LINEAMIENTOS SOBRE EL USO Y MANEJO DE LOS BIENES INFORMÁTICOS DE LA UNIVERSIDAD DE SEGURIDAD PUBLICA DEL SURESTE.

EXPOSICIÓN DE MOTIVOS

Con fundamento en los **artículos 70 y 71**, así como demás disposiciones relativas del **Capítulo I**, sobre el uso, administración y mantenimiento de bienes informáticos, estipulados en el Capítulo Sexto, "**De los bienes Informáticos y sistemas de información", de la *Normatividad para la Gestión y Desarrollo de Tecnologías de Información y Telecomunicaciones***, vigente en el Estado de Chiapas; la Universidad de Seguridad Pública del Sureste establece los presentes lineamientos que norman el uso y manejo adecuado de los bienes informáticos asignados a su personal.

Estos lineamientos tienen como **finalidad garantizar la correcta administración, conservación y protección de los recursos informáticos**, asegurando su óptimo funcionamiento para el cumplimiento de las actividades académicas, operativas y administrativas de la institución.

TITULO PRIMERO
DISPOSICIONES GENERALES

CAPITULO ÚNICO

Artículo 1.- Las disposiciones de estos lineamientos son de orden público e interés social y tienen por objeto establecer las bases para la organización, funcionamiento y administración de los órganos administrativos que integran la Universidad de Seguridad Pública del Sureste, así como las relaciones jerárquicas existentes dentro de la dependencia.

Artículo 2.- La Universidad de Seguridad Pública del Sureste **tiene como objetivo fundamental:**

- Coordinar su funcionamiento institucional.
- Planear, organizar, dirigir y aplicar planes y programas de estudio e investigación.
- Preparar e impartir cursos de capacitación, adiestramiento continuo y actualización profesional.

Estas acciones están dirigidas al **personal operativo y de servicios** de:

- La Secretaría de Seguridad del Pueblo,
- La Fiscalía General de Justicia del Estado,
- Los cuerpos de Seguridad Pública municipales,

Artículo 3.- Para efectos del presente ordenamiento, se entenderá por:

- **Universidad:** Universidad de Seguridad Pública del Sureste.
- **Rector General:** El Rector General de la Universidad de Seguridad Pública del Sureste.
- **Órganos Administrativos:** Todas las estructuras que conforman la Universidad, incluyendo, de manera enunciativa mas no limitativa: Direcciones, Unidades, Áreas y Secciones.
- **Usuarios:** El personal administrativo y operativo que labora en la Universidad.
- **Servicio Express:** Atención inmediata al usuario respecto a fallas o problemas con sus bienes informáticos, o asesoría en el manejo de software (paquetería).

Artículo 4.- Los titulares de los órganos administrativos, así como todo el personal de la Universidad, están obligados a cumplir con las órdenes, instrucciones o acuerdos emitidos por el rector en su calidad de titular de la institución.

Este cumplimiento deberá darse **siempre y cuando no contravenga disposiciones legales** vigentes.

TÍTULO II
LINEAMIENTOS DE INFORMÁTICA

CAPÍTULO I
SOBRE USO DE BIENES INFORMÁTICOS

Artículo 5.- Uso institucional y resguardo de bienes informáticos

El uso de los bienes informáticos (hardware, software, aplicaciones, sistemas e información) está restringido exclusivamente a actividades laborales relacionadas con la Universidad de Seguridad Pública del Sureste y el órgano administrativo correspondiente.

- El usuario debe **firmar el resguardo** del equipo asignado.
- Además, está obligado a **proteger y preservar** los bienes bajo su cargo, tomando medidas para evitar riesgos como:
  - Golpes físicos
  - Robo del equipo o de la información
  - Sobrecargas eléctricas
  - Cualquier otro daño prevenible

Artículo 6.- Uso restringido de bienes informáticos asignados

El usuario debe limitarse al uso de los bienes informáticos (hardware y software) que le han sido asignados.

- Queda **estrictamente prohibido** instalar, modificar o eliminar el software originalmente entregado.
- En caso de requerir recursos adicionales, la solicitud deberá hacerse **por escrito** a través del titular del órgano administrativo a la Unidad de Informática.
- Esta unidad realizará un **dictamen técnico** y, si las actividades del usuario lo justifican, podrá autorizar dichos recursos.

Artículo 7.- Uso autorizado de software y licencias

Todo software utilizado por los usuarios debe contar con la debida autorización y la licencia correspondiente.

- Está prohibido que personal no autorizado instale programas sin licencia o utilice software o sistemas sin el permiso correspondiente.

- También se prohíbe estrictamente realizar copias del software proporcionado para fines laborales.
- Solo el personal autorizado de la Unidad de Informática tiene facultad para instalar software en los equipos institucionales.

Artículo 8.- Procedimiento para cambio de equipo de cómputo entre usuarios o áreas

El cambio de equipo de cómputo entre órganos administrativos o usuarios dentro del mismo órgano debe solicitarse por escrito a la Unidad de Informática y contar con su autorización previa.

La solicitud debe incluir:

- Marca, modelo, número de serie y número de inventario del equipo a transferir.
- Nombre completo del usuario que entrega el equipo y su órgano administrativo.
- Nombre completo del usuario que recibirá el equipo y su órgano administrativo.

Una vez autorizado, el área solicitante es responsable de actualizar la información en los anexos de bienes informáticos en el Sistema SERAPE (Sistema de Entrega y Recepción de la Administración Pública del Estado).

Artículo 9.- Análisis previo de dispositivos USB externos

Cualquier dispositivo de almacenamiento magnético USB externo que no pertenezca a la universidad debe ser previamente analizado por el usuario del equipo de cómputo para asegurarse de que esté libre de virus informáticos que puedan comprometer la integridad de los datos almacenados en el equipo.

Artículo 10.- Responsabilidad de los órganos administrativos en el suministro de materiales.

Los órganos administrativos tienen la responsabilidad de asegurar que se disponga de los materiales necesarios para el correcto funcionamiento de los equipos de cómputo.

Esto incluye requisitar consumibles esenciales como dispositivos de almacenamiento externo, papel, tinta, tóner y otros insumos indispensables para mantener la operatividad.

Artículo 11.- Prohibición de intercambio de componentes y periféricos

Está estrictamente prohibido que los usuarios intercambien componentes o periféricos entre equipos de cómputo. Cada equipo debe mantenerse conforme al listado registrado en el resguardo vigente asignado a cada usuario. **Artículo 12.- Prohibición del movimiento no autorizado de equipos de cómputo**

Queda prohibido que personal no autorizado realice el traslado de equipos de cómputo, tales como computadoras, servidores u otros dispositivos relacionados.

Solo la unidad de informática tiene la autoridad y el conocimiento para llevar a cabo estos movimientos de manera segura, garantizando que los equipos y sus datos no sufran daño durante el traslado.

Artículo 13.- Control y mantenimiento de equipos de cómputo

Solo el personal autorizado de la unidad de informática puede realizar intervenciones técnicas en los equipos de cómputo, tales como abrirlos o extraer componentes periféricos (discos duros, tarjetas de expansión, memorias RAM, etc.).

