no permitidos, (aquellos que no guarden relación con aspectos de trabajo) que pongan en riesgo la seguridad de los recursos informáticos y atenten contra su desempeño.

6. Políticas relativas al servicio de Internet y correo electrónico

6.1. Políticas para el acceso a servicios de Internet y correo electrónico

1. Los servicios de Internet y correo electrónico serán administrados por la Unidad de Gestión Informática.
2. Para la comunicación oficial del SENARA deberá utilizarse la cuenta de correo institucional, en la medida de las posibilidades.
3. El acceso a los servicios de Internet y correo electrónico estarán disponibles para todos los usuarios del SENARA, si las condiciones de infraestructura tecnológica y administrativa lo permiten.
4. El correo electrónico institucional es será una herramienta de comunicación e intercambio oficial de información y no una herramienta de difusión indiscriminada de información.
5. El uso de los servicios de Internet y correo electrónico deberá ser exclusivamente para apoyar y mejorar la calidad de las funciones administrativas y técnicas.
6. La Unidad de Gestión Informática asignará las cuentas de correo de acuerdo a las licencias disponibles.
7. Está prohibido facilitar u ofrecer las cuentas de correo a terceras personas.

8. Se prohíbe a los empleados formar parte de cadenas de mensajes o SPAM, ya que esto contribuye a la saturación de las redes de telecomunicación y facilita la divulgación de su cuenta de correo y la proliferación de virus en la red.
9. Se prohíbe a los funcionarios que tengan acceso al servicio de correo electrónico abrir mensajes de procedencia desconocida.
10. El funcionario que tenga acceso a servicios de correo electrónico deberá evitar divulgar su cuenta a personas o entes desconocidos.
11. Ningún equipo que esté designado como servidor deberá tener asociada una cuenta de correo electrónica.
12. Los mensajes de correo electrónico deberán ser considerados como documentos formales y deberán respetar todos los lineamientos referentes al uso inapropiado del lenguaje.
13. Los funcionarios deberán realizar revisiones periódicas de los mensajes almacenados con el fin de no mantener información innecesaria.
14. La Unidad de Recursos Humanos deberá notificar a la Unidad de Gestión Informática cuando se deba crear, cerrar o inhabilitar una cuenta de correo electrónico.
15. El usuario deberá atender a los avisos de actualización automática del programa de detección de virus e informar a la Unidad de Gestión Informática, cuando la actualización no se realice satisfactoriamente.
16. Los valores de seguridad, de aceptación de cookies y los certificados de los navegadores o browser no deberán ser cambiados, excepto por indicaciones de la Unidad de Gestión Informática.
17. Para el envío de mensajes se aplicarán las siguientes reglas:
    a) Se utilizará siempre el campo de Asunto, a fin de resumir el tema del mensaje. b) No se enviarán mensajes a personas desconocidas, a menos que se trate de un asunto oficial que las involucre.
    c) No se enviarán mensajes a listas globales, a menos que el propietario sea la persona autorizada por el superior para enviar mensajes que involucren a toda la Institución.
    d) La divulgación de mensajes de interés general (actividades internas, invitaciones, notas luctuosas, entre otros) deberá coordinarse con la Unidad de Recursos Humanos la cual definirá el procedimiento para tal fin.
    e) En caso de que fuera necesario un envío masivo se recomienda usar las listas de distribución o usar el campo de "copia oculta" (Bcc ó Cco) para poner la lista de destinatarios, o bien ponerse en contacto con la Unidad de Gestión Informática.

18. Está prohibida la utilización abusiva del correo electrónico y de las listas de distribución incluyendo la realización de prácticas tales como:
    - ✓ Publicación de actividades comerciales privadas.

- ✓ Propagación de cartas encadenadas o participación en esquemas piramidales o actividades similares.
- ✓ Uso del insulto, la amenaza o la difamación a cualquier persona.
- ✓ Suscribirse a periódicos, revistas, semanarios, buscadores de parejas, chats; ni a ningún otro tipo de actividades o boletines electrónicos que no sea el estrictamente relacionado con el área profesional de trabajo del funcionario.
- ✓ Descargar archivos de música, programas, videos, pornografía y cualquier otro tipo de información que no guarde estricta relación con el área profesional del funcionario. La Unidad de Gestión Informática procurará tomar las previsiones del caso para que se bloquee por medio de software especializado, el acceso no autorizado a los servicios antes mencionados.

