MANUAL OPERATIVO DE LA
COORDINACION DE GESTION TECNICA

SEGURIDAD INFORMATICA

POLITICA DE BUEN USO DE LA PC, DISPOSITIVOS Y LUGAR DE TRABAJO

Nro. Versión: 1.2 - Fecha: 21/05/08

Contenido: Política de buen uso de la PC, dispositivos y lugar de trabajo

Seguridad Informática • Coordinación de Gestión Técnica • DNCTLyA
Servicio Nacional de Sanidad y Calidad Agroalimentaria
Av. Paseo Colón 315 - Piso 6º B - Capital Federal - C1063ACD
Teléfono (011) 4121- 5005 - Email: mesadeayuda@senasa.gov.ar

Índice

01. Introducción..... Página 2

02. Política de escritorios limpios..... Página 2

03. Seguridad física y ambiental..... Página 2

04. Protectores de Pantalla y Carpetas Compartidas..... Página 3

05. Contraseñas fuertes..... Página 3

06. Apagado y encendido de la PC..... Página 4

07. Instalación/Desinstalación de Programas y Dispositivos..... Página 4

08. Conclusiones, Recomendaciones..... Página 5

09. Glosario de Términos..... Página 8

10. Contactos..... Página 12

01. Introducción

El motivo del presente manual instructivo es mejorar el uso de los recursos informáticos y del lugar físico que se le fue asignado para la realización de las tareas.
Recuerde que toda la información conservada en los equipos informáticos (Pc´s., servidores, notebooks, etc.), los dispositivos periféricos (mouse, teclado, monitor, parlantes, etc.), papeles (formularios, notas, legajos, etc.) y el mobiliario (escritorio, biblioteca, armarios, etc.) son propiedad del ORGANISMO, por lo que la responsabilidad del correcto uso de los mismos es de su interés.
El uso del correo electrónico, internet, intranet y demás sistemas aplicativos que corren en los equipos puede ser administrado y/o monitoreado por los responsables del Area de Sistemas de acuerdo con las pautas de seguridad definidas, para su uso correcto.
El monitoreo consiste en detectar por medio de aplicaciones de seguridad, como Firewalls o Sistemas Detectores de Intrusos, la presencia de patrones de archivos que indiquen la presencia de virus, keyloggers, etc. En ningún momento “monitoreo” se refiere a “leer” los e-mails o datos del usuario.
Aquí se enumeran una serie de recomendaciones a los usuarios para el buen uso de los recursos.

02. Política de escritorios limpios

Hay que mantener ordenado el escritorio en todo momento del día, al finalizar la jornada se deben recoger todos los papeles sueltos y hojas de trabajo, los mismos se deben guardar en carpetas y cajones. Esto contribuye al orden y limpieza del sector de trabajo.

No se deben dejar papeles pegados en el monitor, ni en la Pc., tampoco en cualquier parte del escritorio, que den el nombre de usuarios o contraseñas de accesos a la Pc., al correo electrónico, internet o cualquier sistema del que sea usuario. Esta información es muy útil para usted y para el Organismo y no debe ser compartida.
Un ejemplo típico es el envío de correo electrónico con difamaciones hacia otra persona o de información importante desde una Pc. “tomada prestada” por otro usuario.

03. Seguridad física y ambiental

Los problemas de corriente en la red eléctrica como picos y baja tensión o apagones, pueden causar diversos daños físicos a su computadora, pudiendo afectar memoria, disco rígido, diversos componentes de la Pc., impresoras y otros dispositivos. No debe pisar, apoyar la silla o escritorios sobre cables eléctricos o de datos, en éstos casos debe comunicarse inmediatamente con el área

correspondiente para su reparación y/o mejor ubicación de los mismos. Esto es muy importante principalmente por su integridad física.

Mantenga limpios todos los dispositivos electrónicos que utiliza en su labor diaria como Pc´s., monitores, mouse, teclados, impresoras, etc.
No ingiera comida ni bebidas sobre los dispositivos, los mismos dañan los componentes internos de los mismos.

04. Protectores de Pantalla y Carpetas Compartidas

Configure el protector de pantalla con un tiempo de inicio de 5 minutos, esto no solo beneficia al mejor cuidado de los recursos de la Pc., además mantiene la confidencialidad de la información y a los datos que quedan expuestos a modificaciones o robos, cuando un usuario se aleja del puesto de trabajo.