Objetivos de esta normativa:

1. **Prevención de daños:** Evitar daños físicos o a los datos por manipulación incorrecta de los equipos.
2. **Protección de la información:** Evitar riesgos a la seguridad y confidencialidad de la información almacenada o transmitida.
3. **Cumplimiento de garantías:** Evitar la anulación de garantías o contratos de soporte técnico por intervenciones no autorizadas.
4. **Responsabilidad técnica:** Garantizar que las intervenciones sean realizadas por personal capacitado, asegurando diagnósticos y reparaciones correctas y seguras.

Artículo 14.- Se prohíbe el uso de dispositivos y la instalación de software que no sean propiedad de la Universidad de Seguridad Pública del Sureste. Esto incluye juegos, programas, antivirus, películas, entre otros.

Excepción: **Solo se permitirá en casos emergentes que el rector o el titular del órgano administrativo lo autorice.**

Artículo 15: Procedimiento para el préstamo de equipos informáticos y de comunicaciones.

1. **Propósito del préstamo:**
   El equipo se presta para apoyar actividades académicas o institucionales, como presentaciones, cursos, talleres, tanto dentro como fuera de la universidad.
2. **Requisitos del documento de préstamo:**
   El préstamo debe registrarse formalmente y contener:
   - Descripción del equipo (tipo, por ejemplo, laptop o proyector).
   - Marca, modelo y número de serie para identificación única.
   - Número de inventario para control y rastreo.
   - Observaciones (estado del equipo, accesorios, etc.).
   - Nombre del solicitante, quien será responsable del equipo. El documento debe firmarse por el solicitante y el personal encargado, asegurando el acuerdo mutuo.
3. **Cancelación del préstamo:**
   - El préstamo se cancela al devolver el equipo, tras una revisión para verificar su estado.
   - En caso de daño o pérdida, se aplican procedimientos para responsabilizar al usuario.
4. **Plazos del préstamo:**
   - **Personal comisionado:** El préstamo dura lo que establezca el oficio de comisión (tiempo que dure la comisión).
   - **Otros usuarios:** El préstamo es por un máximo de 5 días.

Artículo 16.- Durante una inspección o verificación física no se encuentre un bien informático, los servidores públicos que tengan ese bien a su cargo deberán**:**

- Presentar el bien en un plazo máximo de 10 días naturales.

Esto se hace conforme a la Ley del Patrimonio del Estado de Chiapas (Título Sexto, Capítulo I, Artículo 60, Fracción XI).

Además, si se determina que el bien ya no es necesario para el servicio al que estaba destinado o que es inconveniente seguir usándolo, la unidad de informática:

- Concentrará el bien,
- Actualizará el resguardo correspondiente.

Artículo 17.- En el caso de robo de bienes informáticos, el resguardante afectado deberá:

- Presentar una denuncia ante la autoridad correspondiente,
- Dar seguimiento hasta que se concluya el proceso judicial.

Esto debe hacerse conforme a lo que establece la **Ley del Patrimonio del Estado de Chiapas (Título Sexto, Capítulo I, Artículo 60, Fracción X).**

Artículo 18.- Cuando un servidor público dañe o pierda un bien público, no siempre es necesario presentar una denuncia para fincar responsabilidades. En lugar de eso, el servidor público puede firmar un convenio con la dependencia responsable comprometiéndose a:

- Reparar el daño en un plazo máximo de 30 días hábiles,
- O reponer el bien dañado o extraviado por uno igual o con características similares,
- O, si no es posible, pagar el valor económico del bien según el precio de mercado vigente.

Este procedimiento se basa en las obligaciones establecidas en el Reglamento de la Ley Patrimonial de la Administración Pública del Estado de Chiapas (Título Primero, Capítulo Único, Artículo 6).

Artículo 19.- Procedimiento en Caso de Baja Laboral del Usuario

Regula las responsabilidades del usuario (servidor público o empleado) al momento de causar baja laboral, estableciendo las obligaciones relacionadas con la entrega y manejo de los bienes informáticos asignados:

1. Entrega física de los bienes informáticos

- Al causar baja laboral, el usuario está obligado a entregar **físicamente** todos los bienes informáticos que le fueron asignados.
- Los bienes deben devolverse en condiciones iguales a las de su entrega inicial, considerando únicamente el desgaste normal por uso adecuado y previsto.

2. Cancelación de la hoja de resguardo

- El usuario deberá solicitar **por escrito** la cancelación de la hoja de resguardo correspondiente, documento que acredita la asignación de los bienes informáticos.
- La cancelación es necesaria para dejar constancia de que el equipo ha sido devuelto y que el usuario queda liberado de responsabilidad sobre dichos bienes.

3. Entrega de la información contenida en el equipo

- Además de la devolución física, el usuario deberá entregar toda la información almacenada en el equipo a la persona sucesora en el cargo o a quien la autoridad designe.
- La información incluye archivos, documentos, bases de datos, configuraciones y cualquier otro dato generado o almacenado durante el uso del equipo.

4. Responsabilidad sobre la información

- La correcta transferencia de la información garantiza la continuidad administrativa y evita la pérdida de datos relevantes para la institución.
- El usuario es responsable de que dicha información sea entregada íntegra y accesible al próximo responsable del equipo.

CAPÍTULO II
SOBRE EL FUNCIONAMIENTO

Artículo 20.- Uso Adecuado de la Energía Eléctrica para Bienes Informáticos

Regula el uso correcto de la energía eléctrica para los bienes informáticos, con el fin de **evitar daños a los equipos** y garantizar su **funcionamiento óptimo**.

1. Corriente eléctrica independiente

- Los bienes informáticos deberán conectarse a un **circuito eléctrico independiente**, separado de aquellos utilizados para otros equipos o dispositivos eléctricos no relacionados.
- Queda prohibido conectar los equipos informáticos a circuitos que compartan corriente con **contactos eléctricos, apagadores, o interruptores de aire acondicionado**.

- Esta medida busca prevenir interferencias eléctricas y sobrecargas que puedan afectar la estabilidad y funcionamiento de los bienes informáticos.

2. Prohibición de compartir contacto con aparatos de alto consumo

- No se permite que los bienes informáticos compartan la misma toma de corriente con **aparatos eléctricos de alto consumo energético**, tales como:
  - Aires acondicionados
  - Calefactores
  - Microondas
  - Otros dispositivos que puedan generar picos de voltaje o fluctuaciones eléctricas.
- El uso compartido con estos equipos puede ocasionar **daños eléctricos, fallas en el rendimiento** o pérdida de datos en los equipos informáticos.

Artículo 21.- Conexión y Encendido/Apagado de Equipos Informáticos

Establece las normas para la correcta conexión, encendido y apagado de los equipos informáticos con el objetivo de protegerlos contra daños eléctricos y asegurar su funcionamiento adecuado.

1. Conexión a regulador de voltaje o sistema de energía interrumpible (UPS)

- Los equipos de cómputo, incluyendo computadoras y monitores, deberán estar conectados preferentemente a un **regulador de voltaje** o a un **Sistema de Energía Interrumpible (UPS)**.
- **Regulador de voltaje**: Su función es mantener una corriente estable y proteger los equipos contra fluctuaciones, picos o caídas de voltaje que pueden dañarlos.
- **UPS**: Proporciona energía temporal durante cortes eléctricos, permitiendo el apagado seguro del equipo, y además ofrece protección contra picos y sobrecargas eléctricas.

