POLITICAS DE MITIGACION DE RIESGOS

TOMO II

PREVENCIÓN Y POLÍTICAS DE SEGURIDAD

INDICE TOMO II

PREVENCIÓN Y POLÍTICAS DE SEGURIDAD

Proyecto:

"POLÍTICAS DE MITIGACIÓN DE RIESGOS"

Objetivo específico:

PREVENCIÓN Y POLÍTICAS DE SEGURIDAD

ACTIVIDAD 5

"MANUAL PARA EL BUEN USO DE LAS HERRAMIENTAS INFORMÁTICAS PARA EL USUARIO FINAL"

MANUAL PARA EL BUEN USO DE LAS HERRAMIENTAS INFORMÁTICAS PARA EL USUARIO FINAL

Esta actividad contempla la elaboración de 1 manual destinado al usuario final, orientados a Hardware y Software.

Ambos manuales mantienen una estructura similar, enmarcado en el contexto del usuario sin conocimientos de las nuevas tecnologías y para llegar con mayor fluidez al lector se ha decidido utilizar una estructura de preguntas:

¿Qué es?

¿Para que sirve?

¿Cómo se usa?

¿Cómo se cuida?

En rasgos generales. Existiendo particularidades para cada uno en su área.

En esta actividad se hace la entrega de un **"MANUAL DE HERRAMIENTAS INFORMÁTICAS PARA USUARIO FINAL"**, completo, con sus 2 capítulos fundamentales y Anexos que se encuentra en el **TOMO IV "MANUAL DE SOFTWARE Y HARDWARE"**

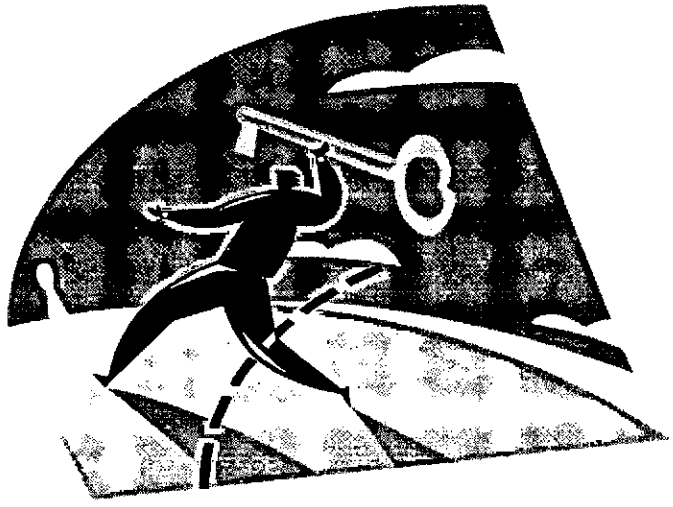
El mismo consta de 2 partes, la primera dedicada a Hardware y la segunda a Software, manteniendo la estructura que se describe en párrafos precedentes. Está orientado específicamente a aquellos usuarios con un mínimo conocimiento de las nuevas tecnologías, incluyendo una breve introducción a Redes, Internet, Intranet, Bases de Datos.

Proyecto:

"POLÍTICAS DE MITIGACIÓN DE RIESGOS"

Objetivo específico:

PREVENCIÓN Y POLÍTICAS DE SEGURIDAD

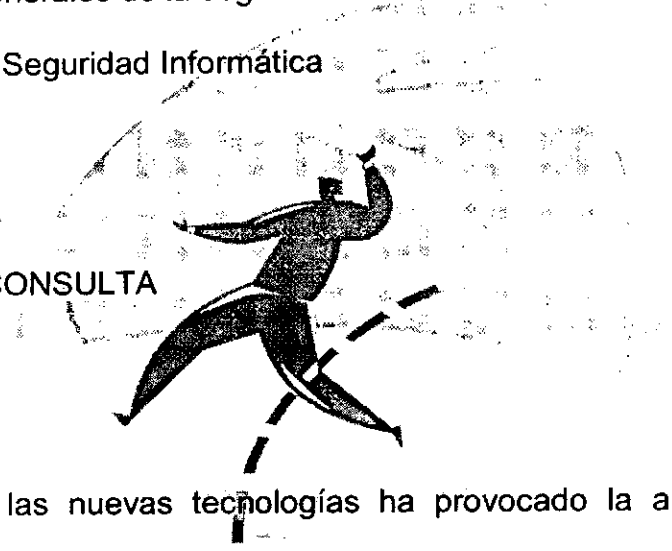


ACTIVIDAD 6

"POLÍTICAS DE SEGURIDAD DE ALCANCE GENERAL"

POLÍTICAS DE SEGURIDAD DE ALCANCE GENERAL

Índice



1. ENUNCIADO

La evolución de las nuevas tecnologías ha provocado la aparición de renovadas necesidades. Los beneficios que son atribuibles a la creación de nuevas tecnologías son muchos, pero también los riesgos se incrementan: la perdida de información, el espionaje, la divulgación de información confidencial, etc.

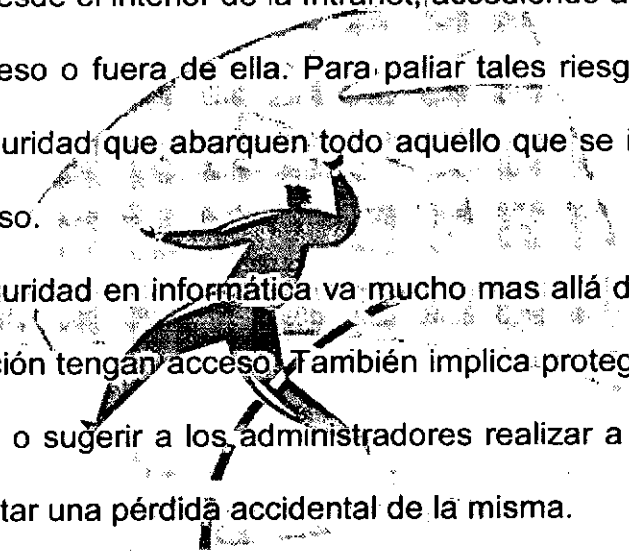
" Las Redes locales se han convertido en un pilar fundamental para el procesamiento de información en la mayoría de las organizaciones, siendo la vía de acceso y uso de Internet en la oficina. La creciente importancia de las LANs demanda la implantación de una adecuada seguridad, que proteja la confidencialidad de los datos y programas y su disponibilidad de uso" Claxion Content Services – Marzo 2001

La seguridad es uno de los aspectos mas conflictivos del uso de las tecnologías de la información. Solo es necesario comprobar como la falta de una política de seguridad global está frenando el desarrollo de Internet en áreas de alto interés y sumamente

prometedoras como el comercio electrónico o la interacción con las Administraciones Públicas.

La ausencia de medidas de seguridad en el ámbito de la informática es un problema al que se enfrentan hoy todas las organizaciones públicas y privadas que han optado por modernizar sus estructuras y procedimientos mediante nuevas tecnologías.

Los atacantes, motivados por un propio desafío o por interés, son una continua amenaza para la integridad de la información. Los ataques pueden suceder de diferentes formas: desde el interior de la Intranet, accediendo a información a la que no se podría tener acceso o fuera de ella. Para paliar tales riesgos, es necesario contar con políticas de seguridad que abarquen todo aquello que se intenta proteger, con un estricto control del uso.



Sin embargo, la seguridad en informática va mucho mas allá de impedir que personas ajenas a la información tengan acceso. También implica proteger a los usuarios contra sus propios errores, o sugerir a los administradores realizar a tiempo el resguardo de información para evitar una pérdida accidental de la misma.

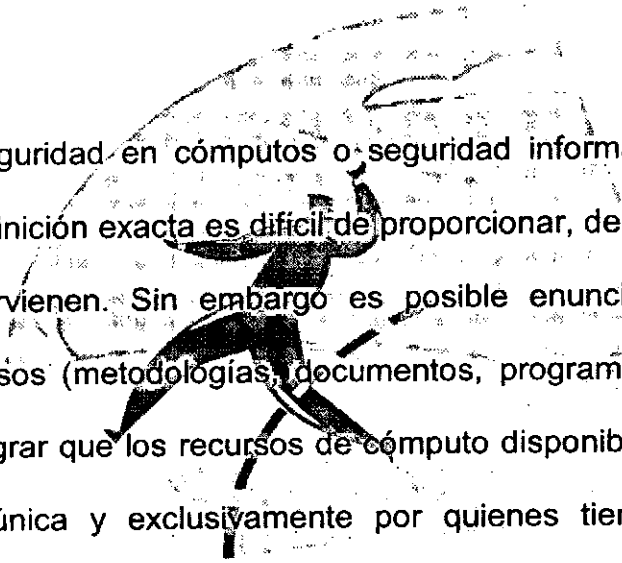
"De acuerdo con los resultados de una encuesta que realizó en este año el Computer Security Institute (CSI) a alrededor de 640 organizaciones de gobierno, privadas y universidades, el 90% reportó fallas en sus sistemas de seguridad (acceso no autorizado); el 70% alteraciones leves, incluyendo la propagación de virus; el 74% pérdidas financieras debido a alteraciones en las computadoras; 42% estuvieron dispuestos y fueron capaces de cuantificar sus pérdidas financieras. El ejemplo anterior es una muestra de la necesidad de contar con esquemas de seguridad para proteger la información; en particular, en las instituciones de la Administración Pública..." Instituto Nacional de Estadística, Geografía e Informática de México (INEGI) - http://www.inegi.gob.mx/informatica/espanol/servicios/boletin/2000/Bpi3-00/seguri.html

2. OBJETIVO

Generación de políticas de seguridad de alcance general, estándares a nivel gerencial, como medidas de resguardo de información en puestos de trabajo, correcta utilización de los recursos de la red, etc.

Las mismas serán las bases para las políticas especificas de cada área técnica como redes, servidores y bases de datos. Con el fin de ser publicadas en la Intranet de gobierno.

3. CUERPO



" ¿Qué es la seguridad en cómputos o seguridad informática? En realidad es un concepto cuya definición exacta es difícil de proporcionar, debido a la gran cantidad de factores que intervienen. Sin embargo es posible enunciar, que Seguridad es el conjunto de recursos (metodologías, documentos, programas y dispositivos físicos) encaminados a lograr que los recursos de cómputo disponibles en un ambiente dado, sean accedidos única y exclusivamente por quienes tienen la autorización para hacerlo." F.A.Q. DE SEG-L (lista de seguridad en castellano)

3.1. Aspectos generales de la seguridad de la información

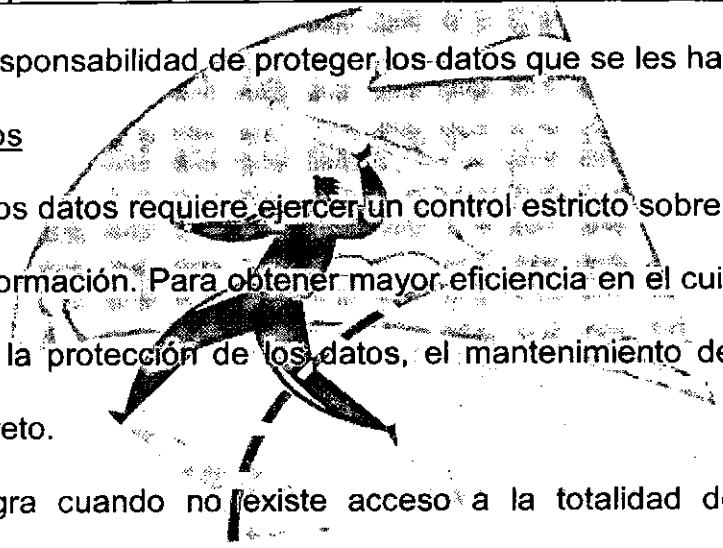
Las medidas de seguridad están basadas en la definición de controles físicos, funciones, procedimientos y programas que conlleven no sólo a la protección de la integridad de los datos, sino también a la seguridad física de los equipos y de los ambientes en que éstos se encuentran.

Con relación a la seguridad misma de la información, estas medidas han de tenerse en cuenta para evitar la pérdida o modificación de los datos, información o software inclusive, por personas no autorizadas, para lo cual se deben tomar en cuenta una

serie de medidas, entre las cuales figurarán el asignar números de identificación y contraseñas a los usuarios.

La seguridad de la información tiene dos aspectos. El primero consiste en negar el acceso a los datos a aquellos usuarios que no tengan derecho a ellos, este consiste en la protección de la privacidad, si se trata de datos personales, y mantenimiento de la seguridad en el caso de datos de la organización.

Un segundo aspecto de la protección es garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso, las cuales tienen la responsabilidad de proteger los datos que se les han confiado.



Protección de datos

La protección de los datos requiere ejercer un control estricto sobre la lectura, escritura y empleo de la información. Para obtener mayor eficiencia en el cuidado se debe tener siempre presente la protección de los datos, el mantenimiento de la privacidad y la seguridad del secreto.

El secreto se logra cuando no existe acceso a la totalidad de los datos sin la jerarquización de acceso a los mismos. La privacidad adecuada se obtiene cuando los datos que puedan obtenerse no pueden enlazarse a individuos específicos o no pueden utilizarse para imputar hechos acerca de ellos.

Sin adecuadas medidas de seguridad se pueden producir los siguientes riesgos:

Accesos no autorizados a:

- *Área de Sistemas*. La libertad de acceso al área de sistemas puede crear un significativo problema de seguridad. El acceso normal debe ser dado solo a la gente que regularmente trabaja en esta área. Cualquier otra persona ajena, puede tener acceso únicamente bajo control. Mantener la seguridad física del área de sistema es la primera línea de defensa. Para ello debe tomar en consideración el valor de sus datos, el costo de protección, el impacto que su

pérdida tiene para la organización y la motivación, competencia y oportunidades de la gente que podría querer dañar los datos o el sistema.

- *PC y/o Terminales de la Intranet*: Las terminales que son dejadas sin protección pueden ser usados erróneamente. Cualquier terminal que puede ser utilizada como acceso a los datos de un Sistema, debe ser encerrada en un área segura o guardada, de tal manera que no sean usados, excepto por aquellos que tengan autorización para ello. Se debe considerar la mejor manera de identificar a los operadores de terminales del Sistema y el uso de contraseñas.
- Información Confidencial: Algunos usuarios o personal no autorizado pueden encontrar alguna forma mediante la cual logran el acceso al sistema o la base de datos y descubrir información clasificada o datos no autorizados.