Evite compartir innecesariamente archivos, carpetas o discos completos. Si debido a sus tareas es necesario que las/los comparta, hágalo solo por el tiempo necesario para copiar o utilizar los archivos y no se olvide de compartir recursos con una contraseña fuerte. (ver contraseñas)

05. Contraseñas fuertes

El uso de contraseñas es necesario para mantener la *confidencialidad* de la información. Se define confidencialidad a que la información sea accesible solo a aquellas personas (usuarios) autorizadas a tener acceso. Este criterio para componer una contraseña debe utilizarse para las contraseñas de correo electrónico, internet, de acceso a la Pc., a los sistemas, carpetas, etc...
Una contraseña para que se la considere fuerte debe contener al menos:

- 8 (ocho) dígitos.
- Caracteres numéricos no consecutivos.
- Caracteres alfabéticos no consecutivos.
- Caracteres especiales como por ejemplo ° # &) ¡ / + % € @
- No deben ser nombres propios o de familiares.
- No deben ser fechas de nacimiento/cumpleaños/aniversarios.
- El uso de una misma contraseña para diversos accesos, facilita que se pueda recordar fácilmente pero también implica el riesgo que si alguien descubre una de ellas, podrá ingresar a todas los lugares donde la haya utilizado.

- Cambie la contraseña la primera vez que se la asignen.
- Recuerde cambiar la contraseña en períodos no prolongados de tiempo (al menos una vez por mes).
- Evite repetir las contraseñas cada vez que las cambia, por lo menos en las últimas 10 (diez) veces.
- No divulgue la contraseña ni la deje anotada en lugares inseguros.

06. Apagado y encendido de la PC

Encienda la Pc. presionando el botón de power (encendido) de la misma, si al intentar ingresar aparecen mensajes o pantallas de error durante el encendido, comuníquese con el Area de Servicios Informáticos para su atención. No demore muchos días en hacer el reclamo ya que aunque usted piense que su Pc. esté funcionando de manera correcta, la realidad es que no es así. El retraso en hacer el reclamo podría derivar en la perdida total de la información y/o del equipo.

Si al encender la Pc. se activa el programa *Scandisk*, o le pregunta si desea utilizarlo, Acéptelo y déjelo trabajar hasta su finalización, no lo detenga, por más tiempo que demore. Si ésta forma de ingreso al Sistema Operativo es frecuente, comuníquese con el Area de Servicios Informáticos para su atención.

Apague la computadora de la manera correcta, es decir, haga click con el mouse en Inicio, luego Apagar y Aceptar, o de la manera que el Sistema Operativo de su Pc. lo permita. De ninguna manera apague presionando el botón de Power o desenchufándola, de este modo se dañará la misma.

07. Instalación/Desinstalación de Programas y Dispositivos

Esta totalmente prohibido realizar instalaciones/desinstalaciones de software y de cualquier dispositivo de hardware sin la correspondiente autorización del sector de Servicios Informáticos.
Cualquiera de estas instalaciones/desinstalaciones efectuadas sin aviso, pueden dañar los componentes de la Pc. y/o en caso de ser virus o software malicioso, puede extenderse a toda la red, ocasionando una caída en los distintos servicios y pérdidas de información.

08. Conclusiones

Recomendaciones sobre el uso y cuidado de los equipos y suministros

Manejo de la PC o estación de trabajo

Mantenga el equipo en perfecto estado de limpieza.
Evite el movimiento de su Pc. cuando esté encendida.
Evite que se introduzcan elementos extraños en la Pc.
Evite que se golpee.
Apague los dispositivos conectados a su Pc. cuando termine de trabajar.
Evite encender el equipo cuando note fallas en el suministro eléctrico.
No deje objetos con líquido muy cerca del equipo

Encendido y apagado del equipo

Encendido del equipo

Encienda primero el monitor, luego la impresora y demás dispositivos conectados.
Encienda la Pc.

Apagado del equipo

Cierre todas las aplicaciones que este utilizando.
Apague la Pc.
Apague el monitor, la impresora y demás dispositivos conectados.

Manejo de las impresoras de cinta

Mantenga la impresora en perfecto estado de limpieza.
Cuando se trabe el papel remuévalo sin ejercer presión.
Si nota una situación anormal en el funcionamiento de la cinta, reemplácela por una nueva.
No remueva las tapas de la impresora, ya que éstas le sirven de protección a la misma.
Evite que se golpee.