2. Conexión directa de impresoras láser

- Las impresoras láser deben conectarse **directamente a una toma de corriente**, sin pasar por reguladores de voltaje ni UPS.

- Esto se debe a que las impresoras láser tienen un **alto consumo energético** y la conexión a dispositivos de protección diseñados para cargas menores podría afectar su funcionamiento.

3. Orden para encender y apagar los equipos

Para evitar daños electrónicos y prevenir pérdida de datos, se deberá respetar el siguiente orden:

- **Encendido:**
  1. Encender el **regulador de voltaje** o UPS (si se utiliza).
  2. Encender el **monitor**.
  3. Encender la **CPU**.
  4. Encender los **equipos periféricos** (impresoras, escáneres, etc.).
- **Apagado:**
  1. Apagar los **equipos periféricos**.
  2. Apagar la **CPU**.
  3. Apagar el **monitor**.
  4. Apagar el **regulador de voltaje** o UPS (si se utiliza).

Artículo 22.- Uso Responsable de Equipos de Cómputo

Establece las **normas de uso responsable** de los equipos de cómputo asignados a los usuarios de la **Universidad de Seguridad Pública del Sureste**, con el fin de **preservar su funcionalidad** y **proteger la integridad de la información** almacenada.

1. Prohibición del consumo de alimentos cerca de los equipos

- **Queda estrictamente prohibido consumir alimentos** en las inmediaciones de equipos de cómputo institucionales.
- Esta medida busca evitar:
  - **Riesgo de derrames**: Los alimentos y sus residuos (sólidos o líquidos) pueden afectar teclados, pantallas, ventiladores u otros componentes sensibles, comprometiendo el funcionamiento del equipo.
  - **Problemas de higiene y mantenimiento**: Los restos de comida pueden generar acumulación de suciedad o atraer plagas, lo
  - cual deteriora progresivamente los dispositivos.

2. Evitar la presencia de líquidos cerca del equipo

- **Se prohíbe colocar recipientes con líquidos** (vasos, termos, botellas, tazas, etc.) cerca de los equipos informáticos.
- Justificación:
  - **Peligro inmediato de daño**: Cualquier derrame accidental de líquido puede generar cortocircuitos que afecten permanentemente el hardware y ocasionen pérdida de datos.
  - El contacto con líquidos es una de las principales causas de **fallas irreversibles en dispositivos electrónicos**.

Artículo 23.- Responsabilidades de la Unidad de Informática en el Mantenimiento de Bienes Informáticos Fuera de Garantía

Son las obligaciones de la **Unidad de Informática** respecto al **mantenimiento de los bienes informáticos** cuyo **periodo de garantía con el proveedor ha expirado**. Su objetivo es garantizar la continuidad operativa de los equipos tecnológicos institucionales, siempre que estos no sean considerados obsoletos.

Responsabilidad posterior a la garantía

- Una vez vencida la garantía otorgada por el proveedor, la **Unidad de Informática** asumirá la responsabilidad de brindar **servicio de mantenimiento preventivo y correctivo** a los equipos informáticos que continúen en uso.
- Este mantenimiento se otorgará siempre que el equipo **no haya sido clasificado como obsoleto**, conforme a los criterios establecidos en el **Artículo 26** del presente lineamiento.

Tipo de servicios que debe garantizar la Unidad de Informática:

- **Mantenimiento preventivo**: Incluye acciones de revisión, limpieza, actualización y ajustes periódicos destinados a evitar fallas y prolongar la vida útil del equipo.
- **Mantenimiento correctivo**: Consiste en la atención y reparación de fallas que afecten el funcionamiento del equipo, incluyendo diagnóstico, reemplazo de componentes (cuando aplique) y pruebas de funcionamiento.

Artículo 24.- Procedimiento para la Solicitud de Mantenimiento Preventivo o Correctivo de Equipos Informáticos

Es el procedimiento formal para solicitar el **mantenimiento preventivo** o **correctivo** de los equipos informáticos dentro de la organización. El objetivo es asegurar que estos servicios sean debidamente **solicitados, documentados y gestionados** por la **Unidad de Informática**, garantizando eficiencia, y control institucional.

1. Solicitud por escrito del Titular del órgano administrativo

- El **Titular del órgano administrativo** será responsable de solicitar, mediante **formato oficial por escrito**, el mantenimiento que requiera el equipo.
- La solicitud puede ser para:
  - **Mantenimiento preventivo**: Con el fin de evitar fallas futuras.
  - **Mantenimiento correctivo**: Para solucionar una falla existente.

Esta documentación garantiza la existencia de un **registro formal** que respalde la intervención técnica.

2. Información obligatoria en la solicitud

Para que la Unidad de Informática pueda atender eficazmente la solicitud, esta deberá incluir los siguientes datos del equipo:

- **Marca y Modelo**: Para identificar el equipo y sus características técnicas.
- **Número de Serie**: Clave única que permite rastrear el historial del equipo.
- **Número de Inventario**: Para comprobar el registro oficial del bien dentro del sistema institucional.

3. Identificación del personal asignado al equipo

- Se debe incluir el **nombre del usuario responsable o asignado** al equipo.
- Esta información facilita:
  - La verificación del uso del equipo.
  - La investigación de causas relacionadas con el daño.
  - La posible asignación de responsabilidades si se detecta un uso inadecuado.

4. Descripción detallada de la falla

- La solicitud debe incluir una **descripción clara y específica del problema** que presenta el equipo.
- Se recomienda incluir:
  - **Síntomas detectados** (ej. "el equipo no enciende", "pantalla congelada", "no reconoce el disco duro").
  - **Condiciones en que ocurrió la falla** (ej. "tras un apagón", "después de instalar un programa"). Cuanta más información se proporcione, **más rápido y preciso será el diagnóstico y la reparación** por parte del personal técnico.

Artículo 25.- Procedimiento para Reposición de Componentes o Reemplazo de Equipos de Cómputo

Es el procedimiento formal que debe seguirse cuando un **equipo de cómputo** requiere la **reposición de un componente dañado** o el **reemplazo completo** del equipo. El proceso está diseñado para ser transparente, documentado y útil para la toma de decisiones administrativas.

1. Notificación por escrito de la Unidad de Informática

- Cuando un equipo presenta **fallas graves** que ameriten el reemplazo de algún componente o del equipo completo, la **Unidad de Informática** debe emitir una **notificación oficial por escrito** al **Titular del órgano administrativo correspondiente**.
- Esta notificación sirve como respaldo documental para justificar la intervención, reposición o sustitución del bien en el inventario institucional.

2. Contenido obligatorio de la notificación

La notificación deberá contener los siguientes elementos mínimos:

- **Marca y Modelo del equipo**: Para identificar de forma precisa el dispositivo.
- **Número de Serie y Número de Inventario**: Para asociar la intervención con el equipo registrado oficialmente.
- **Dictamen de la falla**:
  Debe especificarse con claridad:
  - El diagnóstico técnico.
  - El componente dañado o la causa del problema.

- **Características técnicas de los componentes a reemplazar**: Si el daño no amerita el reemplazo completo, se deben incluir las especificaciones técnicas del componente necesario (ej. tipo y velocidad de memoria RAM, capacidad del disco duro, tipo de fuente de poder, etc.) a fin de asegurar su **compatibilidad** con el equipo existente.