Además, se deben considerar los siguientes aspectos:

- Deben existir programas protegidos que mantengan y controlen a los usuarios y sus derechos de acceso, ya sea por grupos o individualmente.
- Deben implementarse sistemas de contraseñas antes de entrar a un sistema.
- Los programas de control de acceso deberán identificar a los usuarios autorizados a usar determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidos a la lectura o modificación en sus diferentes formas.

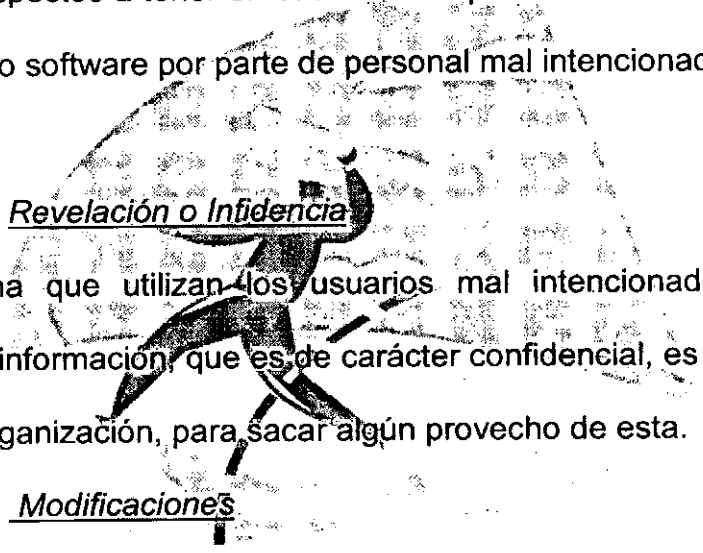
Destrucción

Se puede estar a merced no sólo de la destrucción de la información sino también de la destrucción del equipo informático (hardware), la misma puede darse por una serie de desastres como: incendios, inundaciones, sismos, o posibles fallas eléctricas, etc.

Cuando se pierden los datos y no hay disponibles copias de seguridad, se deben volver a crear los datos o trabajar sin ellos. De hecho, se puede comprobar cómo una gran parte del espacio en disco está ocupado por archivos, que es útil tener a mano pero que no son importantes para el funcionamiento normal.

Para evitar daños mayores cuando la información es destruida, deben realizarse *backups* de la información vital para la organización y almacenarse en lugares adecuadamente preparados para ese fin.

Otro de los aspectos a tener en cuenta en la protección es la posible destrucción del hardware o software por parte de personal mal intencionado.



Revelación o Infidencia

Es otra forma que utilizan los usuarios mal intencionados para su propio beneficio. La información, que es de carácter confidencial, es vendida a personas ajenas a la organización, para sacar algún provecho de esta.

Modificaciones

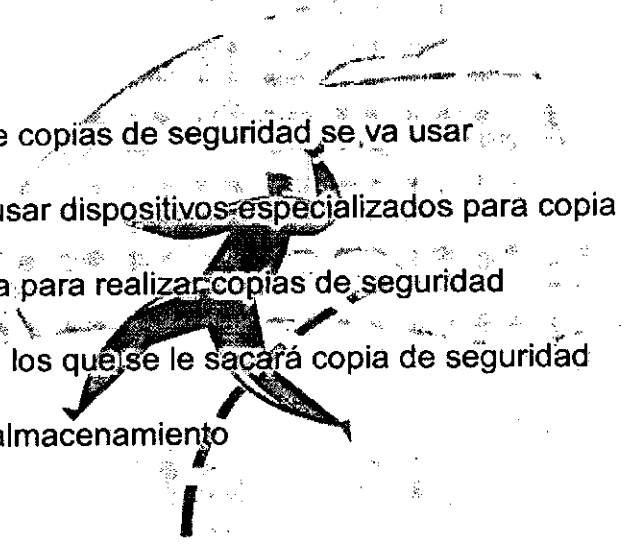
La importancia de los datos que se modifican de forma ilícita, está condicionada al grado en que la organización depende de los datos para su funcionamiento y toma de decisiones. Si fuera posible, esto podría disminuir su efecto si los datos procedentes de las computadoras que forman la base de la toma de decisiones, se verificaran antes de decidir.

Debe ser dada particular atención al daño potencial que pueda efectuar un programador a través de una modificación no autorizada.

La mejor protección contra la pérdida de datos consiste en hacer copias de seguridad, almacenando copias actualizadas de todos los archivos valiosos en un lugar seguro o en varios lugares, especialmente alguna copia fuera del mismo edificio para no correr el riesgo de perder toda la información existente.

Los usuarios deben ser concientizados de la variedad de formas en que los datos pueden perderse o deteriorarse. Una campaña de concientización de este tipo puede iniciarse con una reunión con los usuarios, profundizarse con una serie de seminarios y reforzarse con carteles y circulares relacionados al tema. Este tema de desarrollará en la **Actividad 7** que abarca las pautas generales para la capacitación y la concientización, del Contrato "*Políticas de Mitigación de Riesgos*"

Para la realización de las copias de seguridad es necesario tomar decisiones previas como:



- Soporte de copias de seguridad se va usar
- Se van a usar dispositivos especializados para copia de seguridad
- Frecuencia para realizar copias de seguridad
- Archivos a los que se le sacará copia de seguridad
- Lugar de almacenamiento
- etc.

Un aspecto importante para la seguridad de los datos es la estructura del esquema de clasificación, ya que afectará su implementación. Hay tres formas de clasificar a la seguridad informática:

1) Clasificación por **niveles:**

   Se basa en un esquema de clasificación jerárquica en el que el nivel más bajo es "no clasificado" y el nivel más alto, "secreto o alto secreto". El orden de los niveles implica la importancia relativa de los datos y los requisitos de los procedimientos de seguridad.

   El acceso a los datos se basa en el nivel asignado al usuario y en el nivel de clasificación de los datos; si el nivel del usuario no es igual al nivel de clasificación de los datos, el acceso es desnegado.

2) Clasificación por **categorías**:

   No es jerárquica y se utiliza para grupos independientes de datos y recursos que necesitan procedimientos similares de protección. Las categorías diferentes no tienen ninguna relación ni dependencia entre ellas. Las categorías se asignan tanto a usuarios como a datos; si el usuario no tiene la misma categoría (o categorías) que los datos, el acceso es denegado.

3) La clasificación **combinada**

   Se basa en ambas estructuras. La combinación de niveles jerárquicos y categorías no jerárquicas se representa en una tabla de seguridad. Para realizar la clasificación completa de la información se necesita tanto el nivel como la categoría.

Basándose en esta clasificación, existen distintos criterios de clasificación, que se eligen en basándose en riesgos de los datos y los recursos. Por ejemplo, una clasificación puede hacerse teniéndose en cuenta su sensibilidad a la destrucción, a la modificación o a la difusión de los mismos.

- La sensibilidad a la **destrucción** se refiere al borrado o a no tener disponibles los recursos, datos o programas. Es vital para la supervivencia de la organización que esta información esté convenientemente protegida. Este tipo de sensibilidad afecta a la disponibilidad de la información.
- La sensibilidad a la **modificación** se refiere al cambio de los datos o de los programas. La modificación de los datos o los cambios no detectados es un aspecto a considerar si se manejan datos sensibles. Los cambios no autorizados o no detectados atentan contra una de las principales características de la seguridad de la información: la integridad de los datos y de los programas.
- La sensibilidad a la **difusión** se refiere al conocimiento que se adquiere a través de los datos obtenidos. Esta sensibilidad estará en función del valor de los datos

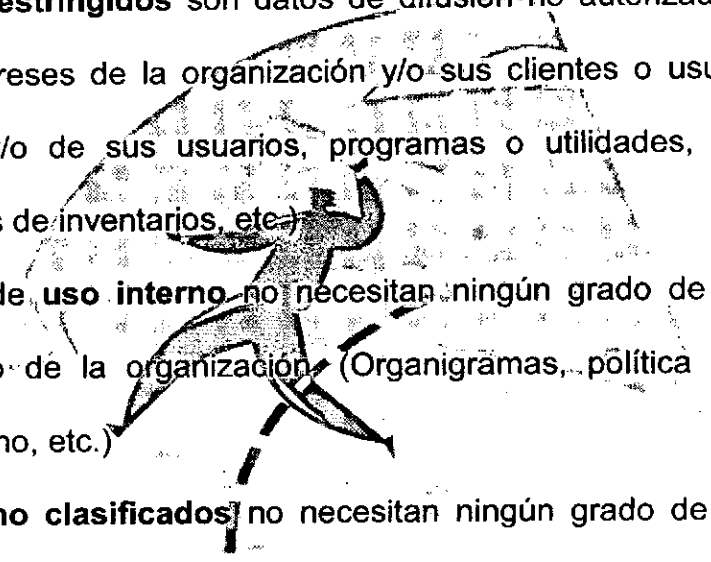
y de los programas y afecta a otra de las características de la seguridad de la información: la confidencialidad.

Como ejemplo, se examina con más detalle, un esquema de clasificación por niveles jerárquicos utilizando como criterio la sensibilidad a la difusión.

Los diferentes niveles son los siguientes:

a) Los datos **confidenciales** son datos de difusión no autorizada. Su uso puede suponer un importante daño a la organización.

b) Los datos **restringidos** son datos de difusión no autorizada. Su utilización irá contra los intereses de la organización y/o sus clientes o usuarios. (Datos de la organización y/o de sus usuarios, programas o utilidades, software, datos de personal, datos de inventarios, etc.)



c) Los datos de **uso interno** no necesitan ningún grado de protección para su difusión dentro de la organización. (Organigramas, política y estándares, listín telefónico interno, etc.)

d) Los datos **no clasificados** no necesitan ningún grado de protección para su difusión. (Informes anuales públicos, etc.)

Para que exista seguridad en la información se deben garantizar los servicios y procedimiento que se describen a continuación

- Confidencialidad

  Es el derecho que poseen individuos y organizaciones para determinar que tipo de información propia puede llegar a ser difundida a terceros y cual no. Si la información privada llega a manos de terceros no autorizados a accederla, se corre el riesgo de que sea difundida rápidamente revelando secretos.

- Integridad

Se refiere a que la información se mantiene tal cual se almacenó, sin sufrir modificaciones ni mucho menos pérdidas. Pensemos que se cambien datos de forma que se pierda información de determinadas deudas a cobrar.

- Disponibilidad

  Es cuando se proveen datos o información a usuarios autorizados en el tiempo previsto, es decir, en el momento que se solicita. Respecto a este punto existen 2 problemas a tener en cuenta:

  - Disponer de la información a tiempo pero que ésta no sea correcta
  - Falta de disponibilidad absoluta, por haberse producido algún desastre.

  En relación con esto último deben existir soluciones alternativas, basadas en medios propios o contratados, copias actualizadas de la información útil y un verdadero Plan de Contingencias que permita restablecer las operaciones en un tiempo inferior o igual al prefijado. Este tema se desarrolla con mayor profundidad en la actividad 3 del contrato "Políticas de Mitigación de Riesgos"

- Autenticación:

  Garantiza que quien dice ser "X" es realmente "X". Es decir, se deben implementar mecanismos para verificar quién está enviando la información..

- No repudio:

  Ni el origen ni el destino en un mensaje deben poder negar la transmisión. Quien envía el mensaje puede probar que, en efecto, el mensaje fue enviado y viceversa.

- Control de accesos:

  Consiste en controlar quién utiliza el sistema o cualquiera de los recursos que ofrece y cómo lo hace.

- Consistencia

Se trata de asegurar que el sistema siempre se comporte de la forma esperada, de tal manera que los usuarios no encuentren variantes inesperadas.

- Auditoria

  Consiste en contar con los mecanismos para poder determinar qué es lo que sucede en el sistema, qué es lo que hace cada uno de los usuarios y los tiempos y fechas de dichas acciones.

En cuanto a los dos últimos puntos resulta de extrema importancia, cuando se trata de los derechos de los usuarios, diferenciar entre "espiar" y "monitorear" a los mismos. La ética es algo que todo buen administrador debe conocer y poseer.

Todos estos servicios de seguridad deben ser tomados en cuenta en el momento de elaborar las políticas y procedimientos de una organización para evitar pasar por alto cuestiones importantes como las que señalan dichos servicios. De esta manera, es posible sentar de forma concreta y clara los derechos y límites de usuarios y administradores. Sin embargo antes de realizar cualquier acción para garantizar estos servicios, es necesario asegurarse de que los usuarios conozcan sus derechos y obligaciones (es decir, las políticas y estándares), de tal forma que no se sientan agredidos por los procedimientos organizacionales.

Asimismo, la seguridad de la información se puede dividir en los siguientes tipos:

- Seguridad física

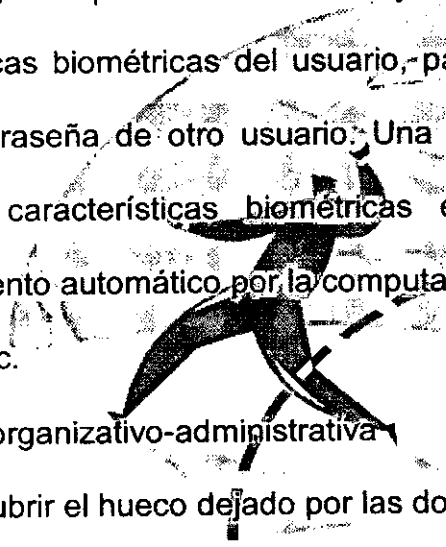
  Como la ubicación de los centros de procesos, las protecciones físicas, el control físico de accesos, las medidas contra el fuego y el agua, y otras similares. ¿Quién tiene acceso a los sistemas? ¿Qué tan confiable es la alimentación eléctrica?. Tiene que haber declaradas políticas de seguridad que:

  - Condicionen el acceso a personas no autorizadas a lugares donde existan componentes vitales para el funcionamiento de los sistemas

- Hablen de la necesidad de contar con UPS en los servidores para el mantenimiento por un tiempo determinado de la energía en caso de perderla

- Seguridad lógica,

  Como el control de accesos a la información exigiendo la identificación y autenticación del usuario, o el cifrado de soportes magnéticos intercambiados entre entidades La **autenticación** suele ser mediante contraseña, si bien sería más lógico, aunque con costos muy altos, que se pudiera combinar con características biométricas del usuario, para impedir la que se pueda ingresar con la contraseña de otro usuario. Una forma de identificar a los usuarios a través de características biométricas es la realización de la firma con reconocimiento automático por la computadora, análisis del fondo de ojo, huellas digitales, etc.



