Universidad La Salle Cuernavaca

POLÍTICA INTERNA

Prevención contra virus informático

Alcance:

Esta política aplica al personal docente y administrativo de la Universidad en sus secciones Bachillerato y Superior (incluyendo posgrado) y aquellos que realicen negocios a nombre de la **Universidad La Salle Cuernavaca A.C.** y que tengan o utilicen equipos o software del mismo.

Propósito:

El objetivo de este documento es establecer las políticas y lineamientos para proteger los equipos de computación de la **Universidad La Salle Cuernavaca** contra virus informáticos o cualquier información que pudiera ser dañina.

POLÍTICA

Es política de la **Universidad La Salle Cuernavaca** que sus maestros y personal administrativo, así como cualquier persona que realice negocios y/o actividades a nombre y/o a favor de la **Universidad** deben proteger los equipos de cómputo contra los virus o cualquier código malicioso que pudiera dañar los equipos y, en su caso, ocasionar la pérdida de información propiedad de la **Universidad**.

Para efectos de la presente política, las siguientes palabras, ya sea que se encuentren referidas en singular o en plural, tendrán el significado siguiente:

a) Antivirus:	Significan los programas que pueden prevenir, detectar y eliminar virus informáticos. Asimismo, son programas que pueden bloquear los virus que pueden dañar los equipos de cómputo y sistemas.
b) Colaboradores:	El personal docente y administrativo de la Universidad La Salle Cuernavaca A.C. (Superior y Bachillerato).
c) Universidad:	Universidad La Salle Cuernavaca A.C.
d) Usuario:	El personal docente y administrativo, así como cualquier otra persona que realice negocios y/o actividades a nombre y/o a favor de la Universidad La Salle Cuernavaca A.C.

Es obligación de todos los **Usuarios** mantener el buen funcionamiento de los equipos de cómputo de la **Universidad,** así como la integridad y confiabilidad tanto de éstos como de la información almacenada en los mismos. Para tales efectos, todos los **Colaboradores** y aquellos **Usuarios** diversos a los **Colaboradores**, de la **Universidad La Salle Cuernavaca** deberán utilizar prácticas seguras de computación y asegurarse de:

- Que el nivel apropiado de los programas anti-virus siempre esté activado en cada computadora que esté en el sitio de trabajo, laptop y servidor que se use para realizar los negocios y/o actividades por, a nombre de, o con de la **Universidad**;

- No deberán cambiar la frecuencia de actualizaciones automáticas de los anti-virus, ni interrumpir, desactivar o modificar las medidas de seguridad implementadas por la **Universidad** para prevenir, detectar y corregir el(los) ataque(s) de virus;

- Reportar de inmediato al área de Tecnología de la Información, cualquier problema con algún virus, o sospecha de incumplimiento o violación de la política por algún colaborador al correo electrónico tics@lasallecuernavaca.edu.mx Asimismo, deberá reportar si su equipo de cómputo presenta problemas de ejecución o funcionamiento y/o su operación muestra un bajo o un mal rendimiento;

- Nunca conectarse o permitir que otros conecten equipos que no sean de la **Universidad** a la red del mismo a menos que se haga a través del área de Tecnología de la Información y se cuente además con la aprobación de la Vicerrectoría.

- Tomar cualquier medida precautoria que sea necesaria y designada por la **Universidad**;

- No deberán intentar deshabilitar la operación eficaz del software anti-virus que opera en las computadoras del sitio de trabajo, en las computadoras portátiles y los servidores de las computadoras que estén conectadas a la red de la **Universidad.**

La violación de esta política sujeta a cualquier colaborador a acciones disciplinarias, que pueden ir desde una amonestación hasta la terminación de la relación laboral, sin perjuicio de las responsabilidades de carácter civil y/o las sanciones de índole penal a las que se pueda hacer acreedor con motivo de su conducta.

Cualquier persona o Usuario que intencionalmente introduzca y/o ejecute un virus al sistema o cualquier otro programa que intente dañar las operaciones de la Universidad, será responsable por los daños y perjuicios que ocasione a la Universidad y a terceros, quedando reservado el derecho de la Institución para ejercitar las acciones de carácter civil, penal o de cualquier otra índole que en su caso procedan contra dicha persona.

El Porqué de esta Política

- Asegurar el ambiente cada vez más interconectado de la tecnología de información de la **Universidad** es responsabilidad compartida de todos los **Usuarios** para preservar los activos de la información de esta institución

- Los virus y programas dañinos tales como “Los Caballos de Troya”, “Rootkits”, “Gusanos” y “Bombas Lógicas“ son amenazas a la seguridad de las operaciones de **la Universidad**. En la actualidad hay miles de virus y de otras amenazas a la seguridad de datos de la institución.

- Además, el creciente uso de conexión a los sistemas de red e Internet incrementa en forma significativa el riesgo de infección por virus. La distribución de documentos creados en

computadoras, con programas tales como Microsoft Word y Excel tienen un gran potencial para extender el virus e infectar los archivos a menos que se tomen las precauciones necesarias para evitar esto.

1. **Responsabilidades de los Usuarios :**

   - Considerando que el incumplimiento para seguir esta política puede comprometer la integridad de los archivos electrónicos y de los datos de la **Universidad**, el cumplimiento es **obligatorio.**

   - Los directores de las secciones y coordinadores son responsables de informar esta política dentro de sus unidades y de tomar acciones disciplinarias en caso de incumplimiento.