7. Políticas relativas al hardware

7.1. Políticas de responsabilidad

1. El hardware que se encuentra en el área de servidores y los armarios de comunicaciones es responsabilidad directa del personal de la Unidad de Gestión Informática, que tendrá que velar por su uso y cuidado.
2. Los otros equipos de cómputo quedarán bajo la responsabilidad del usuario al que se asignen. Estos tendrán la obligación de cuidarlos, mantenerlos limpios y velar por su buen funcionamiento. En el caso de existir algún problema con el equipo deberán de reportarlo inmediatamente a la Unidad de Gestión Informática para que se proceda a su revisión.
3. Los equipos portátiles (laptops, agendas electrónicas, tablets, HandHeld, celulares, etc), serán asignadas a los usuarios con el objetivo de cumplir sus funciones y no deberán utilizarlos para uso personal.
4. Es responsabilidad del usuario custodiar los equipos portátiles asignados; por lo que deberá tomar las medidas de seguridad correspondientes dentro y fuera de la institución para evitar el robo del equipo o información. En caso de robo, se regirá por lo establecido en el manual de activos fijos.
5. Queda entendido que los recursos informáticos asignados a cada usuario lo serán en calidad de herramienta de trabajo; como tal se encuentran permanentemente bajo dominio y control del SENARA, sin perjuicio del derecho a la privacidad de la información almacenada y demás derechos fundamentales establecidos por la Constitución Política.
6. Será responsabilidad de la Unidad de Gestión Informática hacer cumplir las garantías respectivas de cada uno de los equipos; para tal razón se deberán

respetar los sellos de garantía que vienen adheridos a los equipos, y velar porque el usuario final no los despegue.

7. Será responsabilidad de la Unidad de Gestión Informática valorar la necesidad de sustituir algún equipo cuando ya éste no garantice la funcionalidad y operatividad adecuada.

7.2. Políticas de mantenimiento del hardware instalado

1. Los usuarios tendrán el deber de informar sobre el rendimiento de cada equipo, para que sea valorado y de ser necesario mejorado.
2. Las ampliaciones, modificaciones o adquisición de equipo de cómputo, así como la actualización y compra de software, se harán únicamente por funcionarios de la Unidad de Gestión Informática.
3. La entrega, puesta en funcionamiento y cambio de equipo entre las diferentes dependencias del SENARA, se efectuará en coordinación con la Unidad de Gestión Informática y la Unidad de Servicios Administrativos, utilizando para ello los procedimientos establecidos al efecto.
4. En el caso de fallas técnicas del equipo de cómputo, la Unidad de Gestión Informática realizará un diagnóstico preliminar, con el objeto de procurar la solución, o en su defecto, girar las instrucciones del procedimiento a seguir para su reparación.
5. Los equipos de cómputo no podrán ser desmantelados, cambiados, abiertos ni reparados por los usuarios de las oficinas. Asimismo, sus componentes (entiéndase "mouse", disco duro, teclado, memoria, fuente de poder, tarjeta madre, entre otros) no podrán ser removidos por personal no autorizado por la Unidad de Gestión Informática , salvo aquellos casos específicos autorizados por la Unidad de Gestión Informática para atención de fallas técnicas en equipos de cómputo de las oficinas regionales.

7.3. Políticas de resguardo de Activos informáticos

1. La Unidad de Servicios Administrativos llevará y mantendrá el inventario de los recursos informáticos así como el control de la ubicación de los equipos de cómputo en las dependencias del SENARA.
2. Cada Dirección o Unidad debe asignar un responsable de elaborar y mantener su inventario de recursos informáticos y deberá informar a su superior inmediato y a la Unidad de Gestión Informática, sobre cualquier cambio del estado o ubicación del activo.

3. Los equipos de cómputo no podrán ser trasladados a otras oficinas que no sean del SENARA, salvo para alguna situación específica siempre que se cuente con la debida autorización de la Dirección Administrativa, lo cual se hará del conocimiento de la Unidad de Gestión Informática.

7.4. Políticas para el desecho de equipos electrónicos

1. Los equipos electrónicos a ser desechados, serán revisados por funcionarios de la Unidad de Gestión Informática, generando un acta de desecho la cual será entregada a la Unidad de Servicios Administrativos como evidencia de su daño u obsolescencia para que proceda con el respetivo desecho.
2. El SENARA procurará la entrega de sus desechos tecnológicos a empresas recicladoras que cumplan con las normativas vigentes de protección al medio ambiente.