Artículo 26.- Criterios y Procedimiento para la Baja de Equipos Obsoletos

Define los **criterios técnicos y administrativos** para determinar cuándo un equipo informático debe considerarse **obsoleto**, así como el procedimiento a seguir para su baja institucional.

1. Criterios para considerar un equipo como obsoleto

Un equipo será considerado obsoleto si cumple con uno o más de los siguientes criterios:

- **Fallas en el rendimiento**:
  El equipo presenta fallas frecuentes o bajo desempeño debido al desgaste por el tiempo de uso, impidiendo una operación eficiente.
- **Inadecuación tecnológica**:
  El equipo ya no es compatible con aplicaciones actuales o no cumple con los requerimientos tecnológicos vigentes (hardware y/o software).
- **Costo de reparación elevado**:
  Cuando el costo de reparación resulta excesivo o desproporcionado en relación con el valor del equipo, lo que hace inviable su mantenimiento.

2. Procedimiento para solicitar la baja de un equipo obsoleto

- El usuario debe presentar una **solicitud por escrito** dirigida a la **Unidad de Informática**, justificando la necesidad de dar de baja el equipo.
- En la solicitud debe **explicarse la necesidad de actualizar el sistema**, es decir, se debe fundamentar por qué el equipo debe ser retirado del servicio y sustituido por uno que cumpla con los estándares actuales.

Artículo 27.- Criterios para Considerar Funcional un Bien Informático Después de una Falla

Establece los criterios técnicos y operativos para determinar si un bien informático puede seguir siendo considerado **funcional** luego de haber presentado una falla y haber recibido mantenimiento correctivo.

1. Aplicación de mantenimiento correctivo

- El equipo se considera funcional si, tras presentar una falla, se le ha realizado un **mantenimiento correctivo adecuado**, es decir:
  - Las reparaciones necesarias se llevaron a cabo correctamente.
  - El equipo vuelve a operar con normalidad tras la intervención técnica.

2. Ausencia de nuevas fallas

- Para que el equipo se valide como funcional, debe demostrar que:
  - No presenta **nuevas fallas** luego del mantenimiento.
  - Su **rendimiento es estable**, recuperando la operatividad esperada.

3. Compatibilidad con aplicaciones actuales

- Además de su funcionamiento técnico, el equipo debe:
  - Ser **capaz de ejecutar las aplicaciones modernas** necesarias para el trabajo institucional.
  - Contar con los **recursos mínimos requeridos** en términos de hardware y software para cumplir con las demandas tecnológicas actuales.

Artículo 28.- Manejo de Bienes Informáticos Dañados por Uso Indebido

Las acciones a seguir cuando un bien informático presenta fallas **a causa de un mal uso o negligencia** por parte del personal responsable de su resguardo.

1. Causas del daño

Se considera daño por uso indebido cuando el equipo presenta fallas a causa de:

- Exposición a líquidos (mojar el equipo).
- Golpes o caídas.
- Manipulación inapropiada u otro tipo de acción que afecte su integridad física o funcional.

2. Responsabilidad del resguardante

- El **resguardante del bien** (persona a quien está asignado) será responsable de los daños ocasionados.
- Deberá **firmar un convenio con la unidad de informática**, en el que se comprometa formalmente a reparar el daño causado.

3. Plazo para la reparación

- El responsable cuenta con **30 días hábiles** a partir de la firma del convenio para cumplir con la reparación del daño.

4. Opciones para resarcir el daño

El resguardante puede elegir entre dos formas de reparación:

- **Reposición del bien**: Entregar un equipo igual o con características técnicas similares al dañado.
- **Pago del valor del bien**: Cubrir el costo equivalente al valor de mercado del equipo dañado o de uno con especificaciones similares.

Artículo 29.- Procedimiento para el Servicio Exprés de Soporte Técnico

Define el proceso obligatorio que deben seguir los usuarios para recibir atención técnica de forma exprés:

1. Requisito para solicitar el servicio

- El usuario debe **llenar correctamente el formato de solicitud de servicio técnico**.
- Este formulario debe ser **entregado de manera personal** en la **unidad de informática**, específicamente en el área de **soporte técnico**.

2. Disponibilidad del formato de solicitud

- El formulario ha sido previamente **distribuido en formato digital e impreso** a todos los órganos administrativos.

- Los responsables de cada área **ya cuentan con este documento**, por lo que no hay justificación para omitirlo al solicitar el servicio.

3. Condición obligatoria para ser atendido

- Si el usuario:
  - No **llena correctamente la solicitud**, o
  - **No sigue el proceso** establecido, entonces **no se le brindará atención técnica**.

Artículo 30.- Procedimiento para la baja de bienes informáticos no útiles

Los pasos a seguir cuando los **bienes informáticos** dejan de ser funcionales o útiles para los fines originalmente asignados. El proceso comprende tres acciones principales:

1. Solicitud de baja de bienes informáticos

- El responsable del resguardo del bien deberá presentar una **solicitud escrita** para darlo de baja.
- Esta solicitud implica la eliminación formal del bien del inventario institucional.

2. Actualización del resguardo

- De manera simultánea a la solicitud de baja, se debe proceder a la **actualización del documento de resguardo**.
- Esto garantiza que el registro institucional refleje con precisión los bienes aún bajo custodia.

3. Cumplimiento normativo

- Tanto la baja como la actualización deben realizarse conforme a lo establecido en el:
  - **Reglamento de la Ley Patrimonial de la Administración Pública del Estado de Chiapas**
  - **Título Primero, Capítulo Único, Artículo 2, Fracción X**
- Esta fracción regula las disposiciones sobre administración y disposición de los bienes propiedad del estado

CAPÍTULO III

SOBRE EL USO DEL SERVICIO DE RED, CORREO ELECTRÓNICO E INTERNET.

Artículo 31.- Creación y Asignación de Correos Electrónicos Institucionales

Con el fin de fortalecer los canales de comunicación oficial de la Universidad de Seguridad Pública del Sureste, se establece el siguiente procedimiento y marco de responsabilidades respecto a la creación y asignación de correos electrónicos institucionales:

1. Responsabilidad de la Unidad de Informática:

La **Unidad de Informática** será la **única instancia facultada** para la **creación, configuración y administración** de las cuentas de correo electrónico institucional, así como para su correcta asignación y seguimiento.

2. Destinatarios específicos:

Las cuentas de correo electrónico institucional serán asignadas exclusivamente a las siguientes figuras administrativas:

- **Directores**
- **Jefes de unidad**
- **Jefes de área**

Estas cuentas son de uso obligatorio para toda comunicación oficial y deben utilizarse conforme a los lineamientos establecidos por la universidad.

1. **Procedimiento de entrega:**

Una vez creada la cuenta institucional, el procedimiento de entrega será el siguiente:

- Se emitirá una **tarjeta informativa** dirigida al titular del órgano correspondiente, como constancia de la asignación.
- Se entregará un **sobre cerrado** que contendrá:
    - La **dirección de correo electrónico institucional** asignada.
    - Una **contraseña temporal** para el primer acceso a la cuenta.

El usuario deberá **cambiar la contraseña de inmediato** tras el primer inicio de sesión, conforme a los requisitos de seguridad establecidos en los artículos correspondientes del presente lineamiento.