- Seguridad organizativo-administrativa

  Pretende cubrir el hueco dejado por las dos anteriores y la complementa.

  Difícilmente se puede lograr de forma eficaz la seguridad de la información si no existen claramente definidas:

  - Políticas de seguridad
  - Políticas de personal
  - Políticas de contratación
  - Análisis de riesgos
  - Planes de Contingencia.

- Seguridad jurídica

  Pretende, a través de la aprobación de normas legales, fijar el marco jurídico necesario para proteger los bienes informáticos.

3.1.1. Riesgos

Al margen de la seguridad, el mayor riesgo, aun teniendo un entorno muy seguro, es que no se cubran las necesidades de seguridad de la organización

Sobre la seguridad propiamente dicha, los riesgos pueden ser múltiples: el primer paso es conocerlos, y el segundo es tomar decisiones al respecto; conocerlos y no tomar decisiones no tiene sentido y crea una situación de desasosiego e incertidumbre.

Como todas las medidas tienen un costo, se debe analizar cuál es el riesgo máximo que podría soportar la organización, si bien la respuesta no es fácil, porque depende de la criticidad del sector y de la entidad misma, de su dependencia respecto a la información, y del impacto que su falta de disponibilidad pudiera tener en la entidad.

Al analizar el impacto, nunca deberá aceptarse un riesgo que pueda llegar a poner en peligro la propia continuidad de la organización.

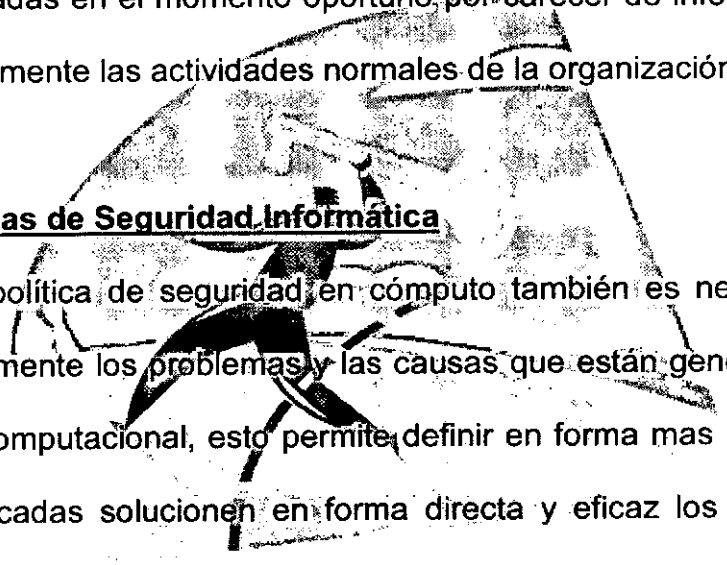
Existen daños de menores consecuencias, siendo los errores y omisiones la causa más frecuente, normalmente de poco impacto pero de frecuencia muy alta, y otras el acceso indebido a los datos (a veces a través de redes), la cesión no autorizada de soportes magnéticos con información crítica (denominado como "sensible"), los daños por fuego, agua (del exterior como puede ser una inundación, o una tubería interior), variación no autorizada de programas, copia indebida, y tantos otros, persiguiendo el propio beneficio o el causar un daño, a veces por venganza.

Otra amenaza es la del *hacker*, que intenta acceder a los sistemas para demostrar (sobre todo para demostrarse a sí mismo) de qué es capaz de ingresar al sistema, así como para demostrar que puede superar las barreras de protección que le hayan establecido. Otras veces, el objetivo del hacker es el de obtener información privada de la organización, para difundirla o venderla.

En definitiva, las amenazas impactan en los datos, en los usuarios, en programas, en equipos, en la red... y en muchos casos, en varios o en todos ellos, como el caso de un siniestro.

La pregunta crítica es: **¿Cuál es la información crítica a proteger?**

Del punto de vista de la continuidad de la organización, sin dudas los datos son los mas críticos. Como consecuencia de cualquier incidencia, se pueden producir pérdidas, que pueden ser no sólo **directas**, sino también **indirectas,** como no poder tomar las decisiones adecuadas en el momento oportuno por carecer de información o paralizar completa o parcialmente las actividades normales de la organización.



3.2. Políticas de Seguridad Informática

"Para crear una política de seguridad en cómputo también es necesario determinar cuales son actualmente los problemas y las causas que están generando deficiencias en el desarrollo computacional, esto permite definir en forma mas real y estándar, las medidas que aplicadas solucionen en forma directa y eficaz los problemas que en seguridad se desean resolver" Políticas de Seguridad en Cómputo del INAOE.

¿Que son las políticas de seguridad informática (PSI)?

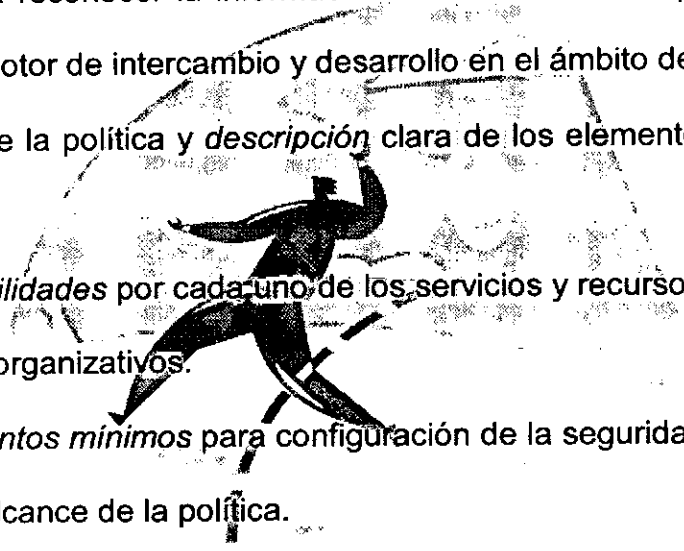
No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los usuarios. Es más bien una descripción de los que se debe proteger y el por qué de ello.

Cada PSI debe ser consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la organización. Es una forma de comunicarse con los usuarios y los gerentes. Establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización.

Una PSI debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere de una disposición por parte de cada uno de los miembros de la organización para lograr una visión conjunta e integral de lo que se considera importante.

Se deben considerar entre otros, los siguientes elementos:

- *Alcance* de las políticas: se deben incluir facilidades, sistemas y personal sobre la cual se aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus funciones.
- *Objetivos* de la política y *descripción* clara de los elementos involucrados en su definición.
- *Responsabilidades* por cada uno de los servicios y recursos informáticos a todos los niveles organizativos.
- *Requerimientos mínimos* para configuración de la seguridad de los sistemas que incluye el alcance de la política.
- *Definición de violaciones* y de las consecuencias de la falta de cumplimiento de la política.
- *Responsabilidades* de los usuarios con respecto a la información a la que tienen acceso.

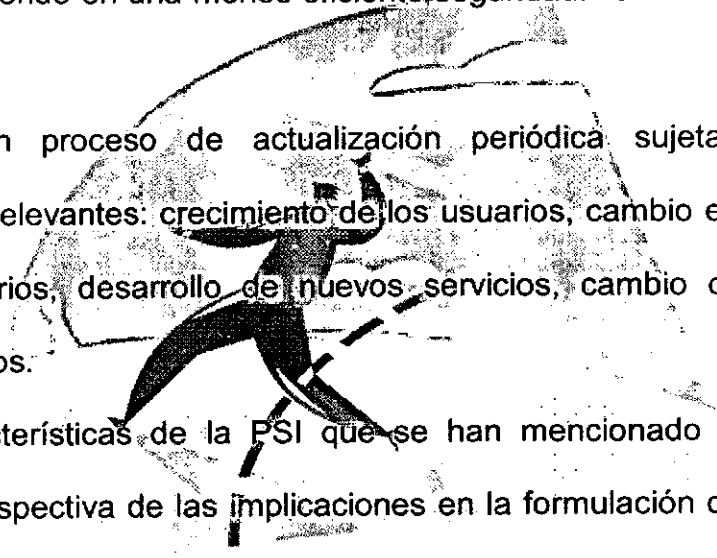


Las PSI deben ofrecer explicaciones comprensibles acerca de por qué deben tomarse ciertas decisiones, transmitir por qué son importantes estos u otros recursos o servicios.

Establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan en la organización. Deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad.

La política debe especificar las autoridades de aplicación y control que deben hacer que las mismas se empleen, el rango de los correctivos y actuaciones que permitan dar indicaciones sobre la clase de sanciones que se deban imponer. No debe especificar con exactitud qué pasara o cuándo algo sucederá.

"Las políticas tienen que ser funcionales, encajando con los requisitos y forma de funcionar de los diferentes empleados y departamentos. Si no contemplan y respetan las dinámicas de trabajo, impedirán la correcta actividad laboral y no se cumplirán las políticas, repercutiendo en una menos eficiente seguridad." Claxion Content Services – Marzo 2001



Deben seguir un proceso de actualización periódica sujetas a los cambios organizacionales relevantes: crecimiento de los usuarios, cambio en la infraestructura, rotación de usuarios, desarrollo de nuevos servicios, cambio o diversificación de servicios entre otros.

Si bien las características de la PSI que se han mencionado hasta el momento, muestran una perspectiva de las implicaciones en la formulación de estas normas, se deben realizar, algunos aspectos generales recomendados para la formulación de las mismas.

- Efectuar un ejercicio de análisis de riesgos informáticos, a través del cual valoren los activos de la organización, el cual le permitirá afinar las PSI de la organización.
- Involucrar a las áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a la PSI.
- Comunicar a todo el personal involucrado en el desarrollo de las PSI, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.

- Identificar quién tiene la autoridad para tomar decisiones, pues son ellos los responsables de resguardar la información confidencial.
- Desarrollar un proceso de monitoreo periódico de las normas en el hacer de la organización, que permita una actualización oportuna de las mismas.
- No dé por hecho algo que es obvio. Hacer explícitos y concretos los alcances y propuestas de seguridad, con el propósito de evitar sorpresas y malos entendidos en el momento de establecer los mecanismos de seguridad que respondan a las PSI trazadas.

Para llevar a cabo un sistema de seguridad informática, se debe establecer la forma de realizar el análisis. En el gráfico que se incorpora a continuación (tomado del Manual de Seguridad del ACERT – Gobierno Nacional) se pueden observar todos los elementos que intervienen para el estudio de una política de seguridad y un análisis de cada uno de ellos y su interacción.

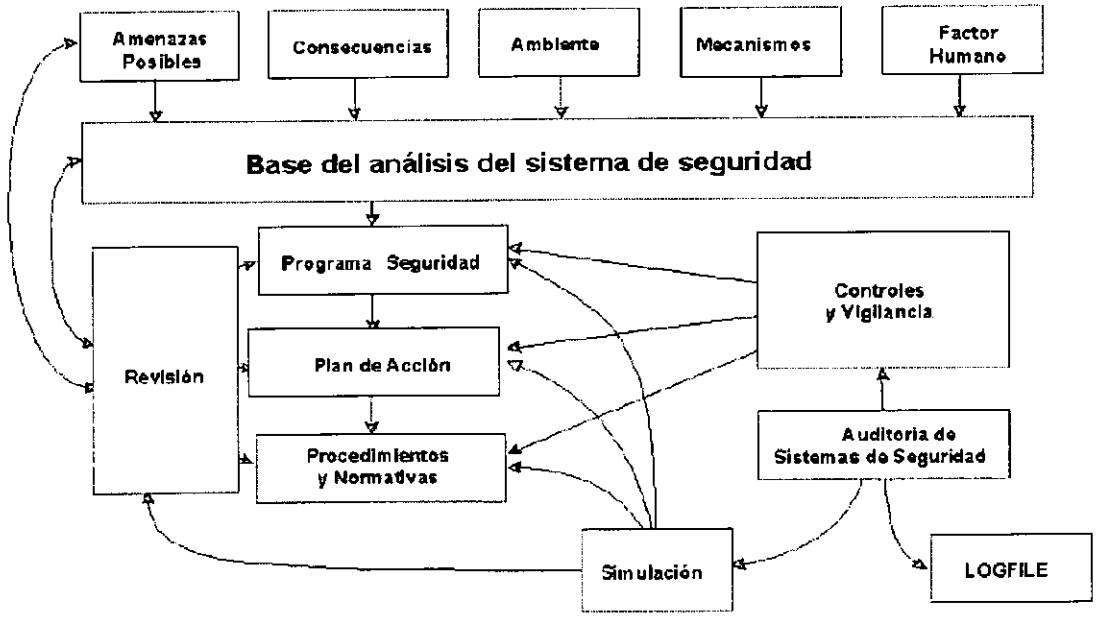
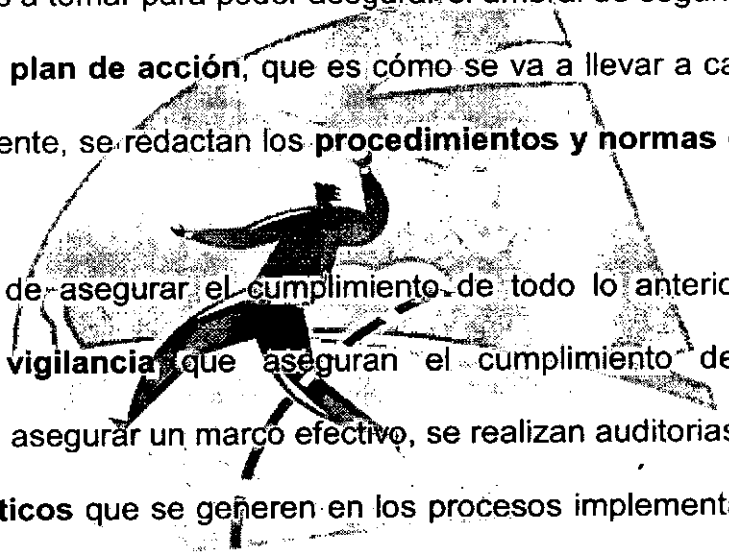


Gráfico 1

Se comienza realizando una evaluación del **factor humano** interviniente, como los usuarios, técnicos, etc. **Mecanismos** con que se cuentan para llevar a cabo los procesos necesarios (mecanismos técnicos, físicos ó lógicos), el **medio ambiente** en que se desempeña el sistema o los sistemas, las **consecuencias** que puede traer aparejado defectos en la seguridad (pérdidas físicas, pérdidas económicas, en la imagen de la organización, etc.), y cuáles son las **amenazas posibles**.

