MUNICIPALIDAD PROVINCIAL DE CORONEL PORTILLO

OFICINA DE TECNOLOGIAS DE LA INFORMACION

NORMA DE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS

Historial de Cambios

Edición	Fecha	Autor	Cambios realizados
01	15/10/2014	Ing. Teofilo Pastor Perez Lazo	Versión Inicial
01	31/10/2014		

1. Objetivo

Definir las medidas de uso y resguardo que debe tener un usuario de la Municipalidad Provincial de Coronel Portillo, en adelante la MPCP, con respecto a los recursos tecnológicos que le son asignados para el desarrollo de su trabajo.

2. Definición de términos

2.1. **Software base:** El software base o software de sistemas puede definirse como programas de cómputo y/o rutinas relacionadas que manejan y apoyan el procesamiento de sistemas de aplicación y hardware de cómputo. Esto incluye el sistema operativo, así como compiladores, el software que se requiere para monitorear y sintonizar el sistema operativo.

2.2. **Licencia de Software:** Autorización o permiso concedido por el titular del derecho de autor, en cualquier forma contractual, al usuario de un programa informático, para utilizar éste en una forma determinada y de conformidad con unas condiciones convenidas.

3. Disposiciones generales

Se tienen definidas las siguientes responsabilidades:

3.1. El Encargado de Seguridad de la Información es responsable de:

- Aprobar el estándar de software antivirus a utilizar por la MPCP y velar por la adecuada administración y actualización del mismo.
- Revisar los reportes de inventarios de software de los servidores y las estaciones de trabajo.

3.2. El Encargado de Seguridad del Centro de control y Mantenimiento de Servidores es responsable de:

- Asegurar que el software instalado en los servidores este de acuerdo a las licencias adquiridas por la MPCP.
- Elaborar los reportes de inventarios de software de los servidores.

3.3. El Encargado General de la Información es responsable de:

- Asegurar que el software instalado en las estaciones de trabajo esté de acuerdo a las licencias adquiridas por la MPCP.
- Elaborar los reportes de inventarios de software de las estaciones de trabajo.

3.4. Los usuarios son responsables de:

- Transferir de manera constante la información crítica para sus labores a las carpetas creadas para tal fin, en los servidores o equipos de procesamiento centralizados.

4. Descripción

4.1. A fin de garantizar el correcto funcionamiento de los equipos, el Encargado General de la Información debe asegurarse que cuente con un plan de mantenimiento preventivo/correctivo de la infraestructura tecnológica de la MPCP, así como los mecanismos de seguridad más adecuados para su protección.

4.2. El Encargado General de la Información debe proveer los mecanismos adecuados para que se respeten permanentemente las instrucciones del fabricante, por ejemplo: protección por exposición a campos electromagnéticos fuertes, uso de corriente estabilizada y otros.

4.3. Los equipos informáticos son entregados por la MPCP a su personal, para que pueda cumplir las labores que se le ha encomendado.

4.4. Los equipos informáticos no serán utilizados por los usuarios para desarrollar labores personales, ni de terceros bajo ninguna circunstancia.

4.5. Es deber de todos los usuarios velar por el buen uso y cuidado de los equipos entregados por la MPCP.

4.6. El usuario es responsable por la información almacenada en el equipo que se le ha asignado. Es responsabilidad de los usuarios alertar al Encargado de Seguridad de la Información, de cualquier riesgo potencial a los que puedan estar expuestos tanto los equipos como la información.

4.7. Los accidentes ocasionados a los equipos entregados por la MPCP causados por descuidos del personal serán responsabilidad del usuario al que se asignó el equipo.

4.8. El personal deberá informar al:

- Encargado de Seguridad de la Información correspondiente, por cualquier daño que pudiera haberse producido sobre el equipo.
- Área de administración en caso de robo.

4.9. Los usuarios son responsables de reportar cualquier acto que atente contra los equipos de la MPCP o cualquier acto sospechoso.

4.10. Por ningún motivo se prestará a terceros el computador personal, computador portátil, etc. que contenga información confidencial.

4.11. Los usuarios no están autorizados a transportar equipos asignados por la MPCP, salvo sean estos equipos portátiles debidamente autorizados. En caso que un equipo portátil sea requerido de manera circunstancial, se necesitará una autorización por escrito del Encargado General de la Información.

4.12. Los equipos deberán ser ubicados en áreas que permitan proveer la seguridad que requiera el equipo en base a la confidencialidad de la información almacenada.

4.13. Todos los equipos informáticos que forman parte de la infraestructura tecnológica de la MPCP, y que deban ser ubicados fuera de las instalaciones de la MPCP, deben cumplir con lo dispuesto en la presente norma.

4.14. En caso que el usuario tenga asignado un equipo portátil este deberá ser resguardado según se indica en la NO-031 – Norma de uso de equipos móviles.