Manejo de las impresoras Láser

Mantenga la impresora en perfecto estado de limpieza.
Cuando el papel se atore, proceda a levantar la tapa superior, levante el toner y tire el papel hacia adelante sin doblarlo.
Si el papel se atora en la parte trasera, baje la tapa y tire cuidadosamente el papel evitando que se rompa.
Trate las piezas con cuidado para evitar daños en la impresora.

Cuando vaya a solicitar acetatos (papel para transparencias) y/o stickers haga la aclaración a Suministros que van a ser utilizados en impresora láser.
El papel a utilizar en la impresora debe ser de 80 grs.

Manejo de Toners y cartuchos de tinta

Sáquelos de su envoltorio original solo al momento de tener que usarlos.
No los agite.
Retire el protector plástico siguiendo las instrucciones del envoltorio.
Colóquelos con cuidado y sin hacer presión excesiva
No los deje sueltos, ni apoyados en ningún lugar.
Manéjelos con cuidado, podría manchar su ropa.
Se recomienda que esta tarea sea realizada por el personal del Area de Soporte Técnico

Manejo de diskettes

Guarde los diskettes en porta diskettes o cajas que ofrezcan las condiciones adecuadas para protegerlos del medio externo.
Escriba la etiqueta antes de pegarla a los diskettes (preferentemente con marcador).
No toque las ventanas de lectura y escritura de sus diskettes.
Es preferible reemplazar la etiqueta a sobrescribirla.
No exponga sus diskettes a campos magnéticos (monitor, parlantes, etc.).
No exponga los diskettes a temperaturas extremas de calor o frío.
No doble sus diskettes.
Manipule los diskettes cuidadosamente.
Si envía sus diskettes por correo postal, introdúzcalos en una caja de cartón.
Al sacar o introducir los diskettes en la unidad de disco no haga presión.
No retire los diskettes de la unidad si la luz está encendida
No coloque objetos pesados sobre los diskettes.
No pegue ganchos a los diskettes.

Manejo de unidades zip

Guarde los zip en su respectiva caja para protegerlos del medio externo.
Escriba la etiqueta antes de pegarla (preferentemente con marcador).
No toque las ventanas de lectura y escritura
Es preferible reemplazar la etiqueta a sobrescribirla.
No exponga sus zips a campos magnéticos (monitor, parlantes, etc.).
No los exponga a temperaturas extremas de calor o frío.

Al sacar o introducir los zips en la unidad de lectura no haga presión.

Manejo de medios ópticos (cd/dvd)

Guarde los cd´s en su respectiva caja para protegerlos del medio externo.
No exponga los cd´s a temperaturas extremas de calor o frío.
Al sacar o introducir los cd´s en la unidad de lectura no haga presión.
Evite rallar la parte posterior del cd.
No limpie el cd frotándolo contra su ropa, hágalo con un paño seco desde el centro hacia fuera.

Manejo de memoria USB, USB flash drive o Pendrive

Antes de retirar la memoria del puerto USB, vaya a "Quitar el Hardware con seguridad", de ninguna manera retírelo sacándolo directamente.
Evite el daño físico, la humedad, los campos magnéticos y el calor extremo.
Al no usarlo, tápelo con el capuchón que trae de fábrica.
En lo posible, enchúfelo en los puertos de entrada que se encuentran en la parte posterior de la computadora.

09. Glosario de Términos

Backup (copia de seguridad o copia de respaldo): Tienen por objetivo mantener cierta capacidad de recuperación de la información ante posibles pérdidas y se refiere a la copia de datos (parcial o total) de tal forma que estas copias adicionales puedan restaurar un sistema después de una pérdida de información.

Carpetas Compartidas: A través de ellas se puede compartir carpetas o archivos con otro usuario o grupo de ellos. Es muy importante utilizar una contraseña para que no acceda personal ajeno a la tarea. Si la Pc se encuentra en el Dominio de Senasa, esta tarea se verá más segura y protegida, además de contar con un servicio de Backup o resguardo de de información.