Una vez evaluado todo lo anterior, se origina un **programa de seguridad,** que involucra los pasos a tomar para poder asegurar el umbral de seguridad que se desea.

Luego, se pasa al **plan de acción**, que es cómo se va a llevar a cabo el programa de seguridad. Finalmente, se redactan los **procedimientos y normas** que permiten llegar a buen término.



Con el propósito de asegurar el cumplimiento de todo lo anterior, se **realizan los controles y la vigilancia** que aseguran el cumplimiento de los tres puntos antepuestos. Para asegurar un marco efectivo, se realizan auditorias a los controles y a los archivos **logísticos** que se generen en los procesos implementados (de nada vale tener archivos logísticos si nunca se los analizan o se los analizan cuando ya ha ocurrido un problema).

Con el objeto de confirmar el buen funcionamiento de lo creado, se procede a **simular** eventos que atenten contra la seguridad del sistema. Como el proceso de seguridad es un proceso dinámico, es necesario realizar **revisiones** al programa de seguridad, al plan de acción y a los procedimientos y normas. Estas revisiones, tendrán efecto sobre los puntos tratados en el primer párrafo y, de esta manera, el proceso se vuelve a repetir.

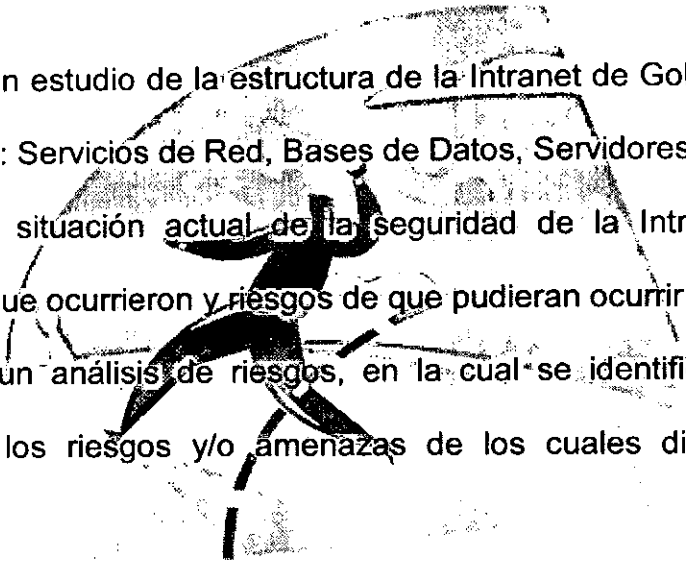
Aspectos a considerar en la seguridad de la Intranet

Los objetivos de la elaboración de las políticas de seguridad en la Intranet de Gobierno de la Provincia de San Luis son:

1 - Como medida correctiva en solución a los problemas de seguridad en cómputo que han ocurrido y de los que actualmente son motivo potencial de incidentes de seguridad.

2 - Como medida preventiva de nuevos ataques que si bien no han ocurrido se desean evitar hasta el mayor grado posible.

Para la elaboración de las políticas de seguridad es importante tratar distintos aspectos, para el cual se describen en forma global las principales partes consideradas:



1. Se realizó un estudio de la estructura de la Intranet de Gobierno de la Provincia de San Luis: Servicios de Red, Bases de Datos, Servidores e Internet
2. Se trató la situación actual de la seguridad de la Intranet, los problemas, incidentes que ocurrieron y riesgos de que pudieran ocurrir estos incidentes
3. Se realizó un análisis de riesgos, en la cual se identificaron los recursos a proteger y los riesgos y/o amenazas de los cuales dichos recursos serán protegidos.
4. Se procedió a la definición de políticas de seguridad

Hasta aquí el tema de las políticas es muy claro pero sirven de muy poco solo en un papel. La parte más difícil de la implementación de un conjunto de políticas es convencer a los usuarios de seguirlas. Por esto es imprescindible, al crear políticas, tener en cuenta el factor humano y buscar una figura que represente autoridad dentro de la organización y que sean quienes las presenten a los usuarios. Es por esto que la SETI ha estado trabajando en la figura del referente informático (Ver Anexo III), quien será el nexo entre la Secretaría y los usuarios finales.

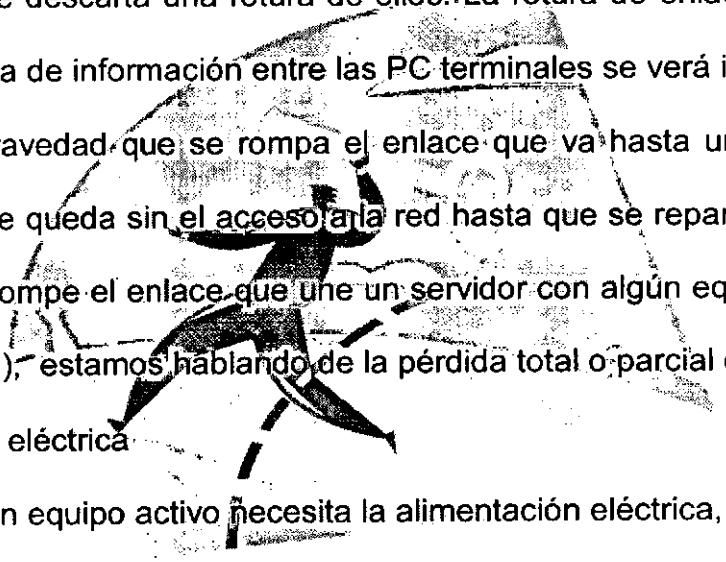
3.2.1. ***Análisis de Riesgos:***

Se analizan de forma general, los problemas y consideraciones que afectan directa o indirectamente a la seguridad y basándose en ellos se generan las políticas de alcance general a implementar en la Intranet de Gobierno de la Provincia de San Luis.

Redes

- Enlaces a la vista

  Dado que inevitablemente existen enlaces entre PC's a la vista y alcance de la gente, no se descarta una rotura de ellos. La rotura de enlaces significa que la transferencia de información entre las PC terminales se verá interrumpida. No es de suma gravedad que se rompa el enlace que va hasta una PC terminal, en este caso se queda sin el acceso a la red hasta que se repare el inconveniente. Pero si se rompe el enlace que une un servidor con algún equipo activo (switch, router, HUB), estamos hablando de la pérdida total o parcial de la red.



- Sobrecarga eléctrica

  Dado que un equipo activo necesita la alimentación eléctrica, una suspensión de esta alimentación hace que el sector que cubre el equipo activo, se incomunique con el resto de la red. Un disparo en la protección térmica puede ser consecuencia de una sobrecarga de energía o un cortocircuito. Este riesgo hace el disparo de la llave térmica que alimenta algún equipo activo, pierda la energía y por consecuencia la incapacidad de distribuir los servicios de red. Una de las causas puede ser la mala utilización de los enchufes que están disponibles en las cajas de conexión para el exclusivo uso de las computadoras.

- Fallo en Caja de Conexión o en Patch Cord

  Las cajas de conexión o también llamados 'periscopios', son los que conectan las terminales en la red. Al estar sobre la superficie de la oficina, están expuestas a todo tipo de deterioro o accidente. Si se sufre algún tipo de rotura o

daño en la caja de conexión, la terminal quedará temporalmente aislada del resto de la red hasta que se le dé una solución.

Una falla en el Patch Cord (nombre técnico que lleva el cable que conecta a una terminal de red con una caja de conexión o 'periscopio') tendría el mismo efecto que la falla anterior.

- Caída de red

  La falta de suministro del servicio de red puede darse por varios motivos:

  - Que se pierda la configuración de red por causas físicas, por error o por mala acción humana. Al perderse la configuración de la red, se paraliza parcialmente o totalmente la conectividad.
  - Que se pierda la conexión a un servidor de red, esto paraliza totalmente el uso de los recursos de la red.

  La pérdida del servicio de red es de vital importancia, dado que existen diversas aplicaciones que necesitan este suministro para poder trabajar, como por ejemplo el Sistema Contable, el Sistema de Expedientes, etc.

- Perdida de la configuración de la red

  El objetivo de cualquier configuración es almacenar las distintas opciones necesarias para la correcta administración o utilización de un software o un recurso. En este caso, la pérdida de la configuración de la red produce que se pierda el servicio de las misma inhabilitándola hasta que se configure nuevamente. Ante este riesgo se tienen que tener copias de seguridad sobre la configuración que se está usando actualmente o que se hayan usado antes.

<u>Bases de datos</u>

- Caída de la Base de Datos

  El problema ocasionado por la caída de una base de datos está relacionado con la disponibilidad de la información almacenada. Al dejar de funcionar el motor de

la base de datos se inutilizan todas las aplicaciones que trabajan con esa base debido a que no tienen información para procesar.

- Revelación de contraseñas

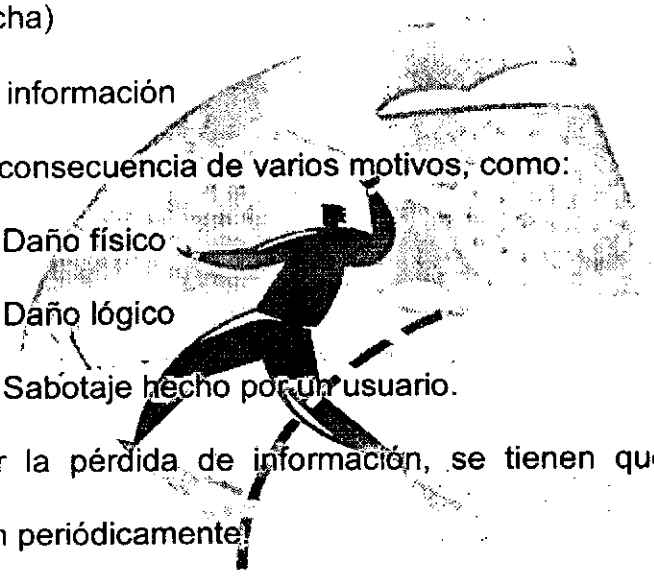
  Provoca un acceso a datos vitales en un sistema. Algún usuario mal intencionado que adquiera esa información puede divulgarla o destruirla (por ejemplo, si se pierde la información de un sistema contable, tendría las consecuencias de que se pierde rastro y control de imputaciones realizadas hasta la fecha)

- Pérdida de información

  Puede ser consecuencia de varios motivos, como:

  - Daño físico
  - Daño lógico
  - Sabotaje hecho por un usuario.

  Para evitar la pérdida de información, se tienen que realizar resguardo de información periódicamente.



Servidores

- Revelación o pérdida de contraseñas del servidor

  La divulgación de una contraseña de un servidor, indica que la persona que la sepa puede llegar a acceder al mismo y ocasionar daños irreparables (y mas si es la que posee todos los privilegios), ya que está operando directamente sobre el Servidor, aunque físicamente no esté en el. Por eso no basta con restringir el acceso a personas no autorizadas al área de servidores, sino también evitar la divulgación de contraseñas del servidor

- No configurar los niveles de seguridad de un nuevo servidor

La seguridad del servidor es algo fundamental. Con la configuración básica no son totalmente seguros, se requiere hilar mas fino este aspecto para minimizar la vulnerabilidad de los sistemas.

Por ello, es imprescindible implementar una buena seguridad en cualquier servidor, de lo contrario, puede convertirnos rápidamente en víctimas de todo tipo de ataques y amenazas.

- Ataque de un hacker

  Es, sin dudas, uno de los más importantes y con consecuencias menos deseadas, dado que un hacker al entrar, dependiendo de sus intenciones, puede llegar a causar desde modificaciones de la información hasta obtenerla para proveerla a otras organizaciones. Otros solo a limitarse a lograr entrar como desafío propio, pero sin realizar daño en la información. Otra consecuencia es que deja la 'puerta abierta' para el ingreso de otros, ya sea divulgando todos los pasos a seguir para ingresar o colocando pequeños programas que se ejecutan en PC's dentro de la red, enviándole periódicamente al hacker la información que este haya configurado en el programa que instaló.

- Caída del Servidor

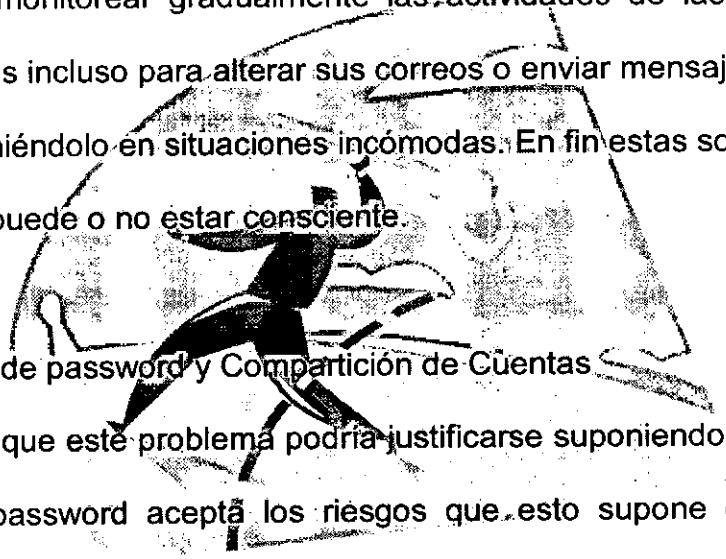
  La caída de un servidor rara vez ocurre. Una de las causas puede ser la falta de corriente eléctrica que lo alimenta, para lo cual se deben instalar UPS que los mantengan funcionando por un tiempo necesario en caso de ocurrir un corte de energía. El tiempo que alimentan de energía al servidor debe permitir el cierre de las aplicaciones que se están ejecutando en el.

Internet

- Mala utilización de servicios de Internet

  Cada vez que se utiliza el correo electrónico, navega por Internet, o hace uso de un servidor FTP, se están revelando datos personales no deseados que pueden

ser recolectados y utilizados por terceros en perjuicios del usuario inocente. Por ejemplo, cada vez que un usuario visita un sitio Web, se suministra de forma rutinaria información que puede ser archivada por cualquier persona o por un hacker. A este no le resulta difícil averiguar la dirección Internet de la máquina que se está operando y su sistema operativo, la dirección del correo electrónico del usuario, qué páginas lee y cuales no, que temas le interesan, cuantas páginas ha visitado, entre otros. Toda esta información sirve finalmente para conocer y monitorear gradualmente las actividades de las víctimas y utilizar dichas pistas incluso para alterar sus correos o enviar mensajes a terceros en su nombre poniéndolo en situaciones incómodas. En fin estas son las amenazas de las que se puede o no estar consciente.