   - La Dirección General a través del área de Tecnología de la Información determinará el nivel de software necesario para garantizar la adecuada protección contra cualquier virus y deberán distribuir las actualizaciones cuando así sea necesario.

   - Todos los **Usuarios** son responsables de que el software anti-virus esté activado en sus computadoras, de reportar de inmediato cualquier virus y de reportar la sospecha de no cumplimiento o violación por parte de alguna otra persona.

   - Los **Usuarios** tienen prohibido descargar o copiar archivos o programas de otros **Usuarios** o de sitios web sin autorización de la Coordinación de Informática, ya que éstos pueden ser vulnerables a la presencia de virus, así mismo tienen prohibido guardar documentos de fuentes que son susceptibles de presentar virus.

   - Autorización. Para ello, quienes requieran de la descarga o copia de dichos archivos o programas para la realización de las actividades propias de la institución, deberán enviar un correo a la dirección de correo electrónico **tics@lasallecuernavaca.edu.mx** en el que justificarán las razones para descargar o copiar dichos programas o archivos.

   - En todos los casos, previa a la apertura, deben pasar o correr respecto de los mismos el programa antivirus vigente y/o actualizado.

   - Los directores y **Usuarios** de la **Universidad** son responsables de garantizar que únicamente las computadoras ya sean 1) propiedad de la **Universidad** o 2) autorizadas y/o administradas por la **Universidad,** estén permitidas en la Red de la institución.

     La autorización para que cualquier otro equipo de cómputo se habilite o permita en la red debe contar con la autorización de la Rectoría, las Direcciones y/o Coordinaciones, a través del área de Tecnología de la Información.

     La aprobación estará sujeta a pruebas que satisfagan las políticas de la **Universidad** de que la protección contra el virus estará actualizada y los parches críticos serán aplicados a la computadora de manera oportuna.

   - Los costos que se generen como resultado de la limpieza de los virus, se deberán facturar

al responsable por la filtración del virus.

Esto incluye los virus que se hubiesen originado de equipos que no son de la **Universidad** (equipos tales como computadoras adquiridas por un proveedor, personal externo o consultores) o virus infiltrados por anexos sospechosos enviados a través de un correo electrónico.

- El uso de los equipos de cómputo propiedad de terceros autorizados, así como los equipos personales autorizados de los maestros y administrativos que laboran en la **Universidad**, únicamente podrán conectarse al servicio de Internet propiedad del mismo **vía inalámbrica**. Será responsabilidad de dichos usuarios autorizados mantener libre de virus, rootkits y códigos maliciosos sus equipos.

2. Aplicación de la Política:

A) ¿Qué hacer en caso de detectar un virus en su PC o Laptop?

Si el software anti-virus en su computadora detecta un virus, de inmediato contacte a la Coordinación de Informática al correo electrónico: tics@lasallecuernavaca.edu.mx dónde le indicarán como proceder, en caso necesario le ayudarán a quitar el virus o si es necesario enviarán un técnico para ayudarlos a eliminar el virus.

Prevención.

Considerando que ninguna medida es 100% efectiva contra la expansión de un virus, la implementación de las medidas contenidas en esta política ayudará significativamente a reducir el riesgo de introducir y expandir los virus en el ambiente de las computadoras de la **Universidad**.

B) ¿Qué software se debe usar?

La Rectoría, las Direcciones y/o Coordinaciones en coordinación con el área de tecnología de la información definirán y proporcionará los productos adecuados así como las instrucciones.

C) Procedimientos.

PC´s, laptops y servidores, sin importar el sistema operativo del software, deberá estar protegido con un software anti-virus y con un nivel de actualización apropiado.

Como mínimo, este software deberá estar activado en todo momento y deberá comprobar todos los ejecutables, archivos, documentos y hojas de cálculo de cualquier archivo abierto, escrito, creado o una operación de transferencia de archivo.

El software se debe configurar para que en forma automática explore todo lo que ingresa de cualquier fuente externa a su recepción (ej. de Internet, memorias flash, entradas externas del correo, etc.).

Periódicamente respalde sus archivos críticos

D) Otras Medidas.

Todos los archivos en todos los servidores se deben escanear debido a los virus que siguen las actualizaciones de los anti-virus que tienen firma electrónica archivada y/o a las mejoras de los motores del software anti-virus.

Todos los servidores del correo electrónico deben tener controles que les permita detectar los virus que infectan los correos electrónicos y archivos con anexos y evitar que éstos sean distribuidos o enviados a otros.

E) **Reportes.**

Cuando un virus es detectado en un punto de acceso de la red de la **Universidad** (ej. En un en un dispositivo **"USB"** o por bajar un archivo desde Internet), se mostrará que nuestras defensas están operando adecuadamente. Usted deberá reportar está situación a la Coordinación de Informática en todos los casos antes mencionados.

Cuando un virus se encuentra en un disco duro o un servidor, esto podría significar que el sistema anti-virus pudiera estar sin actualizar o no estar activado adecuadamente. La persona encargada de quitar este virus debe emitir un reporte de inmediato por este incidente indicando como ocurrió, si lo sabe, y las acciones aplicadas para evitar que vuelva a pasar) y deberá enviar el reporte al área de Tecnología de la Información.

F) **Recursos.**

Contactar al área de Tecnología de la Información en caso de necesitar la última versión de antivirus y los procedimientos respectivos.

Vigencia

La presente Política tendrá vigencia inmediata a partir de la fecha de su aprobación y firma.

Fecha 13 de Noviembre de 2014