8. Políticas relativas al software

8.1. Políticas sobre el uso de licencias de software

1. La Unidad de Gestión Informática dará la asesoría necesaria a los funcionarios del SENARA en el tema de licencias. Los usuarios deberán asegurarse que disponen de las licencias adecuadas al software en uso, ya sea mediante licencias adquiridas de forma centralizada por el SENARA (para software de uso común), por la adquisición individual de las correspondientes licencias, o bien por el uso de software libre. De no ser así, la responsabilidad recaerá totalmente sobre el usuario.
2. El Unidad de Gestión Informática llevará un registro actualizado de los equipos y las licencias vigentes en el SENARA para informar a las respectivas instancias a este respecto.
3. Se prohíbe la instalación de software propiedad del SENARA en equipos que no pertenezcan a la institución. En los casos de convenios de cooperación deberá existir una cláusula que así lo permita.
4. El Unidad de Gestión Informática dará de baja todos los equipos que estén al margen de la ley, en lo que respecta al cumplimiento de la Ley de Derechos de Autor, lo cual se hará en un plazo razonable que será comunicado al responsable de la dirección o unidad respectiva.
5. La Dirección Administrativa Financiera gestionará mediante los presupuestos ordinarios y extraordinarios, la compra de licencias de "software" con la finalidad de que siempre el SENARA se mantenga al día con el uso de licencias. Esta función la hará mediante el concurso y petición de la Unidad de Gestión Informática.

6. La Unidad de Gestión Informática removerá cualquier programa de las máquinas cuando no exista licencia, sin responsabilidad para ésta de los problemas que ocasione directa o indirectamente. Llevará un registro de los programas instalados ilegalmente, para que, ante la reincidencia de mantener programas instalados en forma ilegal, se proceda a reportar el asunto a la Unidad de Recursos Humanos o ante las autoridades superiores, para aplicar la sanción que corresponda por desobediencia según el Reglamento Autónomo de Trabajo del SENARA, lo cual debe tipificarse como falta grave. Para ello, la Unidad de Gestión Informática cuidará de no violentar el derecho a la privacidad de las personas, solicitando previamente la autorización al usuario para proceder con la remoción del programa ilegal.
7. Los medios de instalación originales o acceso a los portales de descarga serán custodiados por la Unidad de Gestión Informática.

8.2. Políticas para la instalación de Software

1. La Unidad de Gestión Informática es será la responsable de la instalación de los programas de software en cada una de las computadoras del SENARA.
2. Queda completamente prohibido a los usuarios realizar instalaciones de cualquier tipo de software en sus computadoras. De requerir un software específico deberá solicitarse a la Unidad de Gestión Informática para que se valore la necesidad de su instalación.
3. Todo software que se instale en las computadoras del SENARA deberá contar con su respectiva licencia y su instalación deberá ser autorizada por la jefatura de la Unidad de Gestión Informática.
4. Queda prohibida la instalación del software adquirido por el SENARA en equipos que no sean de su propiedad.
5. El personal de la Unidad de Gestión Informática deberá mantener un inventario de software y programas instalados en cada una de las computadoras. Este inventario deberá revisarse y actualizarse una vez al año en coordinación con la Dirección Administrativa Financiera.
6. Para la administración y el manejo seguro de la información que se almacena en los computadores del SENARA y para evitar su utilización por personas no autorizadas, se utilizarán los sistemas operativos que ofrezcan mayor seguridad.
7. Conforme se adquieran nuevas versiones del Software, la Unidad de Gestión Informática realizará la respectiva instalación en los equipos de la institución.
8. El software que deberá residir en el disco duro de cada computadora y ser utilizado por los usuarios, es aquel que haya instalado la Unidad de Gestión Informática. En consecuencia, por ningún motivo los usuarios del SENARA, podrán instalar en los

discos duros de las computadoras, ni utilizar por medio de Discos Compactos, llaves USB u otro medio, software no autorizado.

9. En caso de que los usuarios requieran instalar, ejecutar, o copiar de Internet programas (software) diferentes al instalado en sus equipos, deberán coordinar previamente con la Unidad de Gestión Informática. Lo anterior, con el fin de evitar riesgos legales o de funcionamiento de los equipos.