Usuarios

- Revelación de password y Compartición de Cuentas

  A pesar de que este problema podría justificarse suponiendo que el usuario que revela su password aceptá los riesgos que esto supone como deserciones, vengativas o disgustos por la otra parte que pueden materializarse en el daño o revelación de la información, puede acarrear serios problemas hasta de carácter amistoso. Si el password es revelado a una persona externa, o incluso interna, y esta tiene intereses secundarios, una vez obtenido el acceso a una puerta del sistema (cuenta), se tiene mayor posibilidad de obtener otros privilegios que pueden comprometer la información de terceros, el sistema mismo, o servir de puente para un hacker.

- Ataque de Virus

  El ataque de un virus a una PC no solo puede borrar o duplicar información, sino que hasta puede provocar daños físicos en el equipo. La implementación de

sistemas antivirus en las PC's es una medida básica para prevenir daños físicos o daños en la información almacenada en los discos rígido o disquetes.

A los antivirus, es necesario actualizarlos periódicamente debido a que surgen nuevos y distintos virus a diario. Los fabricantes de antivirus, poseen páginas Web que contienen software que actualizan el antivirus que esta instalado en la PC para detectar los nuevos virus existentes.

- Mantenimiento preventivo y correctivo de los recursos de la PC

  Para efectos de mantener la seguridad física por amenazas naturales como el polvo, deterioro, vejez, etc., los referentes informáticos deben planear y organizar al personal necesario para el mantenimiento periódico preventivo y correctivo de los recursos de la computadora.

- Perdida de información

  Como medida de prevención indispensable en caso de desastre o daños a los discos duros, se deben hacer respaldos de la información de todos los datos, quedando estos en un sitio seguro.

  La determinación de los periodos de respaldo de la información estará a cargo del referente informático y en base al movimiento y naturaleza de la información almacenada en las PC a su cargo.

- Robo

  Como el robo depende mas de la habilidad de la persona que lo realiza o de la falta de protección, es algo impredecible que puede provocar altísimos daños en el caso de realizarse. Ante este riesgo, es de suma importancia la prevención. Se deberán controlar los accesos a áreas restringidas y cantidad de PC's disponibles.

3.2.2. Desarrollo de Políticas de seguridad

A) REDES

- A.1 - El cableado entre las cajas de conexión y las Pc terminales, tiene que cumplir con las normas internacionales I.S.O. / E.I.A. / T.I.A.
- A.2 - Los usuarios deben utilizar la alimentación eléctrica de las cajas de conexión para uso exclusivo de las PC'a.
- A.3 - La configuración de los sistemas debe ser estándar y revisada cada 6 meses por personal de área
- A.4 – Se deben realizar copias de seguridad de la configuración de la red.

B) BASES DE DATOS

- B.1 – La gerencia debe destinar a una persona para la administración de contraseñas y mantener documentación actualizada.
- B.2 – Se deben realizar copias de seguridad en un período definido por el administrador de las bases de datos.
- B.3 – Las copias de seguridad se deben resguardar en un edificio distinto al que se encuentran ubicados los servidores

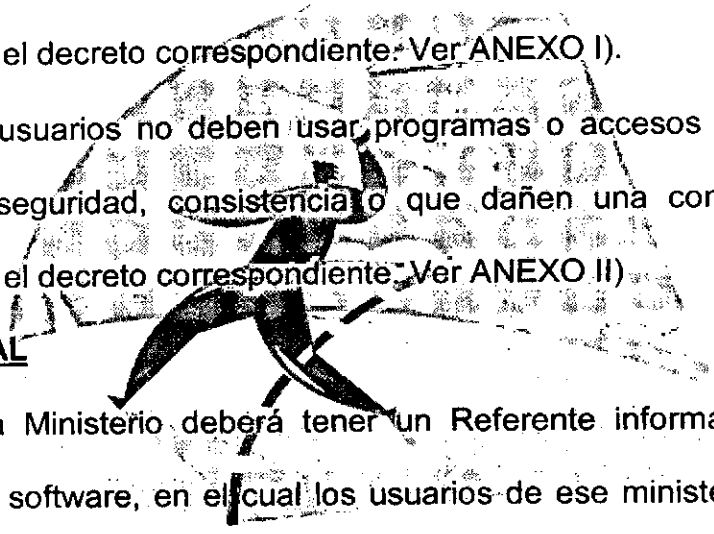
C) SERVIDORES

- C.1 – El encargado de administrar los servidores, debe administrar las cuentas de usuario de la red, definiendo privilegios, tiempo de uso, limite de espacio para almacenar información
- C.2 - La gerencia debe destinar a una persona la administración de los servidores, quien será poseedor de la clave de mas alto privilegio y el encargado de decidir que y a quien se le da cuentas de acceso al servidor.
- C.3 - Se debe instalar y configurar un cortafuego o Firewall a la entrada externa a la red

- C.4 - Los servidores se deben Instalar en una sala especialmente refrigerada y con acceso restringido para el correcto funcionamiento
- C.5 – Los servidores tienen que contar con UPS's que provean de energía por un tiempo necesario para el correcto cierre de las aplicaciones en caso de un corte de energía general

D) INTERNET

- D.1 – Los usuarios no pueden utilizar las facilidades del correo electrónico para envío ni recepción de material molesto, obsceno, ilegal o innecesario (se está redactando el decreto correspondiente. Ver ANEXO I).
- D.2 – Los usuarios no deben usar programas o accesos no autorizados que alteren la seguridad, consistencia o que dañen una computadora (se está redactando el decreto correspondiente. Ver ANEXO II)



E) USUARIO FINAL

- E.1 - Cada Ministerio deberá tener un Referente informático capacitado en hardware y software, en el cual los usuarios de ese ministerio consultarán sus dudas o problemas. El referente informático es quien será capacitado y encargado de transmitir los conocimientos a todos los usuarios de ese Ministerio
- E.2 - El Referente informático deberá tener una lista con todas las claves de las computadoras pertenecientes a su ministerio y será el quien se encargue de controlar el acceso
- E.3 - El referente informático tendrá a cargo la administración de las cuentas de los usuarios en las computadoras de su ministerio y será el responsable de la instalación de software
- E.4 - Los usuarios tendrán acceso a la computadora a través de una cuenta Usuario

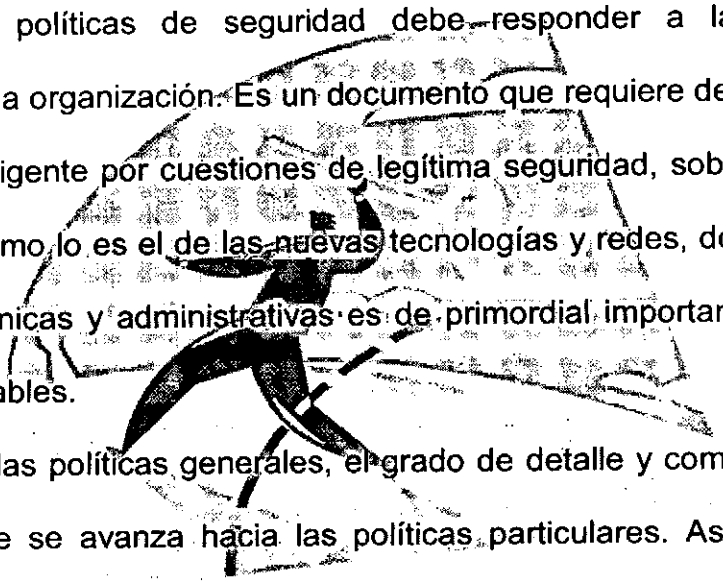
- E.5 - El usuario no podrá compartir recursos en la red sin el consentimiento del referente informático, quien conoce las consecuencias del problema.
- E.6 - El referente informático tendrá que tomar decisiones acerca de la instalación de software antivirus en las computadoras para evitar la infección de los datos por parte de un virus informático.
- E.7 - El referente informático será el responsable de que todo software instalado en alguna computadora contenga su respectiva licencia original.
- E.8 - En cada computadora terminal tiene que realizarse copias de seguridad llevadas a cabo por el referente informático o por el mismo usuario
- E.9 - Los usuarios no autorizados no pueden tener acceso remoto a servidores
- E.10 - Por ningún motivo está permitido resetear, desconectar periféricos o provocar interrupciones eléctricas en cualquier computadora o en la red.
- E.11 - El referente informático deberá llevar una planilla donde estén asentadas todas las computadoras, ubicación y características de la misma.
- E.12 - La gerencia deberá controlar el acceso a lugares restringidos, llenando una planilla donde se registre el día, hora de entrada, hora de salida, motivo de ingreso y nombre de la persona que ingresa
- E.13 - Cada repartición deberá contar con matafuegos en lugares estratégicos para el uso en caso de provocarse un incendio
- E.14 - Personal del proyecto "Administración del parque Informático" realizará auditorias en las áreas para comprobar Hardware y Software de la computadora

4. CONCLUSIÓN

Como se deduce después de este análisis, debido a que existen varios tipos de riesgos, tener una Intranet 100% segura es imposible, y mas aún sin contar la gran cantidad riesgos que van o pueden surgir. Tener una Intranet invulnerable causaría

mas dolores de cabeza que facilidades en la ejecución de herramientas. Solo analizando los propios requerimiento específicos y características propias, se puede ayudar a definir una eficiente estrategia de seguridad sin que se interrumpan las actividades de los usuarios, que es uno de los objetivos de la creación de la Intranet. Por eso, es indispensable que se tomen medidas preventivas para disminuir el máximo posible de los riesgos, declarando políticas de seguridad que abarquen los aspectos generales y mas orientadas al usuario final.

En definitiva las políticas de seguridad debe responder a las necesidades y características de la organización. Es un documento que requiere de constante revisión para mantenerlo vigente por cuestiones de legítima seguridad, sobre todo en ámbitos tan cambiantes como lo es el de las nuevas tecnologías y redes, donde la vigencia de las soluciones técnicas y administrativas es de primordial importancia para mantener los sistemas confiables.



Así, partiendo de las políticas generales, el grado de detalle y complejidad requeridos aumenta conforme se avanza hacia las políticas particulares. Asimismo, entre más detallada y compleja es una política, se requiere actualizarla con mayor frecuencia, y es más complicado el proceso de su implementación.

Teniendo como idea principal y punto de partida que el objetivo básico y fundamental de las políticas de seguridad es reducir el impacto de los riesgos a que se encuentra expuesta la información que se maneja en la Organización debido a su conexión a Internet, principalmente, y demás puntos de riesgo que se han analizado, para lo cual se deben implementar sin demora todos los procedimientos técnicos y administrativos necesarios que permitan asegurar el manejo responsable y ético de dicha información.

Como conclusión se puede tener en cuenta las dos cuestiones fundamentales para implementar con éxito una política de seguridad: es necesario que las mismas sean aprobadas por la autoridad correspondiente para que se asegure su cumplimiento y la

asignación de recursos necesarios. Y es necesario que se realicen revisiones periódicas que las mantengan siempre actualizadas y acorde con la situación real del entorno. Esto asegurará la adecuación del nivel de seguridad a las necesidades de la organización y el correcto seguimiento y control de riesgos.

5. BIBLIOGRAFÍA

- Monografías.com – Sitio de monografías temáticas. Información publicada en www.monografias.com - Las consultadas fueron las siguientes:
  - ✓ Seguridad en una Intranet - Trabajo realizado y enviado por: Carlos A Morales Ochoa. - cmorales@serpaprosa.com.mx - Licenciado en Informática – UNAM
  - ✓ Seguridad Informática – Tema Hackers - Trabajo realizado por: MERLAT, Máximo – (merlatm@ciudad.com.ar) - Estudiante 5to. Año Ing. en Sistemas - PAZ, Gonzalo – (gonzalop@fbelgrano.com.ar) - Estudiante 5to. Año Ing. en Sistemas - SOSA, Matias – (invitroblues@yahoo.com) - Estudiante 5to. Año Ing. en Sistemas - MARTINEZ, Marcelo – Estudiante 5to. Año Ing. en Sistemas
  - ✓ Firewalls y Seguridad en Internet - Autor: Daniel Ramón Elorreaga Madrigal - Ingeniero Electronico - Universidad Nacional Autonoma de México - E-mail: dan_dds@yahoo.com
- Universidad Nacional Autónoma de México (UNAM) – En su Dependencia de la Dirección General de Servicios de Cómputos – Información publicada en www.asc.unam.mx/
- Universidad de Granada - Trabajo SIE - Seguridad en Internet – Información publicada en : www.geocities.com/CapeCanaveral/2566/seguri/seguri.html

- Lafacu.com – Sitio de trabajos ordenados temáticamente – Información publicada en: www.lafacu.com
  - ✓ La información como activo estratégico – Trabajo realizado por Emilio del Peso Navarro - Licenciado en Derecho e Informático y Miguel A. Ramos - Doctor en Informática, CISA Profesor de la Universidad Carlos III de Madrid
  - ✓ Evaluación de seguridad de un sistema de información – Trabajo realizado por: Elaborado por José Alfredo Jiménez – E-mail : alfredo_jimenez@megalink.com
- A.R.C.E.R.T. – Coordinación de Emergencias en Redes Teleinformáticas – Administración Pública Nacional – Manual de Seguridad en Redes publicado en www.arcert.gov.ar
- I.N.A.O.E. Instituto Nacional de Astrofísica, Óptica y Electrónica de México - Políticas de Seguridad en Cómputos – Información publicada en: http://www.inaoep.mx/~moises/S.O./politica.html
- Claxion – IT Security Specialist – Información publicada en su sitio www.claxion.com
- SEG-LFAQ - Universidad Jaume I. de España -Departamento de Lenguajes y Sistemas Informáticos – Información publicada en http://moon.inf.uji.es/~inigo/seg-lfaq.html
- Instituto Nacional de Estadística, Geografía e Informática de México (INEGI) – Información publicada en: www.inegi.gob.mx

6. GRUPOS DE CONSULTA

Toda la tarea investigativa de esta actividad se ha realizado con la colaboración de otras áreas y grupos de la S.E.T.I., por lo tanto, se mencionan a continuación:

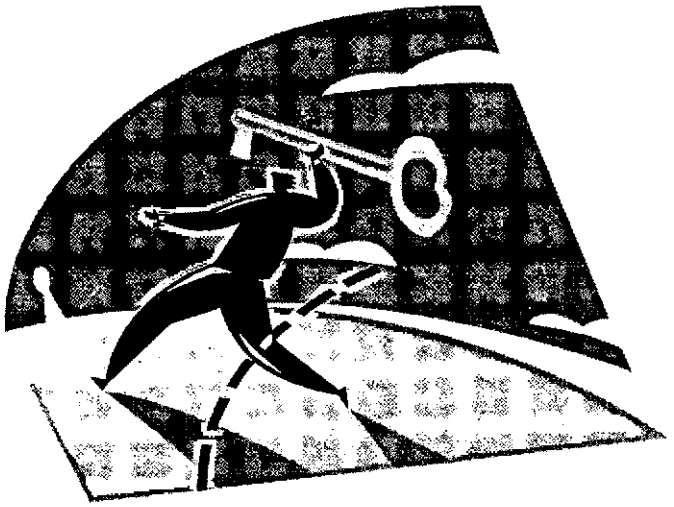
- **REDES INTEGRADAS** – Referente Roberto Kiessling, Supervisión del experto Cintia Dalvit Santandert.
- **POLÍTICAS CORPORATIVAS DE DATOS** – Referente Matias Mauro Fredes. Supervisión del experto Rolf Schenk.
- **POLÍTICAS DE ADMINISTRACIÓN DE SERVIDORES** – Referente Alejandro Silnik, experto.
- **ADMINISTRACIÓN DEL PARQUE INFORMÁTICO** – Referente Aldo Polanco, experto.