Artículo 32.- Confirmación de Recepción de Información por Correo Institucional

Con el propósito de **garantizar la correcta recepción de mensajes oficiales**, así como establecer un **registro confiable de la correspondencia institucional**, se dispone lo siguiente:

1. Obligación del receptor:

Toda persona que reciba un mensaje o información a través del **correo electrónico institucional** deberá **enviar un acuse de recibo al remitente**, como confirmación de que la comunicación fue recibida de manera correcta y oportuna.

2. Contenido obligatorio del acuse de recibo:

El acuse de recibo deberá incluir, al menos, los siguientes datos:

- **Nombre del remitente**: Para identificar de forma clara quién envió la información.
- **Fecha de recepción**: Para dejar constancia del día en que fue recibido el mensaje.
- **Hora de recepción**: Para especificar la hora exacta en que fue recibida la comunicación.

Este procedimiento es de cumplimiento obligatorio y será considerado como parte del **control interno de correspondencia digital** de la Universidad de Seguridad Pública del Sureste.

Artículo 33.- Identificación Obligatoria en Envío de Información por Medios Electrónicos.

Con el fin de garantizar la transparencia y responsabilidad **en el manejo de la información institucional enviada por medios electrónicos, se establece que todo envío de información realizado a través de medios electrónicos, deberá** incluirse de forma precisa y *obligatoria la siguiente información:*

1. **Nombre del Órgano Administrativo** de adscripción del remitente.

2. **Nombre completo del usuario** que realiza el envío.
3. **Fecha y hora** exactas del envío del mensaje o documento.

Esta disposición permite identificar de manera clara al responsable del contenido remitido, fortaleciendo el control institucional sobre la comunicación oficial y reduciendo riesgos de ambigüedad, pérdida de información o suplantación de identidad.

Artículo 34.- Responsabilidad en el Uso y Actualización de Claves de Acceso

Los usuarios serán responsables del **uso adecuado, confidencial y seguro** de su **clave de acceso y contraseña** a los sistemas institucionales, especialmente al **correo electrónico institucional**, considerando las siguientes disposiciones:

1. **Responsabilidad individual:** Cada usuario deberá **mantener en secreto su contraseña** y evitar compartirla con terceros, bajo ninguna circunstancia. El mal uso o divulgación de esta información será considerado una falta a las normas de seguridad institucional.
2. **Actualización periódica:** Las contraseñas deberán ser **cambiadas cada tres (3) meses** como medida preventiva para:
    - Reducir el riesgo de **robo de información**.
    - Prevenir **accesos no autorizados** a cuentas institucionales.
    - Evitar **vulnerabilidades** que puedan comprometer datos sensibles o confidenciales.
3. **Seguridad de la cuenta:** El incumplimiento de esta disposición podría derivar en la **suspensión temporal del acceso** y en la aplicación de medidas correctivas o disciplinarias, conforme a la normatividad vigente.

Artículo 35.- Depuración Periódica del Correo Electrónico Institucional

Con el objetivo de **mantener la eficiencia operativa** y evitar la saturación de los buzones institucionales, se establece que los usuarios deberán realizar de forma **periódica la depuración de los correos electrónicos recibidos**, eliminando aquellos mensajes que ya no sean necesarios para sus funciones laborales o administrativas. Esta práctica busca:

- Optimizar el uso del **espacio de almacenamiento** en los servidores de correo institucional.

- Prevenir **problemas de entrega** de nuevos mensajes por buzones saturados.
- Facilitar el **acceso ágil a la información** relevante y actual.

Artículo 36.- Uso Responsable del Servicio de Internet y Correo Electrónico Institucional

Con el fin de asegurar el uso correcto, eficiente y seguro de los servicios de **Internet** y **correo electrónico institucional** en la Universidad de Seguridad Pública del Sureste, se establecen los siguientes lineamientos de cumplimiento obligatorio:

1. Uso exclusivo para fines institucionales:

Los recursos de Internet y del correo electrónico institucional deberán ser utilizados **únicamente para actividades relacionadas con las funciones académicas, administrativas o de gestión institucional.** Está estrictamente prohibido su uso con fines personales, comerciales, recreativos o ajenos a los intereses de la universidad.

2. Prohibición de inscripción a listas de correos:

No se permite utilizar la cuenta de correo institucional para **suscribirse a listas de distribución, boletines o plataformas** que no estén directamente relacionadas con las responsabilidades laborales del usuario dentro de la universidad.

3. Prohibición de compras personales:

Los usuarios **no deben realizar compras personales** o contratar servicios a título individual a través del correo electrónico o utilizando la red institucional. Este recurso está destinado exclusivamente para fines académicos y administrativos autorizados.

4. Prohibición de envío de SPAM y cadenas de correos:

Queda estrictamente prohibido:

- **Enviar correos masivos no solicitados (SPAM)**, independientemente de su contenido.
- Participar en **cadenas de correos electrónicos**, incluyendo mensajes que incentiven su reenvío, por muy inofensivos que parezcan.

Estas prácticas generan tráfico innecesario en la red y pueden vulnerar la seguridad institucional.

5. Seguridad en la navegación y descarga de archivos:

Los usuarios deberán:

- **Verificar que cualquier archivo descargado** desde Internet esté libre de virus o software malicioso.
- **Utilizar herramientas de protección** (antivirus actualizado y navegación segura) y actuar con precaución al abrir enlaces o archivos adjuntos.
- **Evitar descargar software o contenido de sitios no confiables** que pueda poner en riesgo los sistemas informáticos de la institución.

Artículo 37.- Procedimiento para la Creación de Cuentas de Usuario con Acceso a la Red Institucional.

Con el objetivo de **garantizar el uso adecuado y seguro de los servicios de red** de la Universidad de Seguridad Pública del Sureste, se establece el siguiente procedimiento para la **creación de cuentas de usuario**:

1. Responsabilidad del titular del Órgano Administrativo:

La **solicitud de creación de cuentas de usuario** deberá ser gestionada **exclusivamente por el titular del Órgano Administrativo, jefe de unidad o jefe de área correspondiente**.
El personal operativo **no podrá realizar solicitudes directas**. Esta medida asegura un control jerárquico y responsable sobre el acceso a los recursos institucionales.

2. Solicitud formal por escrito:

Toda solicitud deberá realizarse de **manera formal y por escrito** a la **Unidad de Informática**, permitiendo llevar un **registro documentado** de las cuentas solicitadas, su propósito y la persona responsable de la gestión.

3. Acceso a los servicios de red:

La cuenta de usuario será creada **únicamente cuando el personal necesite acceder** a los servicios digitales proporcionados por la red institucional, como:

- Plataformas académicas
- Sistemas administrativos
- Herramientas de comunicación institucional
- Bases de datos
- Otras aplicaciones relacionadas con sus funciones laborales

4. Justificación de la necesidad:

El titular del Órgano Administrativo deberá **incluir una justificación clara y específica** que respalde la necesidad del acceso a los servicios de red por parte del personal.
Esto garantiza que las cuentas sean otorgadas solo a **usuarios cuyas responsabilidades** lo requieran, fortaleciendo así la seguridad y el uso racional de los recursos tecnológicos.