9. Políticas relativas a la seguridad

9.1. Políticas generales de seguridad de acceso

1. La Unidad de Gestión Informática será la responsable de la seguridad de acceso a los sistemas operativos, sistemas de información, bases de datos, y redes que operen en los equipos de cómputo del SENARA.
2. La Unidad de Gestión Informática establecerá los mecanismos adecuados para el control, verificación y monitoreo de cambios en passwords, número de sesiones activas, seguridad lógica, física, de todas las actividades relacionadas con el uso de tecnologías de información.
3. Para evitar situaciones de peligro para el SENARA, se desactivarán o bloquearán las cuentas de usuario a aquellas personas que estén en vacaciones, con permisos o incapacidades mayores a un mes, para lo cual deberá informar la jefatura respectiva.
4. En caso de despido de un funcionario, el permiso de acceso deberá desactivarse o bloquearse previamente a la notificación de la persona sobre la situación. La Unidad de Recursos Humanos deberá notificar a la Unidad de Gestión Informática cuando se deba crear, cerrar o inhabilitar los accesos a un funcionario.
5. El administrador de los sistemas operativos, sistemas de información, bases de datos o redes asignará la clave de acceso al usuario.
6. La Jefatura que esté a cargo de la dependencia será responsable de notificar por escrito a la Unidad de Gestión Informática sobre el ingreso, salida o traslado de un usuario a su cargo. Esto con el fin de que se creen, inhabiliten, modifiquen o eliminen los privilegios de acceso a las diferentes plataformas, dominios y dispositivos correspondientes.
7. La Unidad de Gestión Informática no cambiará ninguna clave de acceso, si no es por solicitud expresa de su dueño. En caso de ser necesario y a solicitud de la jefatura se bloquearán los accesos de un usuario específico.
8. Cada usuario deberá salvaguardar la confidencialidad de la clave de acceso (password) y abstenerse de facilitarla a terceros por cualquier motivo. Cada usuario será responsable de las acciones que se reporten ejecutadas con clave de

acceso. En los casos de sustitución, se asignará al sustituto, un nombre de usuario y una clave de acceso transitoria y nunca la correspondiente a la persona sustituida.

9. Cada usuario generará sus propias claves de acceso, cada cierto período de tiempo en la medida que las posibilidades técnicas que así lo permitan. Las conformará mediante el empleo de letras mayúsculas, minúsculas y números. El período lo establecerá la Unidad de Gestión Informática, dependiendo de la sensibilidad de la información.
10. El usuario no deberá dejar las claves de acceso escritas en medios o lugares donde puedan ser obtenidas por terceros (Ej.: monitor, carpetas, escritorio)
11. Cuando el usuario olvide u extravié su clave de acceso, deberá acudir a la Unidad de Gestión Informática e identificarse como propietario de la cuenta para que se le proporcione una nueva, o la utilización de cualquier otro medio de verificación que la Unidad de Gestión Informática defina para la restauración de contraseñas.
12. La clave de acceso nunca deberá ser compartida o revelada; hacer esto responsabiliza al usuario que prestó su clave de acceso, de todas las acciones que se realicen con la misma.
13. La Unidad de Gestión Informática implementará estrategias para que se generen clases de acceso con niveles adecuados de seguridad.
14. Los usuarios deberán aplicar medidas preventivas cuando se ausentan de las labores, antes de retirarse del lugar de trabajo donde se ubique el equipo de cómputo. El usuario deberá tomar las siguientes precauciones mínimas:
    a) Concluir las sesiones activas de cualquier sistema informático al finalizar las tareas;
    b) Proteger el equipo contra usos no autorizados mediante un mecanismo de bloqueo de seguridad autorizado por la Institución;
    c) Cerrar la conexión con los servidores.
15. Bajo ninguna circunstancia deberá compartirse la cuenta de usuario de Dominio o de Computadora asignada por el SENARA, ni la clave de acceso a dicha cuenta. Estas deberán manejarse conforme lo establezca la normativa interna del SENARA y el usuario a quien se le asigne será el único responsable del uso que les dé.
16. Está prohibido el almacenamiento, la transmisión, transferencia y difusión de datos de carácter personal en los equipos del SENARA, sin contar con autorización válidamente emitida por quien esté legitimado para ello.
17. Los activos y recursos informáticos no deberán conectarse a sistemas de cómputo ajenos al SENARA, a menos que sea estrictamente necesario para el cumplimiento de sus fines, en cuyo caso deben darse las siguientes condiciones:
    a) Que se sigan los procedimientos de seguridad adecuados para proteger la información propiedad del SENARA o que esté bajo su custodia.
    b) Que la conexión sea autorizada por la Unidad de Gestión Informática.
18. En el caso de los funcionarios a quienes se les otorgue permiso con o sin goce de salario o para aquellos que concluyen su relación laboral con la institución, la

Unidad de Recursos Humanos de la Dirección Administrativa Financiera, de inmediato pondrá esta situación en conocimiento de la Unidad de Gestión Informática, con el fin de que las correspondientes cuentas de correo, nombre de usuario y clave de acceso, sean temporalmente suspendidas o eliminadas, según corresponda.