Contraseña o Clave: También llamada password, es una forma de autenticación que utiliza datos secretos para controlar el acceso hacia algún recurso, como puede ser la Pc, carpetas o archivos compartidos, el correo electrónico, etc., y es un método de seguridad que se utiliza para identificar a un usuario La contraseña debe mantenerse en secreto ante aquel a quien no se le permite el acceso.

Disco Rígido: También llamado Hard disk, HD, HDD (hard disk drive) o Disco duro, es un dispositivo de almacenamiento de datos permanente que utiliza tecnología magnética.

Dominio: Es un grupo lógico de máquinas que comparten cuentas de usuarios y seguridad de los recursos. Los usuarios de un mismo dominio tendrán un inicio de sesión único en el Servidor del Dominio para acceder a los recursos de cualquier parte de la red y una cuenta única para acceder a las máquinas del dominio.

Firewall: Es un dispositivo que puede ser de software o hardware, que conecta las Pc. de la red y el acceso a Internet y controla todas las comunicaciones que pasan de una red a la otra y en función de ello permite o deniega su paso.

FTP (File Transfer Protocol): El Protocolo de Transferencia de Archivos se lo suele utilizar para enviar archivos a través de Internet.

Hardware: Se refiere a todos los componentes físicos, aquellos que se pueden tocar, en el caso de una computadora personal serían el disco rígido, la disketera, monitor, teclado, memoria, etc.

IDS (Intrusion Detection System): El Sistemas Detector de Intrusos es una herramienta de seguridad que intenta detectar o monitorizar los eventos ocurridos en un determinado sistema informático o en la red, en busca de intentos de comprometer la seguridad de dicho sistema o la red misma.

Internet: Es un conjunto de redes de computadoras creada a partir unir redes de menor tamaño (LAN o redes locales) con redes de mayor tamaño (WAN o redes extensas), formando una gran "red de redes" que es la más grande del mundo. A Internet no solo se pueden conectar computadoras, también cámaras, teléfonos, etc.
Los servicios más utilizados en Internet son: Correo Electrónico, la WWW o Word Wide Web, FTP o Protocolo de Transferencia de Archivos, los Grupos de Noticias, IRC o Chat y los Servicios de Telefonía como Videoconferencias.

Intranet: Es una red de computadoras dentro de una red de área local (LAN) privada, empresarial o educativa que proporciona herramientas de Internet. Sus funciones principales son de acceso a la información, listados, informes y consultas con el fin trabajar en forma remota y estar conectados al lugar de trabajo o de consulta las 24 horas del día; es también un importante medio de difusión de información interna del Organismo a todos los niveles.
Generalmente el acceso a las mismas es vía WEB.

IRC (Internet Relay Chat): La Charla Interactiva por Internet o Chat como es más conocido, es un servicio que permite entablar una conversación en tiempo real con una o varias personas por medio de texto, permitiendo también el envío de imágenes, archivos, etc.

Keyloggers: Es un programa que recoge las pulsaciones que realiza el usuario sobre el teclado para enviárselo a través de Internet, averiguando normalmente las contraseñas que el usuario teclea.

Pendrive: Es un dispositivo de almacenamiento para guardar la información que puede utilizar memoria flash y que son resistentes a los rasguños externos y al polvo
Estas memorias se han convertido en el sistema de almacenamiento y transporte personal de datos más utilizado, y su capacidad de almacenamiento es de 1, 2, 4, 8 GB o más (esto supone, como mínimo, el equivalente a 715 disquetes).
Las memorias actuales cumplen la especificación USB 2.0, lo que les permite alcanzar velocidades de escritura/lectura de hasta 480 Mbit/s teóricos.
Su mayor utilidad es el transporte de datos entre dispositivos y su facilidad de acarreo a los distintos sitios.
Supuestamente la memoria flash que lleva puede retener los datos durante unos 10 años y escribirse un millón de veces.

Protector de Pantalla: Un protector de pantalla es una aplicación que protege el sistema y el hardware de la computadora durante largos periodos de trabajo; Este se activa cuando el sistema esta inactivo por un determinado tiempo. Los protectores de pantalla son utilizados para realizar un ahorro de energía, y las imágenes que se muestran son generalmente interactivas.

ScanDisk: Es un programa utilizado para comprobar tanto la integridad de la superficie física del disco rígido de la Pc. como la entereza de los datos almacenados en él.