Artículo 38.- Control de Acceso mediante Cuentas de Usuario con Privilegios Definidos

Con el propósito de **garantizar la seguridad de los sistemas institucionales** y proteger la integridad de los datos y recursos tecnológicos de la Universidad de Seguridad Pública del Sureste, se establece lo siguiente:

La creación y asignación de cuentas de usuario deberá realizarse bajo criterios de **privilegios definidos**, asegurando que cada usuario tenga acceso únicamente a los módulos, sistemas o información que le correspondan según sus funciones.

Objetivos específicos:

- **Restringir el acceso** a información sensible o crítica únicamente a usuarios debidamente autorizados.
- **Prevenir el uso indebido** de los sistemas mediante el establecimiento de niveles de acceso diferenciados.
- **Fortalecer la trazabilidad** de las acciones realizadas en los sistemas, vinculándolas directamente con los usuarios responsables.
- **Evitar brechas de seguridad** provocadas por accesos no controlados o cuentas genéricas.

La **Unidad de Informática** será responsable de la **creación, modificación y cancelación** de cuentas, en coordinación con los titulares de los Órganos Administrativos, según los requerimientos operativos.

Artículo 39.- Control de las Configuraciones de Red

Con el objetivo de garantizar la **correcta administración de los recursos tecnológicos** y minimizar los riesgos de fallos operativos o vulnerabilidades de seguridad, se establece que:

La responsabilidad exclusiva de realizar configuraciones de red **recae en la Unidad de Informática.**

Esta medida tiene como finalidad:

- **Centralizar y controlar** las tareas técnicas relacionadas con la conectividad, estructura de red y sus componentes.
- **Prevenir interrupciones** en el servicio ocasionadas por intervenciones no autorizadas.
- **Evitar riesgos de seguridad** derivados de configuraciones inapropiadas realizadas por personal no capacitado o no autorizado.

Cualquier modificación, ajuste o intervención en la configuración de red deberá ser solicitada formalmente y ejecutada únicamente por el personal autorizado de la **Unidad de Informática**.

Artículo 40.- Complejidad para Contraseñas de Cuentas Institucionales

Con el propósito de **fortalecer la seguridad de las cuentas de usuario** y prevenir accesos no autorizados a los sistemas informáticos de la Universidad de Seguridad Pública del Sureste, se establecen los siguientes **requisitos obligatorios de complejidad para la creación de contraseñas**:

1. Restricción relacionada con el nombre de usuario:

La contraseña **no debe contener el nombre de usuario**, ni fragmentos del nombre completo que incluyan **más de dos caracteres consecutivos**. Esta medida busca evitar el uso de contraseñas predecibles basadas en datos personales fácilmente vinculables al titular de la cuenta.

2. Longitud mínima:

Toda contraseña deberá contar con una **longitud mínima de seis (6) caracteres**, con el fin de asegurar un nivel básico de complejidad y dificultar su vulneración mediante ataques de fuerza bruta o técnicas automatizadas de descifrado.

3. Diversidad de caracteres:

La contraseña deberá incluir, al menos, **tres de las siguientes cuatro categorías** de caracteres:

- Letras **mayúsculas** (A–Z)
- Letras **minúsculas** (a–z)
- **Dígitos numéricos** (0–9)
- **Caracteres no alfanuméricos** (por ejemplo: !, $, #, %)

Artículo 41.- Caducidad y Actualización de Contraseñas de Cuentas de Dominio

Con el objetivo de mantener un **alto nivel de seguridad** en el acceso a los sistemas informáticos de la Universidad de Seguridad Pública del Sureste, se establece la **caducidad obligatoria** de las contraseñas asignadas a las cuentas de dominio. Para ello, se definen los siguientes lineamientos:

1. Vigencia de 90 días:

Cada contraseña tendrá una **vigencia máxima de 90 días**, lo que implica que el usuario deberá **realizar el cambio correspondiente al menos una vez cada tres meses**. Esta medida busca minimizar el riesgo de accesos no autorizados en caso de que las credenciales hayan sido comprometidas.

2. Solicitud automática de cambio:

Una vez transcurrido el periodo de vigencia, el sistema generará de forma automática una **solicitud de cambio de contraseña**, obligando al usuario a actualizar sus contraseñas antes de continuar con el uso de los servicios institucionales. Este mecanismo asegura un control regular y sistemático del acceso.

3. Asistencia técnica:

En caso de que el usuario tenga **dificultades técnicas** para realizar el cambio de contraseña, podrá solicitar el **apoyo de la Unidad de Informática**, la cual brindará la asistencia necesaria para asegurar el cumplimiento de esta política de seguridad sin comprometer el acceso legítimo a los recursos institucionales.

Artículo 42.- Solicitud anticipada de cambio de contraseña

Si un usuario requiere cambiar su contraseña antes de cumplirse el plazo establecido de 90 días, deberá presentar una solicitud por escrito ante la Unidad de Informática.

Dicha solicitud debe estar firmada por el titular de la cuenta o, en su caso, por el titular del órgano administrativo al que pertenece el usuario.

Artículo 43.- Uso y Responsabilidad de las Cuentas de Red

Se establece que toda **cuenta de red asignada a los usuarios de la Universidad de Seguridad Pública del Sureste** será de uso exclusivo e intransferible. El titular de la cuenta será plenamente responsable por cualquier actividad realizada a través de la misma. Para tal efecto, se determinan las siguientes disposiciones:

1. Uso exclusivo de la cuenta:

- **Cuenta personal e intransferible:** La cuenta de red es de **uso individual y exclusivo** del usuario al que le fue asignada. Está prohibido permitir que terceras personas la utilicen, así como **compartir el nombre de usuario o contraseña** bajo cualquier circunstancia.
- **Implicaciones del uso compartido:** En caso de que el usuario comparta su cuenta, será **responsable por cualquier acción realizada**, aun cuando no haya sido ejecutada directamente por él. La simple cesión de acceso constituye una violación a esta política.

2. Responsabilidad por el uso de la cuenta:

- **Responsabilidad total:** El titular de la cuenta será considerado **plenamente responsable** por el uso, mal uso o abuso que se realice desde su acceso. Esto incluye actividades no autorizadas, accesos indebidos a sistemas institucionales, o daños provocados por el uso malintencionado de la cuenta.
- **Consecuencias legales y de seguridad:** Cualquier uso indebido que derive en daños a la **infraestructura tecnológica**, violaciones de seguridad o acceso no autorizado a información confidencial podrá derivar en la **aplicación de sanciones disciplinarias** e incluso **acciones**

legales, de conformidad con la normativa institucional y la legislación vigente.

Artículo 44.- Cancelación de Accesos por Baja Laboral

Cuando un usuario cause **baja laboral** en la Universidad de Seguridad Pública del Sureste, será su **responsabilidad** solicitar de manera **formal y por escrito** a la **Unidad de Informática** la **cancelación de todos los accesos** a sistemas informáticos, plataformas digitales, servicios en red y cualquier otro recurso tecnológico que le haya sido asignado durante el desempeño de sus funciones.

Esta acción tiene como finalidad **proteger la seguridad y confidencialidad de la información institucional**, así como garantizar el cierre ordenado de sus responsabilidades tecnológicas.