9.2. Políticas de seguridad de acceso a sistemas operativos

1. La activación y desactivación de usuarios de sistemas operativos estará a cargo del personal técnico de la Unidad de Gestión Informática.
2. En la activación de usuarios de sistemas operativos, se crearán identificadores de usuario utilizando el estándar de la letra inicial del nombre seguida del primer apellido.
3. Siempre que los sistemas operativos utilizados lo permitan, deberá controlarse el número de intentos de ingreso fallidos. Luego de un determinado número de intentos, deberá bloquearse la cuenta del usuario y no permitir su ingreso al sistema. La cuenta deberá estar bloqueada por 30 minutos y el administrador de seguridad podrá desbloquearla antes por solicitud del usuario involucrado.
4. En el caso que el sistema operativo lo permita, se deberán implementar las bitácoras de seguimiento a los accesos, donde se registren los ingresos al sistema y los intentos fallidos.

9.3. Políticas de seguridad de acceso a sistemas de información

1. La activación y desactivación de usuarios de los sistemas de información estará a cargo del personal técnico de la Unidad de Gestión Informática.
2. La Unidad de Gestión Informática asignará la clave de acceso al usuario.
3. Para otorgarle acceso a las diferentes aplicaciones del sistema, de acuerdo con las funciones que debe desempeñar el usuario, la jefatura correspondiente deberá hacer la solicitud formal a la Unidad de Gestión Informática.
4. En toda transacción que se realice en el sistema se deberá grabar el nombre del usuario, la fecha y la hora en que se realizó.

9.4. Políticas de seguridad de acceso a bases de datos

1. La Unidad de Gestión Informática velará porque toda base de datos que sea instalada, cuente con los controles de seguridad que garanticen la confiabilidad de la información.

2. Los códigos de acceso de los usuarios a las bases de datos, utilizarán el estándar indicado en los manuales o procedimientos establecidos por la Unidad de Gestión de TI.
3. El administrador de la base de datos asignará la clave de acceso al usuario.
4. El sistema de seguridad deberá contemplar el bloqueo de claves luego de tres intentos fallidos de acceso, cuando la base de datos lo permita.
5. La Unidad de Gestión Informática implementará controles para que todos los respaldos de información se encuentren almacenados en medios externos como disco duro, Unidad de respaldo USB, CD's o DVD's.
6. Los diferentes centros de datos del SENARA se respaldarán mutuamente en sus servidores y los medios físicos se resguardarán en los diferentes sitios.

9.5. Políticas de seguridad de acceso a redes

1. El administrador de redes asignará las claves de acceso a los usuarios, además procederá conforme con la activación y desactivación de usuarios de las redes del SENARA.
2. Para la utilización de las redes de datos, los nombres de usuario para las mismas se crearán siguiendo el esquema de letra inicial del nombre seguido por el primer apellido.
3. Para otorgarle acceso a las redes de datos, de acuerdo con las funciones que debe desempeñar el usuario, la jefatura correspondiente deberá enviar la solicitud formal a la Unidad de Gestión Informática.

9.6. Políticas de ubicación de los centros de procesamiento de información y comunicaciones

1. Los centros de procesamiento de información y comunicaciones deberán estar ubicados dentro del edificio del SENARA, a menos que se disponga instalarlos en sitios externos especializados con la seguridad necesaria.
2. Los centros de Datos deberán estar completamente cerrados y con una única puerta de acceso, la cual deberá permanecer siempre cerrada. Las llaves de acceso estarán en custodia del personal de la Unidad de Gestión Informática.
3. Todo el cableado eléctrico que sea utilizado en los equipos de los centros de procesamiento de información y comunicaciones deberá ser totalmente independiente al cableado normal del edificio.
4. Para efectos de cableado eléctrico y de datos se utilizarán las normas de cableado que se fundamenten en las mejores prácticas utilizadas en el mercado.