DE LA INFORMACIÓN EN LOS EQUIPOS

4.15. Toda la información almacenada en los equipos entregados, se considera información de la MPCP.

4.16. La MPCP podrá en cualquier momento hacer revisiones de la información almacenada en los equipos con el objeto de asegurar que los mismos se estén usando en cumplimiento con las funciones para las que fueron asignados.

4.17. Los usuarios no deben modificar la configuración del software base.

4.18. Los usuarios están prohibidos de instalar cualquier tipo de software en los equipos asignados por la MPCP. El Encargado General de la Información través de sus miembros es la única autorizada para realizar instalaciones en los equipos de la MPCP.

4.19. El software "freeware" o "shareware" adquirido por correo o por cualquier otro servicio de Internet no es permitido, salvo que sea evaluado y aprobado por el Encargado de Seguridad del área de la Información.

4.20. El Encargado de Seguridad del Centro de control y Mantenimiento de Servidores es responsable de asignar a todos los usuarios de la MPCP un espacio donde puedan almacenar información a ser respaldada según los mecanismos estándares. El área de OTI es responsable de velar por que la información de los usuarios esté incluida en las estrategias de respaldo de la MPCP y que los usuarios estén almacenando la información crítica en los espacios asignados.

4.21. El usuario será responsable de mantener depurado el espacio asignado.

4.22. La información que no sea almacenada en las ubicaciones asignadas por el Encargado de Seguridad del Centro de control y Mantenimiento de Servidores no será incluida en las estrategias de respaldo de la MPCP, en consecuencia, es responsabilidad del usuario respaldar esta información.

4.23. Debe evitarse conservar información restringida y/o confidencial en los discos duros de las estaciones de trabajo, la misma deberá conservarse en los equipos de procesamiento centralizados

en la medida que la plataforma tecnológica lo soporte. El usuario es responsable por la seguridad que brinda a la información conservada en su estación y, en especial, por la que está expuesta para consulta o acceso de otros usuarios por vía de los recursos compartidos, ya sea que tengan o no contraseñas de acceso.

4.24. Si la información residente en una estación de trabajo está cifrada para evitar la manipulación no autorizada, la llave de encriptación y el material utilizado para la generación de ésta, no deben estar almacenadas en el mismo medio en donde reside la información cifrada.

4.25. La información sensible o confidencial, una vez impresa, debe ser retirada de la impresora inmediatamente.

4.26. Los empleados no deben navegar por las computadoras o redes de la MPCP, a menos que sea una función de su cargo, y que esto tenga un propósito demostrable y justificado.

4.27. El usuario responsable del computador personal debe de bloquear el mismo cuando por causa laboral o extra laboral está en necesidad imperiosa de ausentarse de su lugar de trabajo (Windows + L). Esto impide tanto el acceso no autorizado al sistema, como a las aplicaciones. El usuario que no deje bloqueado su computador al ausentarse, será responsable por el uso no autorizado del equipo, de la red o de las aplicaciones instaladas.

4.28. Todos los equipos de cómputo deben contar con un protector de pantalla institucional o uno autorizado por el área de OTI y el Encargado General de la Información, que exija el ingreso de una contraseña para permitir utilizar los recursos e información contenida en el equipo.

4.29. Todos los equipos de cómputo deben tener contraseñas de inicio de sesión y contraseña de BIOS. La administración de las contraseñas de BIOS debe encontrarse a cargo del personal del área de OTI.

DE LA ASIGNACIÓN DE LOS EQUIPOS

4.30. El área de OTI en el momento de asignar un equipo a un usuario o cambiar alguna de las partes del equipo asignado, debe registrar un inventario del equipo y partes asignadas, obteniendo la firma del usuario como conformidad de la recepción o la modificación.

DE LA AUDITORÍA Y REVISIÓN DEL USO DE LOS EQUIPOS Y ESTACIONES DE TRABAJO

4.31. El área de OTI deberá:

- Elaborar un inventario total del software instalado en las estaciones de trabajo emitiendo un informe dirigido al Encargado de Seguridad del área de OTI en el que se indique las estaciones que tienen instalado software no autorizado y de qué tipo es éste, dicho informe deberá ser analizado para tomar las medidas que correspondan.

- Verificar aleatoriamente o sobre la base de los registros de auditoría o eventos de seguridad, si el usuario ha modificado la configuración del software base o hardware de su equipo, notificando de este hecho al usuario, a su supervisor directo y al Encargado de Seguridad de la Información correspondiente.

4.32. El área de OTI deberá incorporar en sus actividades la revisión selectiva del inventario de equipos asignados a usuarios, verificando en forma aleatoria la asignación efectuada y el uso.

5. Vigencia

Entrará en vigencia a partir de su aprobación.

6. Aprobación

Será aprobada mediante Resolución de Gerencia General.