Artículo 45.- Gestión del Acceso a Internet en el Entorno Laboral

Con el fin de garantizar un uso adecuado, seguro y eficiente del acceso a Internet dentro de las instalaciones de la Universidad de Seguridad Pública del Sureste, se establece el siguiente procedimiento para su gestión:

1. Asignación de privilegios:

La **Unidad de Informática** será la instancia responsable de **otorgar los privilegios de acceso a Internet** a los usuarios, en función de las necesidades operativas de cada área.

2. Modificación de privilegios:

Si un usuario requiere **modificar sus privilegios de acceso** (por ejemplo, ampliar o restringir el acceso a determinados sitios o servicios), deberá **presentar una solicitud por escrito**, la cual deberá ser **autorizada por el titular del Órgano Administrativo** al que pertenece.

3. Responsabilidad compartida:

El **uso adecuado de Internet es responsabilidad conjunta** del usuario y del titular del Órgano Administrativo.
Ambos deberán asegurarse de que el acceso se utilice exclusivamente para fines institucionales y en apego a las políticas, lineamientos y normatividad

vigente. El **mal uso** de este recurso podrá dar lugar a sanciones conforme a lo establecido en este lineamiento.

Artículo 46.- Uso Indebido de Internet

Se considerará **uso indebido del servicio de Internet** por parte del usuario cualquier acción que contravenga las políticas de uso aceptable establecidas por la Universidad de Seguridad Pública del Sureste. Particularmente, se incluyen, pero no se limitan a las siguientes conductas:

- Enviar o publicar, a través de Internet o del correo institucional, **mensajes o imágenes discriminatorias, abusivas, ofensivas o amenazantes**.
- Utilizar los equipos de cómputo institucionales para **cometer fraudes** o realizar **actividades de pirateo** de software, películas, música u otros contenidos protegidos por derechos de autor.
- **Robar, utilizar o descubrir contraseñas de terceros** sin autorización expresa.
- Descargar, copiar, distribuir o instalar software o archivos electrónicos **sin la debida licencia o autorización legal**.
- Compartir o divulgar **material o información confidencial** de la universidad sin el consentimiento correspondiente.
- Acceder a **sitios web no autorizados** o de contenido inapropiado para el entorno institucional.
- Enviar, publicar o difundir información que resulte **difamatoria hacia la universidad, sus servicios o su personal**.
- Introducir intencionalmente **software malicioso** (virus, spyware, troyanos, etc.) en la red de la universidad o realizar acciones que pongan en riesgo la **seguridad de los sistemas** y programas instalados.
- Hacer uso de redes sociales con **fines no laborales** durante el horario institucional.
- Ingresar a sitios de **pornografía, apuestas o cualquier otro contenido contrario a los fines educativos y administrativos** de la institución.

Artículo 47.- Actualización del Software Antivirus

Es obligación de cada usuario mantener actualizado el software antivirus instalado en el equipo de cómputo que le haya sido asignado. Esta medida es esencial para garantizar la protección de los sistemas institucionales frente a amenazas informáticas. En este sentido, se establecen las siguientes disposiciones:

1. Obligación del usuario:

Cada usuario es responsable de mantener **actualizada la base de datos de su software antivirus**. Esto implica asegurarse de que el sistema reciba periódicamente las actualizaciones necesarias para **detectar y neutralizar las amenazas de seguridad más recientes**.

2. Notificación en caso de problemas:

En caso de que el usuario **no pueda realizar la actualización por sí mismo**, ya sea por problemas técnicos, falta de permisos, acceso restringido u otra causa justificada, deberá **notificar de inmediato a la Unidad de Informática**, para que el personal correspondiente realice la actualización de manera oportuna.

3. Responsabilidad de la Unidad de Informática:

La Unidad de Informática será responsable de llevar a cabo la **actualización del software antivirus** en aquellos casos en que el usuario no pueda hacerlo por sus propios medios. Esta intervención tiene como finalidad **garantizar la protección continua de los sistemas informáticos** de la Universidad.

Artículo 48.- Respaldo de Información en el Servidor de Archivos

Todo Órgano Administrativo que haga uso del servidor de archivos en red para compartir información entre su personal deberá realizar, de manera periódica, el **respaldo de la información correspondiente al propio Órgano**, contenida en dicho servidor.

Esta acción tiene como finalidad **garantizar la disponibilidad, integridad y recuperación** de los datos en caso de que se presenten eventualidades como fallas técnicas, pérdida de información, accesos no autorizados o incidentes de seguridad.

CAPÍTULO IV
SOBRE RESPONSABILIDADES

Artículo 49.- Resguardo de Equipo de Cómputo y/o Periféricos

La Unidad de Informática será responsable de elaborar el documento de resguardo correspondiente al equipo de cómputo y/o periférico que se asignará a cada usuario. Este documento deberá elaborarse al momento de la entrega del equipo, entregándose **una copia al usuario resguardante**, mientras que **el original quedará bajo resguardo en la Unidad de Informática**.

El formato de resguardo deberá contener la siguiente información:

- **Número de Control:** Número identificador del usuario.
- **Nombre:** Nombre completo del usuario resguardatario.
- **Ubicación:** Área administrativa en la que se encuentra asignado el usuario.
- **Puesto:** Categoría o cargo que ocupa el usuario dentro de la institución.
- **Descripción del Equipo:**
  - Número de Inventario
  - Descripción del equipo
  - Marca
  - Modelo
  - Número de Serie
  - Precio
  - Estado del equipo
  - Observaciones pertinentes
- **Firmas requeridas:**
  - Del usuario resguardatario
  - Del titular de la Unidad de Informática
  - Del titular del Área de Recursos Materiales.

Artículo 50.- Entrega de Información y Recursos al Cese de Funciones

Toda persona que cese en sus funciones dentro de esta universidad y que tenga bajo su resguardo o responsabilidad el desarrollo, operación o administración de sistemas de información y equipo de cómputo, deberá realizar la **entrega formal y por escrito** de toda la documentación y recursos relacionados con dichos sistemas.

La entrega deberá hacerse al **titular del Órgano Administrativo correspondiente** o a la persona que le suceda en el cargo, y deberá incluir, como mínimo, lo siguiente:

- Documentación fuente utilizada para el análisis y desarrollo del proyecto
- Manuales técnicos y de operación
- Archivos de código fuente
- Respaldo actualizado del sistema
- Bases de datos
- Cualquier archivo o información almacenada en medios magnéticos, electrónicos o digitales relacionados con los sistemas administrados.

Esta disposición tiene como fin **garantizar la continuidad operativa** de los sistemas institucionales y la **protección de la información** bajo custodia del personal saliente.

Artículo 51.- Entrega de Equipo de Cómputo y Cancelación de Resguardo al Cese de Funciones

El personal que deje de prestar sus servicios en esta universidad y tenga bajo su resguardo o responsabilidad equipo de cómputo deberá realizar la **entrega física y por escrito** del equipo correspondiente al **titular del Órgano Administrativo** o a quien le suceda en el cargo.

Asimismo, deberá **solicitar por escrito a la Unidad de Informática** la **cancelación del documento de resguardo** correspondiente, a fin de dar por concluida formalmente su responsabilidad sobre dicho equipo.

Artículo 52.- Actualización de Resguardo por Cambio de Equipo o Dispositivo.