Proyecto:

"POLÍTICAS DE MITIGACIÓN DE RIESGOS"

Objetivo específico:

PREVENCIÓN Y POLÍTICAS DE SEGURIDAD

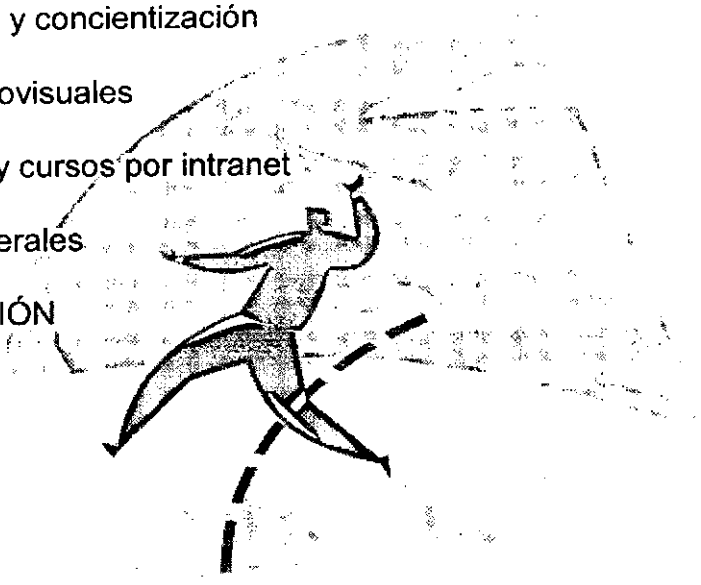


ACTIVIDAD 7

"PAUTAS GENERALES PARA LA CAPACITACIÓN Y CONCIENTIZACIÓN"

PAUTAS GENERALES PARA LA CAPACITACIÓN Y CONCIENTIZACIÓN

Índice



1. ENUNCIADO

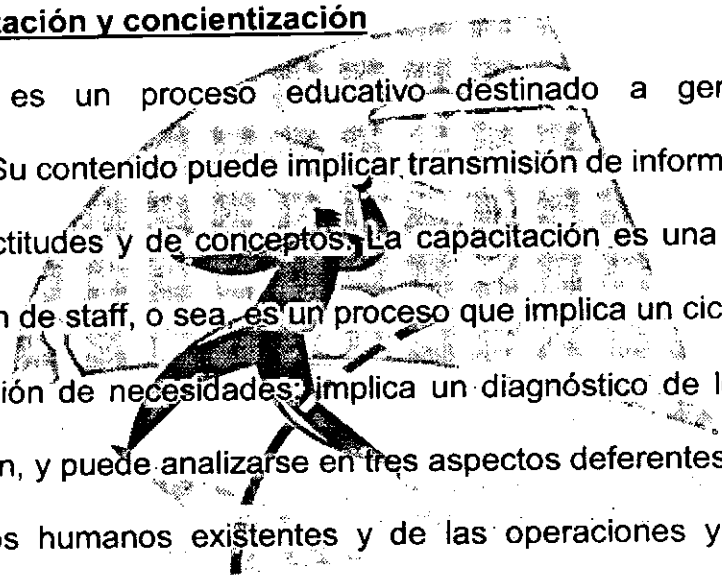
La informática y las nuevas tecnologías han adquirido en los últimos tiempos, una aceleración en el crecimiento de nuevos y potentes equipos o programas. La estrategia que la provincia tome frente al desafío de la revolución en las telecomunicaciones e internet en el mundo será central mientras desee obtener un rápido aumento de la productividad que permita mantener el crecimiento económico y la mejora de la calidad de vida de la población.

2. OBJETIVO

Confeccionar pautas generales para la capacitación y la concientización de los usuarios en las medidas de prevención para evitar las contingencias y minimizar los riesgos en todo lo posible, que serán consensuadas y entregadas a la Gerencia de Cocientización Comunitaria a fin que los mismos realicen la campaña correspondiente

3. CUERPO

3.1 Capacitación y concientización

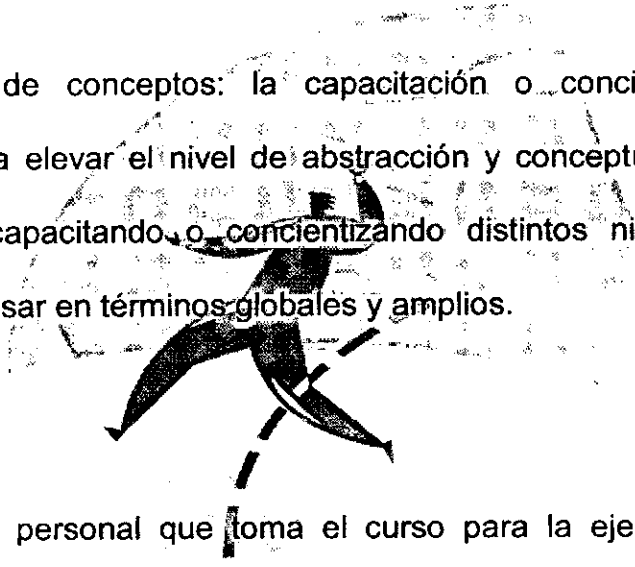


La capacitación es un proceso educativo destinado a generar cambios de comportamiento. Su contenido puede implicar transmisión de información, desarrollo de habilidades, de actitudes y de conceptos. La capacitación es una responsabilidad de línea y una función de staff, o sea, es un proceso que implica un ciclo de cuatro etapas:

- Determinación de necesidades: implica un diagnóstico de los problemas de la capacitación, y puede analizarse en tres aspectos deferentes: organizacional, de los recursos humanos existentes y de las operaciones y tareas que deben realizarse
- Programación de capacitación: busca planear en qué entrenar, a quien entrenar, cuando entrenar, donde entrenar y como entrenar, con el fin de utilizar la tecnología instruccional mas adecuada.
- Implementación y ejecución: implica la relación del binomio instructor / aprendiz y la relación instrucción / aprendizaje
- Evaluación de resultados: busca obtener retroalimentación del sistema y puede hacerse en el ámbito organizacional, de los recursos humanos o de las tareas y operaciones

En un programa de capacitación se tienen en cuenta los siguientes elementos:

- Transmisión de información: el elemento más importante en un programa de capacitación o concientización, es el contenido que se transmite.
- Desarrollo de habilidades: se trata de un entrenamiento a menudo orientado a las tareas y operaciones que van a ejecutarse.
- Desarrollo o modificación de actitudes: por lo general se refiere al cambio de actitudes negativas por actitudes más favorables entre los trabajadores. También puede involucrar e implicar la adquisición de nuevos hábitos y actitudes..
- Desarrollo de conceptos: la capacitación o concientización puede estar conducida a elevar el nivel de abstracción y conceptualización de ideas y de filosofías, capacitando o concientizando distintos niveles de personas que puedan pensar en términos globales y amplios.



Objetivos:

- Preparar al personal que toma el curso para la ejecución inmediata de las diversas tareas particulares de la organización.
- Proporcionar oportunidades para el continuo desarrollo personal.
- Cambiar la actitud de las personas, con varias finalidades.

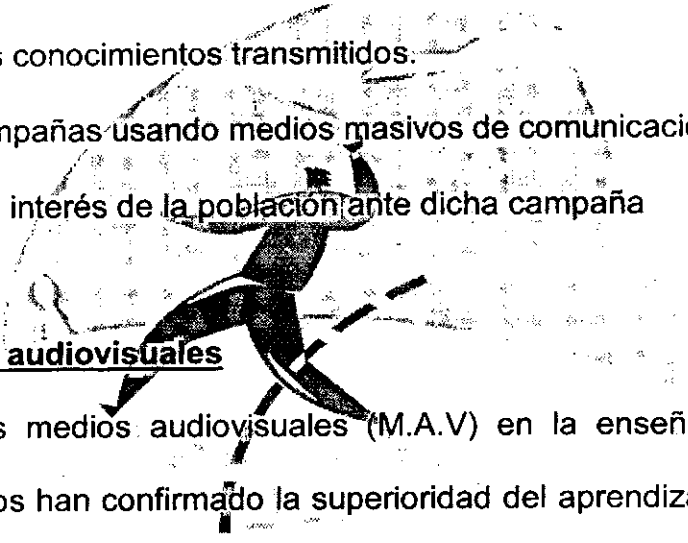
En la concientización, por otra parte, no se tiene en cuenta la forma de educar o como enseñar, sino como captar la atención de cierta clase de gente. No se consideran las habilidades del docente para el dictado de un curso, sino las habilidades que se usen para captar la atención e interés de la población con la campaña.

"Convencidos de que todo proceso de cambio es efectivo en la medida que todos los que participan del mismo deben estar comprometidos y conscientes de su relevancia,

se han tomado acciones tendientes a concientizar al personal de todos los niveles sobre la identificación y complejidad de los problemas, sus repercusiones potenciales y prepararnos para garantizar una puesta en producción definitiva exitosa." (Actividad 8 – Punto 3.2. Concientización y Capacitación del Contrato "Política de Mitigación de Riesgos")

Objetivos:

- Diseño de una campaña apuntando a gente para que tome conciencia, adquiera y ejecute los conocimientos transmitidos.
- Realizar campañas usando medios masivos de comunicación
- Despertar el interés de la población ante dicha campaña



3.2. Medios audiovisuales

La eficacia de los medios audiovisuales (M.A.V) en la enseñanza es indiscutible. Numerosos estudios han confirmado la superioridad del aprendizaje realizado a través de la técnica audiovisual.

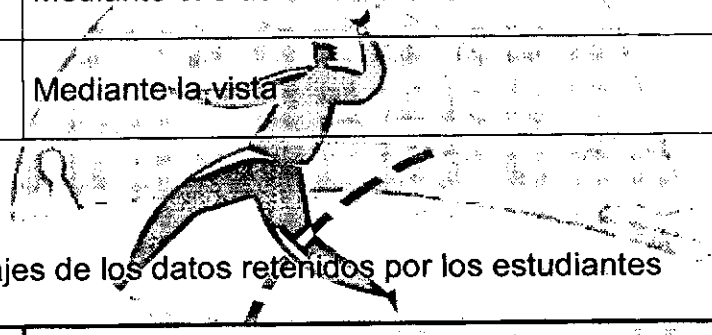
Brevemente se puede afirmar que los M.A.V.:

- Favorecen la retención
- Mantienen la atención
- Mejoran la percepción
- Facilitan la síntesis
- Estimulan el análisis
- Modifican las actitudes
- Dinamizan la participación

A este respecto, la oficina de estudios Secondy Vacuum Oil elaboró los siguientes datos:

A) ¿Cómo aprendemos?

PORCENTAJE	SENTIDO
1%	Mediante el gusto
1,5%	Mediante el tacto
3,5%	Mediante el olfato
11%	Mediante el oído
83%	Mediante la vista



B) Porcentajes de los datos retenidos por los estudiantes

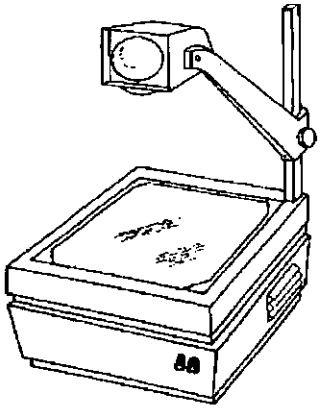
PORCENTAJE	DATOS RETENIDOS
10%	de lo que leen
20%	de lo que escuchan
30%	de lo que ven
50%	de lo que ven y escuchan
70%	de lo que se dice y se discute
90%	de lo que se dice y luego se realiza

C) Método de enseñanza

Método de enseñanza	Datos retenidos después de 3 horas:	Datos retenidos después de 3 días:
A: Solamente oral	70%	10%
B : Solamente visual	72%	20%
C: Oral y visual conjuntamente	85%	65%

La utilización de los medios audiovisuales en forma sistemática requiere unas instalaciones mínimas que eliminen las incomodidades que suponen: dificultades de oscurecimiento del aula, inadecuadas condiciones acústicas, falta de aparatos y material, etc. Todo ello unido a la rutina que acompaña muchas veces el quehacer docente, hace que estos valiosos colaboradores de la enseñanza, sean relegados al olvido o a una utilización esporádica que a veces lo único que consigue es alterar la marcha normal de las explicaciones.