9.7. Políticas de ambiente de los centros de procesamiento de información y comunicaciones

1. El área asignada para los centros de procesamiento de información y comunicaciones deberá estar dotada con las condiciones ambientales necesarias para garantizar un entorno físico conveniente para su funcionamiento.
2. El espacio de los centros de procesamiento de información y comunicaciones deberá estar climatizado permanentemente a una temperatura que se encuentre entre los 18° y 20° para garantizar el mejor rendimiento de los componentes electrónicos y alargar la vida útil de los mismos.

9.8. Políticas sobre "Responsabilidad de funcionarios por uso de los equipos"

1. Los funcionarios del SENARA usarán el equipo de cómputo en labores exclusivamente de trabajo y serán responsables por el uso adecuado de las herramientas tecnológicas.
2. Los usuarios deberán abstenerse de utilizar los recursos informáticos de la institución para realizar actividades personales o con fines lucrativos. Los recursos asignados deberán ser utilizados únicamente para cumplir los objetivos organizacionales.
3. El costo por la reparación o sustitución de los equipos de cómputo a raíz de los desperfectos causados por situaciones de descuido en su uso, lo asumirá el usuario responsable, sin perjuicio de las sanciones disciplinarias que correspondan, para lo cual se seguirá el respectivo procedimiento administrativo.
4. Será prohibido a todos los funcionarios de cualquier nivel, utilizar el equipo de la oficina para bajar de internet: juegos, música, videos, fotos, "screensavers" y todo archivo que provenga de fuentes no confiables; así como todo tipo de material pornográfico, que atenta contra el trabajo o el honor de las personas.
5. Ningún usuario estará autorizado para almacenar material pornográfico, u ofensivo en ningún medio de almacenamiento de las computadoras, dispositivos periféricos u otro dispositivo de almacenamiento, mucho menos propagarlo a otras personas.
6. La Unidad de TI y la Unidad de Servicios Administrativos, deberán velar porque el equipo tenga protección contra fallas de energía eléctrica o reducciones de voltaje.
7. La Unidad de TI deberán utilizar antivirus actualizados para revisar todo medio antes de ingresarlo al equipo, con el propósito de evitar que éste sea contagiado al igual que la red institucional. Si no tienen instalado los antivirus tendrán la responsabilidad de notificarlo a la Unidad de Gestión Informática.

8. Los usuarios de equipos deberán procurarse los conocimientos imprescindibles para el manejo de sus programas, así como realizar copias de seguridad de los datos que consideren relevantes, lo cual puede resultar verdaderamente importante cuando los discos duros colapsen por cualquier razón.
9. Todo usuario será responsable de mantener respaldos de la información de acuerdo a sus necesidades. En caso de las aplicaciones el responsable por los respaldos es el administrador de la red y si es del caso, el Administrador de la Base de Datos.
10. Por razones de seguridad se prohíbe el uso de mensajería instantánea, chat o similares a menos que se justifique el uso para lo cual debe solicitarse por la jefatura a la Unidad de Gestión Informática, manifestándose los cuidados y supervisión que ejercerá sobre su uso.
11. Está prohibido a los funcionarios del SENARA, conectarse a Internet utilizando equipos no autorizados a los que oficialmente se encuentren en servicio.
12. Las computadoras son propiedad de la institución y son asignadas a los funcionarios para que desarrollen sus funciones.

9.9. Políticas para el aseguramiento de la Calidad de los desarrollos informáticos.

1. Deberá existir un plan de pruebas de aceptación de los sistemas, los cuales deberán ser coherente con los requisitos, la especificación funcional del sistema y la infraestructura existente.
2. El plan de pruebas de aceptación, deberá incluir todos los recursos necesarios (Humanos, Materiales así como de Hardware y Software).
3. Se deberán realizar los siguientes tipos de pruebas:
    - ✓ Pruebas unitarias (pruebas ejecutadas por el desarrollador del módulo del sistema o de la modificación requerida, su objetivo es validar la funcionalidad del módulo en forma aislada).
    - ✓ Pruebas conjuntas (pruebas ejecutadas por todos los desarrolladores de cada uno de los módulos del sistema, su objetivo es validar la funcionalidad del sistema completo).
    - ✓ Los usuarios involucrados deberán realizar pruebas de aceptación de los sistemas antes de su liberación al ambiente de producción.
    - ✓ La Unidad de Gestión Informática deberá asegurar el cumplimiento de los estándares establecidos para todo el ciclo de vida de desarrollo del proyecto.