Sistema Aplicativo: Es un programa o conjunto de ellos, que brindan un servicio para el que fueron especialmente diseñados. Ej. administración, facturación, personal, etc.

Sistema Operativo: Es un programa destinado a permitir la comunicación del usuario con la computadora y gestionar sus recursos de una forma eficaz, facilitando la interacción del hardware con el resto de las aplicaciones. Ej: Windows, Linux, Dos, etc.

Software: Es intangible, existe como información, es el conjunto de programas y procedimientos necesarios para hacer posible la realización de una tarea específica, esto incluye sistemas aplicativos, sistemas operativos, base de datos, planilla de cálculos, etc.

USB (Universal Serial Bus): Es un puerto que sirve para conectar distintos dispositivos a una computadora como teclados, Mouse, escáner, cámaras digitales, parlantes, teléfonos celulares, impresoras, etc.
Es un estándar de conectores y su principal característica es que los pueden conectarse y desconectarse con la computadora en funcionamiento, configurándose de forma automática.

Unidades ZIP o Discos ZIP: Los discos ZIP son dispositivos magnéticos, extraíbles y de alta capacidad que pueden leerse y escribirse mediante unidades ZIP, son similares a los disquetes (floppy) pero son mucho más rápidos y ofrecen una capacidad de almacenamiento mucho mayor. Así como los disquetes suelen ser de 1'44 MB los discos ZIP existen en dos tamaños, de 100 y 250 MB.
En la actualidad se ven reemplazados por los CD´s o DVS´s.

Videoconferencia: Es una comunicación simultánea bidireccional de audio y video, que nos permite establecer reuniones individuales o con grupos de personas situadas en lugares alejados entre sí

Virus: Un virus informático es un programa que se copia automáticamente y que tiene por finalidad alterar el normal funcionamiento de una computadora, un grupo de ellas o la red.
Se ejecuta en el ordenador sin previo aviso y puede corromper el resto de los programas, datos e, incluso el mismo sistema operativo.
Algunos ejemplos de virus:
Worms o gusanos: se registran para correr cuando inicia el sistema operativo ocupando la memoria y volviendo lento al ordenador, pero no se adhieren a otros archivos ejecutables. Utilizan medios masivos como el correo electrónico para esparcirse de manera global.

Troyanos: suelen ser los más peligrosos, ya que no hay muchas maneras de eliminarlos.

No son virus en si mismo, acostumbra ser un programa alojado dentro de una aplicación, una imagen, un archivo de música u otro elemento de apariencia inocente, que se instala en el sistema al ejecutar el archivo que lo contiene. Una vez instalado parece realizar una función útil pero internamente realiza otras tareas de las que el usuario no es consciente.

Jokes o virus de broma: no son realmente virus, sino programas con distintas funciones, pero todas con un fin de diversión, nunca de destrucción, aunque pueden llegar a ser muy molestos.

Hoaxes o falsos virus: son mensajes con una información falsa; normalmente son difundidos mediante el correo electrónico, su común denominador, es pedirle al usuario que los distribuya "a la mayor cantidad posible de conocidos". Suelen ser cadenas de mensajes por enfermos, solidarios, denuncias, premios excesivos, etc.

10. Contactos

Área de Servicios Informáticos
E-mail: serviciosinformaticos@senasa.gov.ar
Teléfono: 4121-5005

Área de Aplicaciones Centrales
E-mail: aplicaciones@senasa.gov.ar
Teléfono: 4121-5125

Área de Ingeniería en Comunicaciones, Voz y Datos
E-mail: comunicaciones@senasa.gov.ar
Teléfono: 4121-5210

Área de Seguridad Informática
E-mail: seguridad@senasa.gov.ar
Teléfono: 4121-5214

Coordinación de Gestión Técnica
E-mail: gestión@senasa.gov.ar
Teléfono: 4121-5266

Documentación

Título del documento	MGSI Política de Buen Uso de la P.C., dispositivos y lugar de Trabajo.
Pertenece	Manual de Gestión de Seguridad de la Información
Versión	1.0
Fecha	03/01/2007
Dueño de Datos	Coordinación de Gestión Técnica
Propietario	Seguridad Informática
Responsable	Ing. Damián Ienco

Revisión Histórica

Fecha	Versión	Motivo
15/08/07	1.0	Primer versión
05/09/07	1.1	Segunda versión
21/05/08	1.2	Tercer versión