Cada vez que se realice un cambio de equipo informático o dispositivo asignado a un usuario, **éste deberá** solicitar por escrito a la Unidad de Informática **la** actualización del documento de resguardo correspondiente. **Dicha actualización permitirá mantener un control adecuado del inventario y asegurar la correcta información de los equipos asignados.**

Artículo 53.- Mantenimiento Preventivo e Inspección de Equipos de Cómputo

La Unidad de Informática será responsable de realizar **mantenimiento preventivo** a los equipos de cómputo asignados a los Órganos

Administrativos, con una **frecuencia mínima de una vez cada seis meses**. Asimismo, cada **cuatro meses** se llevará a cabo una **inspección técnica de los archivos** que incluirá:

- Revisión de archivos almacenados
- Verificación y actualización del software antivirus
- Inspección del estado de la paquetería y programas instalados
- Verificación de contraseñas o códigos de acceso
- Identificación de posibles **violaciones de seguridad** y usos indebidos o no autorizados del equipo

Estas acciones tienen como objetivo **garantizar el buen funcionamiento, seguridad y cumplimiento normativo** en el uso de los recursos informáticos institucionales.

Artículo 54.- Firma y Verificación del Resguardo de Bienes Informáticos

El usuario deberá **firmar o rubricar el documento de resguardo** correspondiente a los bienes informáticos que le hayan sido asignados, en un **plazo máximo de tres días hábiles** contados a partir del momento en que le sea presentado dicho documento.

Previamente a la firma, el usuario está obligado a **verificar que los datos registrados en el resguardo coincidan físicamente con el equipo o dispositivo entregado**, incluyendo número de inventario, características técnicas, estado y demás elementos descritos.

Artículo 55.- Revisión Física de Bienes Informáticos

Cuando se lleve a cabo una **revisión física de los bienes informáticos** con fines de **actualización de inventario**, el usuario deberá **facilitar dicha revisión** presentando la totalidad de los equipos y dispositivos que le hayan sido asignados y que estén registrados en su documento de resguardo. Esta colaboración es obligatoria y tiene como objetivo mantener actualizado el control institucional del patrimonio tecnológico.

CAPITULO V
SOBRE EXPECTATIVAS DE PRIVACIDAD

Artículo 56.- Sustitución Temporal de Disco Duro para Recuperación de Información

La Unidad de Informática tendrá la **facultad de retirar el disco duro** de un equipo de cómputo cuando se **imposibilite el acceso al sistema operativo** por medios convencionales, es decir, cuando no sea posible ingresar de ninguna forma al sistema.

Esta acción tendrá como finalidad la **recuperación de la información institucional** relacionada con el Órgano Administrativo correspondiente y con la Universidad de Seguridad Pública del Sureste, garantizando la conservación y resguardo de datos relevantes para las funciones institucionales.

Artículo 57.- Acceso a Equipos por Ausencia del Usuario Resguardante.

La Unidad de Informática tendrá la **facultad de acceder a un equipo de cómputo** y **sustraer información relacionada con el Órgano Administrativo correspondiente** en los casos en que el **usuario resguardante del equipo se encuentre ausente** y dicha información sea requerida para la continuidad operativa de las funciones institucionales.

Esta intervención deberá realizarse en presencia del **titular del Órgano Administrativo** o de un **representante autorizado**, a fin de garantizar la transparencia del procedimiento y proteger la confidencialidad de los datos.

Artículo 58.- Supervisión de Archivos y Accesos a Internet

La Unidad de Informática tendrá la **autoridad para acceder a los equipos de cómputo institucionales** con el fin de realizar tareas de **supervisión de archivos y control de accesos a internet**, bajo condiciones específicas que garanticen el respeto a los procedimientos administrativos y la seguridad de la información.

1. Acceso para Supervisión Técnica:

a) La Unidad de Informática podrá llevar a cabo la **verificación de archivos almacenados** en los equipos de cómputo, así como el **monitoreo de la actividad en línea**, lo cual incluye:

- Revisión de documentos digitales almacenados
- Análisis de historial de navegación web
- Evaluación de registros de acceso a internet
- Supervisión del uso de aplicaciones conectadas a la red

b) Estas acciones tienen como objetivo **detectar posibles usos indebidos**, preservar la integridad de los sistemas institucionales y asegurar el cumplimiento de las políticas tecnológicas vigentes.

2. Calendarización y Notificación de la Supervisión:

a) La supervisión **no será realizada de forma arbitraria**. Deberá establecerse una **calendarización previa**, en la que se definan las fechas y horarios específicos de las revisiones.

b) Dicha calendarización deberá ser **notificada con antelación** a los usuarios involucrados, garantizando que estén debidamente informados y puedan colaborar durante el proceso.

CAPITULO VI
SOBRE EL INCUMPLIMIENTO DE LAS POLITICAS

Artículo 59.- Cumplimiento de Obligaciones por Parte de los Servidores Públicos.

Los servidores públicos que tengan asignados bienes informáticos estarán obligados a cumplir con lo establecido en el presente lineamiento, **así como con las** disposiciones contenidas en la normatividad institucional y legal aplicable.

Artículo 60.- Responsabilidad por Incumplimiento de Normas y Políticas

La **Universidad de Seguridad Pública del Sureste** hará **responsable al usuario** de las consecuencias derivadas del **incumplimiento de las políticas, lineamientos y normas** establecidas en el presente documento.

Dicha responsabilidad se sustentará en lo dispuesto por el siguiente marco normativo:

- **Ley Patrimonial de la Administración Pública del Estado de Chiapas**

  - Publicación No. 259-2A-Sección-2010
  - **Título Primero**, Artículo 5, Fracción XV
  - **Título Cuarto**, Capítulo I, Artículo 44, Fracción VIII y Fracción IX
  - **Título Sexto**, Capítulo I, Artículo 60, Fracción X y Fracción XI

- **Reglamento de la Ley Patrimonial de la Administración Pública del Estado de Chiapas**

  - **Título Primero**, Capítulo Único, Artículo 6

DISPOSICIONES TRANSITORIAS

Artículo Primero.- Las normas y políticas contenidas en el presente documento podrán ser modificadas o adecuadas conforme a las necesidades que se presenten, mediante acuerdo autorizado por la **Rectoría de la Universidad de Seguridad Pública del Sureste**. Una vez aprobadas dichas modificaciones o adecuaciones, se establecerá la fecha de su vigencia y publicación oficial.

Artículo Segundo. - El desconocimiento de las normas establecidas en este documento por parte de los usuarios de los equipos de cómputo **no exime de la responsabilidad** ni libera de la aplicación de sanciones y/o penalidades derivadas de su incumplimiento.

ACUERDOS

Las presentes **Políticas de Uso y Resguardo de Bienes Informáticos** serán **aplicables a todo el personal operativo y administrativo** de la **Universidad de Seguridad Pública del Sureste**.

Cualquier **usuario que incurra en la violación** de estas disposiciones será sujeto a la **sanción disciplinaria correspondiente**, conforme a la normatividad interna y legislación aplicable.

La **Jefatura de la Unidad de Informática** será la instancia responsable de **difundir este documento** a todas las áreas que integran la Universidad, asegurando su conocimiento y cumplimiento por parte de todos los usuarios.

La presente normativa **entrará en vigor al día siguiente de su difusión oficial**.

MTRO. PABLO FILIBERTO CAMACHO AGUIRRE
RECTOR DE LA UNIVERSIDAD DE SEGURIDAD PÚBLICA DEL SURESTE.