4. Si existe un sistema anterior, el sistema nuevo se pondrá en producción de forma coordinada con la retirada del anterior, migrando los datos si es necesario.

5. En caso de aplicar, deberá haber un período de funcionamiento en paralelo de los dos sistemas (nuevo y anterior), hasta que el nuevo esté funcionando con todas las garantías. Sin exceder los tiempos en el paralelo definidos entre los usuarios y Sistemas.
6. De aplicar, el sistema anterior sólo se deberá usar en modo de consulta, únicamente para obtener información, sólo en el caso de que la información del sistema anterior no ha sido migrada al nuevo.
7. Los usuarios responsables deberán emitir un documento de liberación del sistema a producción.
8. Dependiendo de la naturaleza del proyecto se recomienda realizar un procedimiento para llevar a cabo el mantenimiento. Este deberá estar aprobado por la Unidad de Gestión Informática y los usuarios responsables.
9. El procedimiento para realizar el mantenimiento deberá tener en cuenta los tiempos de respuesta máximos que se pueden permitir ante situaciones de no funcionamiento.
10. Para reportar y dar seguimiento a cualquier problema o para el mantenimiento del sistema deberá aplicarse el procedimiento de establecido por el Unidad de Gestión Informática para estos efectos.

9.10 Política de Administración de Riesgos

Establecer un marco de control y gestión del ciclo de vida de los riesgos asociados a las tecnologías de información, considerando su costo-beneficio y definiendo los planes de acción que debe ser comunicado y aprobado por el órgano competente en materia de riesgo tecnológico.

Los lineamientos para la administración de riesgos de las tecnologías de información se detallan en los siguientes apartados:

9.1 La Unidad de Gestión Informática realizará revisión anual de la administración de riesgos en los procesos administrativos.

9.2 La responsabilidad en el seguimiento y tratamiento a los riesgos de cada proceso es del Jefe de Proceso y de los riesgos de contexto estratégico es de la Jefatura de la Unidad de Gestión Informática.

9.3 Un plan de manejo de riesgos es igual que un mapa de riesgos.

9.4 No todos los riesgos de los procesos están registrados en el Plan de Manejo de Riesgos Institucional, pues éste sólo contiene aquellos riesgos priorizados en los procesos y que tengan mayor impacto en los objetivos institucionales.

9.5 Los auditores internos evaluarán en cada ciclo de auditoría que los procesos de acuerdo a la metodología establecida tengan identificados los riesgos y les den tratamiento.

10. Política para la definición del Modelo de Arquitectura y Estandarización de TI

Los lineamientos para la definición de la administración las tecnologías de información se detallan en los siguientes apartados:

10.1 Estándar de sintaxis de datos

- Todas las contrataciones de desarrollo o mantenimiento de software, deberán cumplir con el modelo de arquitectura de información definido por la Unidad de Gestión Informática de SENARA.

- La Unidad de Gestión Informática del SENARA deberá revisar periódicamente con miras a actualizar el estándar de sintaxis de datos de acuerdo a las últimas tendencias tecnológicas.

10.2 Estándar de programación (diccionario de datos)

- Todas las contrataciones de desarrollo o mantenimiento de software, deberán referenciar el estándar de programación y diccionario de datos en el pliego de cartel licitatorio de tal forma que el adjudicatario cumpla con el modelo de arquitectura de información del SENARA.

- La Unidad de Gestión Informática del SENARA deberá revisar periódicamente con miras a actualizar el estándar de programación de acuerdo a las últimas tendencias tecnológicas.

- La Unidad de Gestión Informática del SENARA deberá clasificar toda su documentación según el estándar de clasificación de documentación.

- La Unidad de Gestión Informática deberá garantizar la integridad y consistencia de todos los datos almacenados.

10.3 Estado

Se refiere al estado de la política los cuales pueden ser:

- ***Para aprobación***: la Unidad de Gestión Informática entrega el documento para revisión.

- ***En revisión por parte de***: la Gerencia General.

- ***Aprobado***: el departamento a cargo de la revisión dispone de ocho días hábiles para la aprobación, si procede, del documento.

Nivel de Aprobación - Se refiere al nivel de aprobación requerido para que la política sea oficial, dicho nivel depende del alcance de la política. A saber:

- Nivel 1: Jefatura de Unidad
  Alcance solo aplica a la Unidad de Gestión Informática.