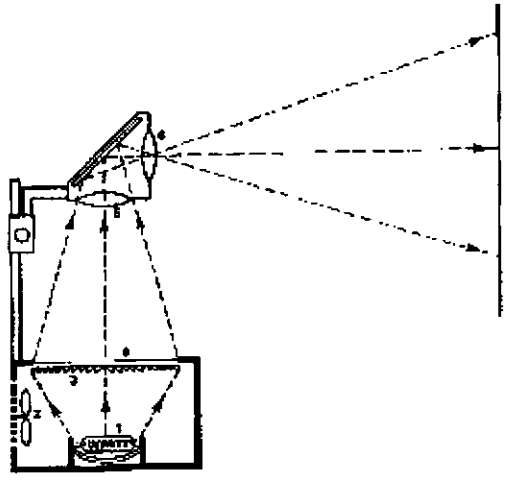
3.2.1. El retroproyector



Elementos de retroproyector

Los principales elementos de que consta son:

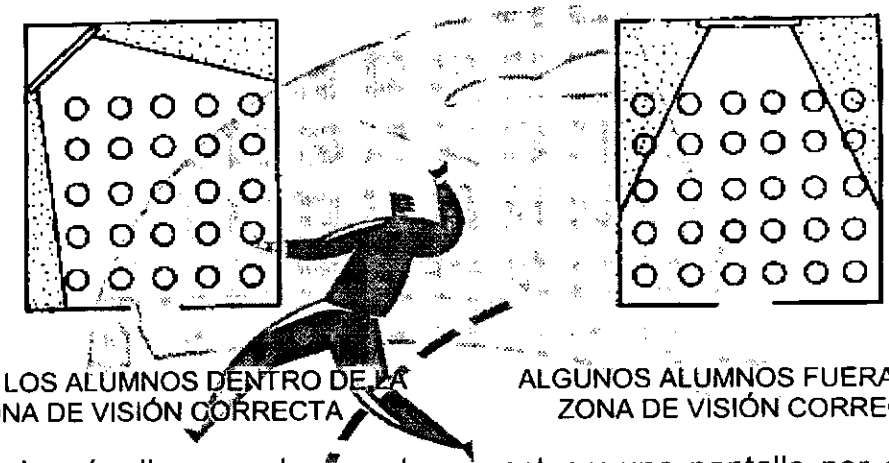
1. Un foco de luz, que generalmente consiste en una lámpara halógena de cuarzo de potencia variable (normalmente desde 420 hasta 1000 vatios).
2. Un ventilador, que refrigera el conjunto, y evita el deterioro de la lámpara por el calor. La alta potencia exigida para la retroproyección hace necesario un sistema de refrigeración.
3. La lente de Fresnel que recoge los rayos de luz convirtiéndolos en un haz uniforme y concentrado, lo distribuye por igual en toda la superficie de la placa de trabajo y lo canaliza hacia el objetivo.
4. La placa de trabajo (platina), constituida por un cristal resistente y colocada encima de la lente Fresnel, cuyas dimensiones suelen ser de 25 x 25 cm y de 28,5 x 28,5 cm. Sobre esta placa se colocan las transparencias.
5. Un objetivo, cuya finalidad es lograr una imagen lo más perfecta posible sobre una pantalla. Para facilitar el enfoque de este objetivo se dispone de un mando en la cabeza de proyección.
6. Un espejo de reflexión, cuya finalidad es desviar el haz de luz luminoso que llega vertical a la cabeza de proyección, en horizontal.



Condiciones de proyección

Una buena proyección y su aprovechamiento por parte de los alumnos depende de varios factores:

1. **Colocación del retroproyector en el aula.** Es conveniente situar el retroproyector y la pantalla en el ángulo derecho del aula, y no en el centro de la pared, ya que de esta manera todos los alumnos quedan dentro de la zona de visión correcta, al tiempo que dejamos libre el frontal delantero, en el cual suele estar situado el encerado, para poder ser utilizado al mismo tiempo.

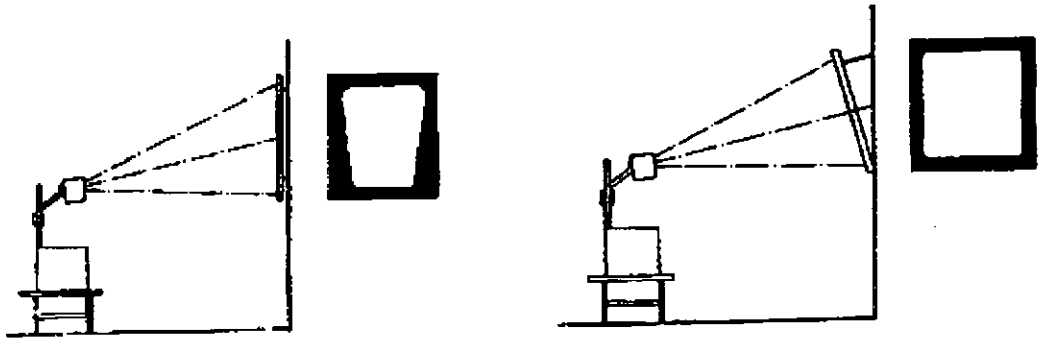


TODOS LOS ALUMNOS DENTRO DE LA ZONA DE VISIÓN CORRECTA

ALGUNOS ALUMNOS FUERA DE LA ZONA DE VISIÓN CORRECTA

Lo ideal sería disponer de un retroproyector y una pantalla por aula, estando ambos fijos y permanentes.

2. **Colocación del profesor.** El retroproyector deberá estar a la derecha del profesor, preferiblemente sobre una mesita auxiliar que permita colocar la platina al nivel de la mesa.
3. **Colocación del retroproyector respecto a la pantalla.** El haz de luz del retroproyector ha de formar un ángulo de 90° con la pantalla a fin de evitar distorsiones en la imagen.



Para no interferir la visibilidad a los alumnos de las filas más alejadas, la pantalla deberá situarse a la altura conveniente, precisándose entonces inclinar el objetivo hacia arriba y dar la misma inclinación hacia adelante a la pantalla.

4. **Tamaño de la imagen en la pantalla**. La imagen debe ser lo suficientemente amplia para ser vista desde todos los ángulos de la clase.

   Al aumentar la distancia retroproyector - pantalla se aumenta la imagen pero disminuye la nitidez de ésta.

5. **Colocación de los alumnos**. No deben estar ni demasiado cerca ni demasiado lejos. Normalmente se obtiene una perfecta visión colocando a los alumnos en una distancia que va desde dos hasta seis veces la base de la imagen y en el interior de un ángulo de 30° ambos lados del eje de la imagen.

<u>El material de paso. Las transparencias</u>

Uno de los problemas más graves que condicionan el empleo de los medios audiovisuales es el de disponer de material de paso adecuado.

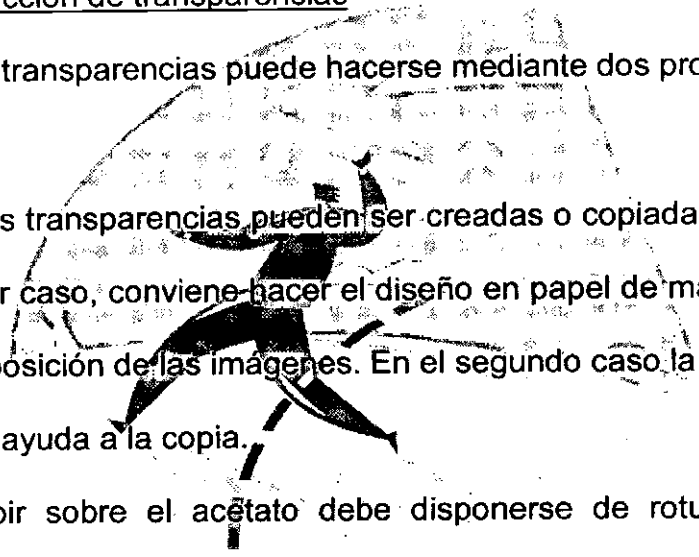
Tener retroproyectores, magnetoscopios o equipos de cine es sólo cuestión de dinero. Pero una vez que

se tienen surge el grave problema: ¿qué vamos a presentar a través de estos aparatos?

La solución no está en el material de paso comercial que se nos ofrece. En parte porque su precio suele ser alto; pero sobre todo, porque rara vez se adapta a los objetivos, ritmo y necesidades del profesor. Por esta razón es necesario que le profesor sepa preparar su propio material de paso.

Técnicas de producción de transparencias

La elaboración de transparencias puede hacerse mediante dos procedimientos: manual y mecánico.

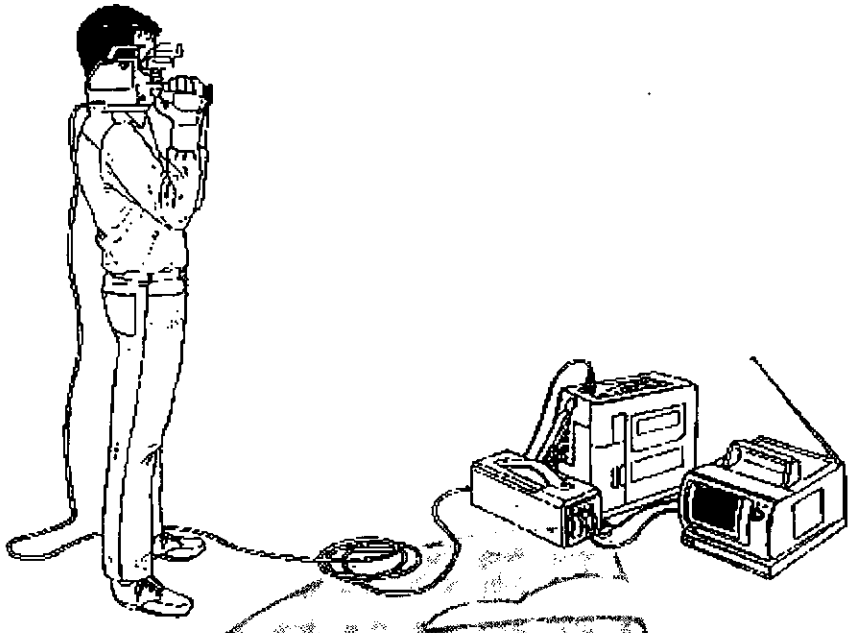


- **Manual**. Las transparencias pueden ser creadas o copiadas de libros o revistas. En el primer caso, conviene hacer el diseño en papel de manera que dé idea de la forma y posición de las imágenes. En el segundo caso la misma transparencia del acetato ayuda a la copia.

  Para escribir sobre el acetato debe disponerse de rotuladores de distintos colores y grosores.

- **Mecánico**. Incluye siempre un original y una máquina que haga la reproducción. Los sistemas más utilizados son el Termal (o de calor) y la fotocopia.

3.2.2. El Vídeo



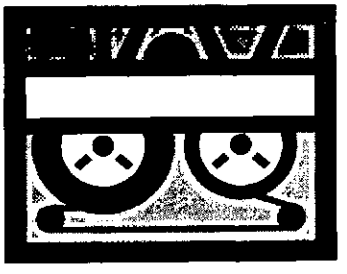
Elementos básicos de un equipo de vídeo

Un equipo grabador / reproductor de vídeo está constituido fundamentalmente por los siguientes elementos:

1. **Magnetoscopio**. Posibilita el registro y la reproducción de las informaciones (audio, vídeo y sincronismos) almacenadas sobre la cinta magnética.

   De los distintos formatos existentes, incompatibles entre sí, los utilizados generalmente en Telefónica por el profesorado son el VHS, el Beta, y en ocasiones el U - Matic (baja banda).

2. **Cassette vídeo**. Está constituido por dos bobinas coplanarias de cinta magnética ubicadas en el interior de una cajita de plástico.

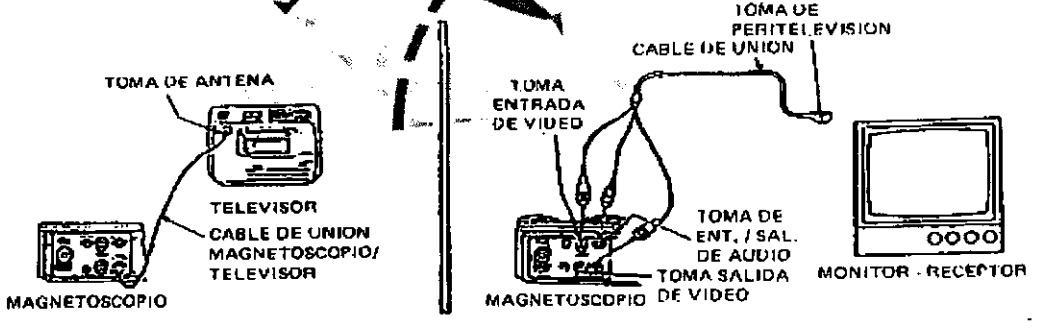
   Los videos domésticos utilizan cassettes con cinta de 1/2 pulgada de ancho, la cual presenta: una pista de audio en la parte superior; una serie de pistas de vídeo muy juntas dispuestas en diagonal en la parte central, y una pista de control en la parte inferior.

   El formato de la cinta deberá corresponder con el del magnetoscopio a utilizar.

3. **Televisor**. Nos permite visionar aquello que ha sido previamente grabado en la cinta de vídeo o que está siendo recogido por la cámara. Para ello, en el caso de un televisor normal con entrada de antena, basta con conectar dicha entrada con la salida del magnetoscopio y sintonizar con el canal correspondiente en el televisor. En el caso de trabajar con monitores el conexionado es diferente, dado que estos tienen separada la entrada de vídeo y la de audio.
4. **Cámara**. Generalmente, el equipo de vídeo es utilizado por el profesorado como reproductor de la información registrada anteriormente en una cinta.

   Cuando lo que se desea es generar la información es preciso contar con una cámara de grabación.

   Existen distintos tipos de cámaras, siendo aconsejable emplear una que sea del mismo sistema / marca que el magnetoscopio, afín de evitar tener que recurrir al uso de adaptadores.



   Las cámaras suelen estar equipadas con un micrófono incorporado, generalmente omnidireccional, para la grabación del sonido.

3.2.3. Afiches

Es el medio mas utilizado en campañas de concientización, ya que al tener grandes dimensiones, capta la atención de la gente.

Tiene la ventaja de que puede distribuirse por casi todos los sitios posibles de paso constante de las personas, como escaleras, ascensores, salas de recepción y por ello tiene una llegada masiva.

Debe contar con un diseño atractivo que llame la atención de las personas y los lean.