- Nivel 2: Comité Tecnologías de Información.
  Alcance es institucional y su afectación queda a nivel de plan táctico y/u operativo de TI.

- Nivel 3: Junta Directica
  Alcance es institucional y su afectación es a nivel de plan estratégico de TI.

II. Políticas relativas al cumplimiento de las normas

1. Para la sana administración de sus sistemas informáticos y a fin de evitar y controlar instrucciones maliciosas, personal autorizado de la Unidad de Gestión Informática procederá a llevar a cabo revisiones periódicas en los sistemas y equipos de cómputo institucionales, a fin de garantizar que se encuentran libres de códigos malignos, así como asegurar que los usuarios posean instalado el software estándar y/o aprobado por el SENARA. Esta actividad siempre se realizará en presencia del usuario encargado del equipo.
2. La jefatura o encargado de cada dependencia será el responsable de velar por que estas disposiciones se cumplan y reportará a la mayor brevedad a la Unidad de Gestión Informática cualquier anomalía que se presente. Asimismo, la Jefatura podrá también solicitar a la Unidad de Gestión Informática una revisión técnica del sistema informático en aquellas dependencias donde existan indicios de una utilización inadecuada de éstos.
3. La Unidad de Gestión Informática del SENARA, será el ente contralor de la administración de los recursos informáticos en el SENARA.
4. Las faltas cometidas al tenor de lo dispuesto en el presente documento, serán sancionadas de conformidad con las disposiciones establecidas en el Reglamento Autónomo de la Institución y el Código de Trabajo así como las demás disposiciones vigentes y aplicables, sin perjuicio de las responsabilidades civiles y penales que deba asumir el infractor.

Glosario de términos utilizados

A continuación se presentan en orden alfabético una serie de términos que son utilizados en el presente reglamento:

Área de Tecnologías de Información: lugar físico específico donde se encuentra equipo de cómputo especializado.
Base de Datos: Conjunto de datos organizados de tal modo que permita obtener con rapidez diversos tipos de información.
Browser: Programa o aplicación informática que se usa para navegar por las redes informáticas y acceder a documentos, imágenes y demás información.
CD: Siglas en inglés de Disco Compacto (Compact Disk), placa circular de material plástico donde se graba información por medio de láser codificado.
Chat: Conversación interactiva en tiempo real, en Internet.
Cookies: Archivo que se implanta en el disco duro del usuario por el sitio visitado en Internet, contiene información acerca del usuario.
Correo Spam: Se utiliza este término para identificar todo aquel correo denominado como "Correo Basura" o correo no deseado.
Hardware: junto de componentes que integran la parte material de una computadora, impresora o equipo de comunicación.
Internet: Red informática de comunicación internacional que permite el intercambio de todo tipo de información entre sus usuarios. El nombre proviene del acrónimo de las palabras inglesas International Network (red internacional).
Normativa: Conjunto de normas aplicables a una determinada materia o actividad.
Outsourcing: término en idioma inglés para La subcontratación, externalización o tercerización
Perfil de usuario: Grupo de privilegios o roles de trabajo que se asignan a una persona, de acuerdo con las características que tenga su puesto con el fin de que pueda desempeñar sus funciones.
Rol: Grupo de derechos o privilegios para el uso de recursos informáticos que asignan a uno o más usuarios, por ejemplo: derechos de lectura, escritura, modificación o borrado sobre una tabla de datos.
Recuperación: Es la tarea que se lleva a cabo cuando es necesario volver al estado de la aplicación al momento del último respaldo, a partir de los datos de la última copia de seguridad realizada.
Respaldo: Es la obtención de una copia de los datos en otro medio magnético, de tal modo que a partir de dicha copia es posible restaurar el sistema o la información.
Seguridad lógica: Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

SENARA: Servicio Nacional de Aguas Subterráneas, Riego y Avenamiento. DRAT: Distrito de Riego Arenal Tempisque

Software: Es un término genérico que designa al conjunto de programas de distinto tipo (sistema operativo y aplicaciones diversas) que hacen posible el funcionamiento y la operación del computador.

TI: Tecnología de Información.

Virus: Es un programa informático que se ejecuta en el ordenador sin previo aviso y que puede corromper el resto de los programas, archivos de datos e incluso el mismo sistema operativo.

UGI: Unidad de Gestión Informática