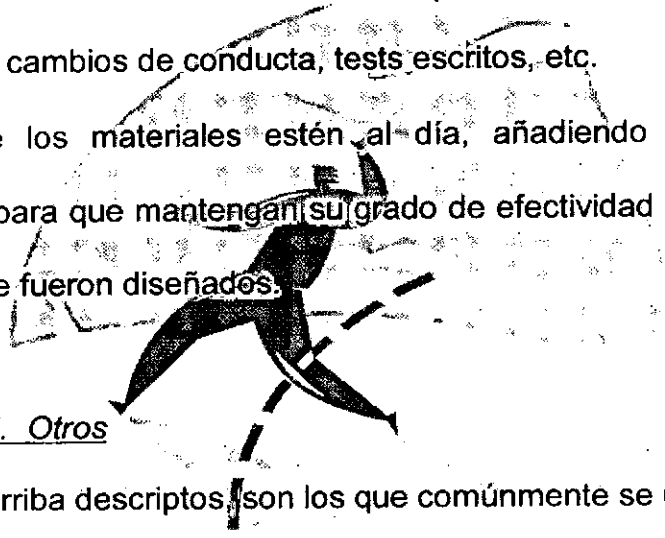
3.2.4. *Revisiones de detalles externos al material audiovisual*

Tanto si el material va a ser utilizado individualmente, en pequeño grupo o en gran grupo, es conveniente comprobar una serie de detalles que de no considerarse podrían contribuir a la no consecución de los objetivos previstos:

- Estudiar la disposición de local, tomas de corriente eléctrica, colocación de la pantalla y proyectores, control de luces, etc.
- Preparar todo el equipo necesario y auxiliar. extensores, lámparas de repuesto, fusibles, adaptadores, etc.
- Proporcionar un mínimo de comodidad a la audiencia: ventilación, temperatura, tipo de asientos, etc.
- Preparar el material a distribuir.
- Preparar el material audiovisual en la posición y en la secuencia correcta.

- Preparar la actitud del grupo hacia el material audiovisual.
- Emplear buenas técnicas en la utilización del material: centrado de imagen, foco, nivel de sonido, etc.
- Explotar directamente los materiales después de su utilización.

- Considerar la reacción del grupo para posibles modificaciones.
- Evaluar la efectividad de los materiales por diversos métodos: observación de reacciones, cambios de conducta, tests escritos, etc.
- Cuidar que los materiales estén al día, añadiendo o sustituyendo nuevo contenido, para que mantengan su grado de efectividad y cumplan los objetivos para los que fueron diseñados.



3.2.5. Otros

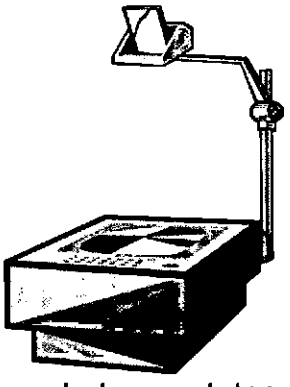
Todos lo medios arriba descriptos son los que comúnmente se usan para la difusión de campañas de concientización y para el dictado de cursos de capacitación. Los medios restante se usan con poca frecuencia, como por ejemplo:

- Propagandas en radio
- Propagandas en televisión
- Debates en radio / Tv
- Pasacalles
- Protectores de pantallas
- Folletos
- Correo electrónico
- etc

3.2.6. *Pautas generales para uso de M.A.V*

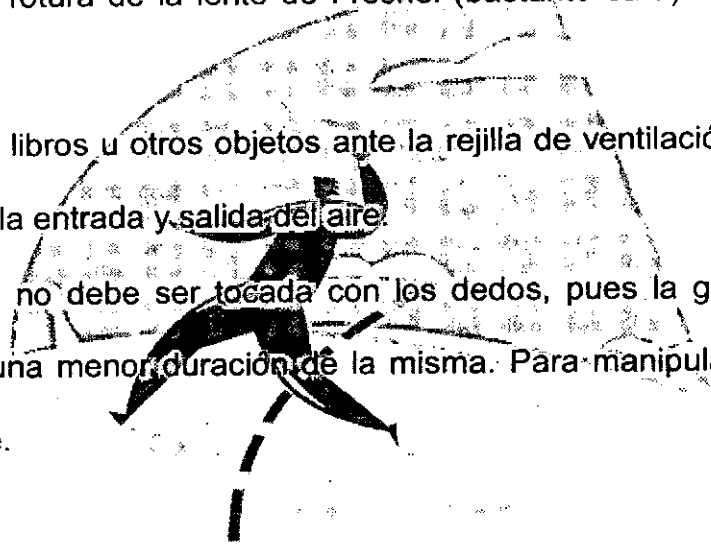
Retroproyector

- Antes de comenzar la clase debe comprobarse que el aparato funciona correctamente y colocarle en la situación adecuada para una perfecta visión.
- Antes de conectar el aparato debe asegurarse que la corriente que admite es del mismo voltaje que la corriente de la red instalada en el edificio.
- Para el uso del retroproyector no hace falta que la clase se encuentre oscurecida. El retroproyector puede utilizarse con luz natural.
- Cuando el profesor está utilizando el retroproyector y desea dirigir la atención a un punto determinado de la imagen, no es conveniente que se vuelva hacia la pantalla y señale en ella con la mano o con un puntero. Aparte de que, en esta situación, no domina a la audiencia, produce sombras sobre la pantalla que obstaculizan la visión completa. Lo correcto es que señale sobre le documento instalado en el retroproyector. Así se aprovecha una de las principales ventajas del aparato que consiste en el contacto continuo con los alumnos, al permanecer siempre enfrente a ellos.



- Durante la clase con el retroproyector, el profesor debe tenerlo encendido siempre que su explicación exija la imagen. Es mejor encender y apagar cuando sea necesario, que no mantenerlo todo el tiempo encendido, puesto que aparte del consiguiente calentamiento del aparato y de los acetatos, la atención de los alumnos se dirige a la zona de proyección, y si ésta no coincide con las palabras del profesor en ese momento, lo más probable es que se pierdan en el vacío.

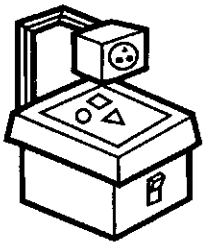
- El retroproyector es un aparato resistente. Lo único que puede dar una sorpresa al usuario es la lámpara. Tiene una vida teórica de 50 a 75 horas. El resto del mecanismo funcionará sin alteración y sin cuidados especiales durante años. Se deben tener siempre algunas lámparas de repuesto.
- Procurar no mover el aparato mientras no estén completamente frías las lámparas. Se corre el riesgo de que se fundan.
- Hay que tener cuidado con los golpes fuertes o caídas del aparato. Ello podría provocar la rotura de la lente de Fresnel (bastante cara) o de las lentes de la cabeza.
- No coloque libros u otros objetos ante la rejilla de ventilación del aparato, pues dificultarán la entrada y salida del aire.
- La lámpara no debe ser tocada con los dedos, pues la grasa de los mismos influye en una menor duración de la misma. Para manipularla ayudarse de un trapo suave.



Transparencias

- Una transparencia no debe contener toda la información posible, sino solo la esencial.
- La calidad técnica y estética de la trasparencia ha de ser buena. De entrada, el alumno infravalorará aquellas
- transparencias sin calidad, acostumbrado como está a las imágenes de la publicidad, televisión, etc.
- Despiertan más el interés las transparencias en colores que las de blanco y negro.

- Si se quieren obtener zonas de color plano y uniforme, lo ideal es el color adhesivo transparente que se encuentra en el mercado bajo diversas marcas. Es fácil dibujar el contorno a lápiz por la parte del papel protector y luego recortarlo con tijeras. Una vez hecho esto se separa el protector citado y se adhiere la hoja de color sobre le acetato.

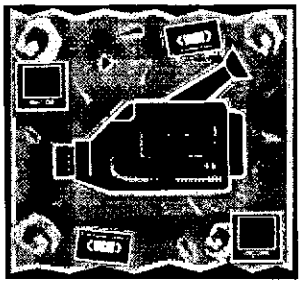


- Los dibujos en las transparencias estimulan la atención.
- Es muy importante comprobar experimentalmente que el tamaño de las letras será suficiente para su legibilidad por todos los alumnos. En general se recomienda que sean todas las mayúsculas, de palo seco y de una altura no inferior a los 4 mm.
- La escritura de los textos que aparezcan en la transparencia debe ser horizontal.
- Cuando se quiera destacar algún elemento, se pueden utilizar los siguientes recursos: colocarlo arriba y a la derecha de la transparencia; asignarle mayor tamaño o distinto color y forma;. enmarcarlo; separarlo suficientemente del resto...
- En el caso de transparencias "en libro" el número máximo de superposiciones (debido a la progresiva disminución de la nitidez conforme se aumenta el número de hojas de acetato) es de 4 - 5.

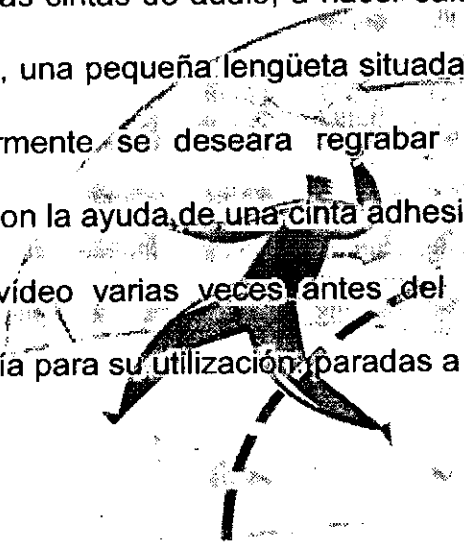
Video

- Antes de comenzar la clase debe comprobarse que el equipo funciona correctamente.
- Situar el monitor en un lugar que permita a todos los alumnos una perfecta visión del mismo (es aconsejable colocarlo en alto, por encima del nivel de las cabezas, especialmente cuando la clase tiene una estructura lineal).

- Al finalizar las sesiones de visionado se recomienda rebobinar la cinta totalmente, pues de lo contrario podría originarse una deformación mecánica en la cinta.



- Los videocassetes deben guardarse en su estuche protector cuando no se estén utilizando, a fin de evitar que se deposite polvo en la cinta.
- Para evitar el borrado no deseado de una cinta de vídeo se procederá, como ocurre con las cintas de audio, a hacer saltar, por medio de un destornillador o unas pinzas, una pequeña lengüeta situada en uno de los costados de la cajita. Si posteriormente se deseara regrabar bastará con obturar el orificio de protección con la ayuda de una cinta adhesiva.
- Visione el vídeo varias veces antes del comienzo del curso y elabore una pequeña guía para su utilización: paradas a realizar, puntos a resaltar, etc.



Afiches

- Tienen que estar ubicados en lugares estratégicos para su visualización
- Se deben colocar en lugares distintos de la organización
- No se debe utilizar demasiado texto.
- Se tienen que combinar colores se manera que se llame la atención del personal

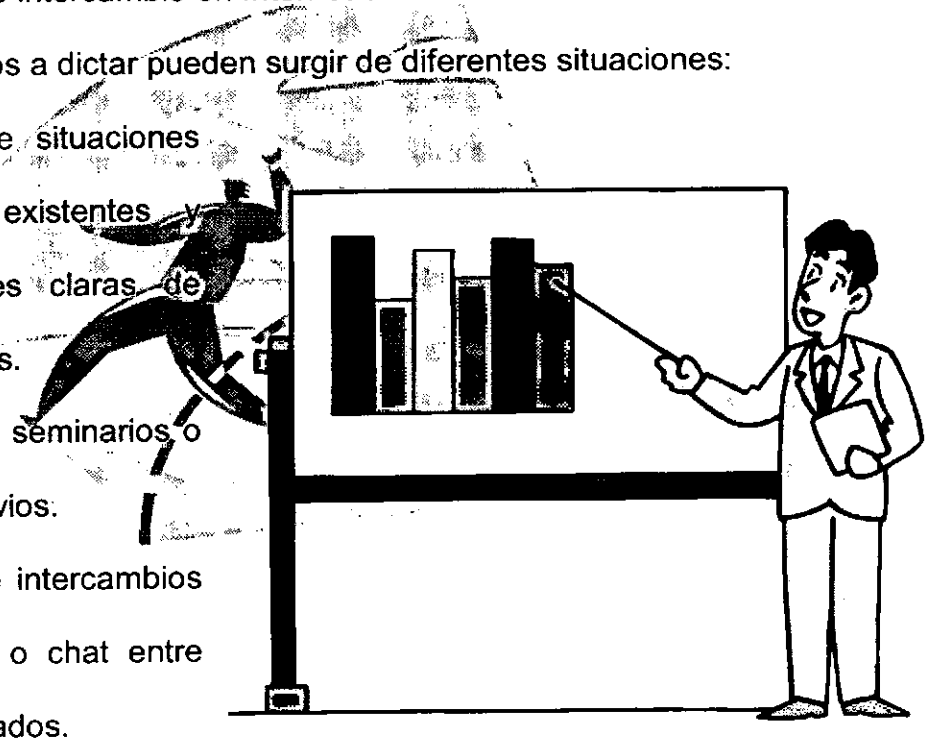
3.3. Seminarios y cursos por intranet

Si bien el sistema general de administración del programa de seminarios por Internet podría utilizarse en forma comercial, la filosofía con la que se plantea, de modo general, tanto para el desarrollo de la APP , como para el desarrollo del programa de seminarios por Intranet, es la de generar un espacio independiente y no comercial, de

trabajo e intercambio entre trabajadores de la APP de toda La Provincia. Con esta filosofía se debe realizar el reclutamiento de colaboradores para el dictado de los seminarios (así como para el desarrollo de los otros espacios en la Intranet). Todos los colaboradores inicialmente realizarán su tarea de manera ad-honorem. Y la SETI realizará todo el desarrollo y mantenimiento del sistema, de forma gratuita para los participantes de todos los seminarios.

En consecuencia, el reclutamiento de colaboradores se debe dar a partir de experiencias de trabajo e intercambio en Internet e Intranet.

Los seminarios y/o cursos a dictar pueden surgir de diferentes situaciones:



- ✓ A partir de situaciones laborales existentes y necesidades claras de los usuarios.
- ✓ A partir de seminarios o cursos previos.
- ✓ A partir de intercambios vía e-mail o chat entre los interesados.
- ✓ A partir de propuestas puntuales de la SETI.
- ✓ A partir de propuestas de Entes externos o privados.

En síntesis, el programa se va construyendo paso a paso.

Cada seminario debe ser semillero y la ocasión para crear nuevas y diferentes modalidades de trabajo.

La experiencia acumulada permite funcionar de un modo mas seguro, sistematizar y facilitar muchos procesos, y por lo tanto, encarar de un modo potenciado los nuevos pasos que se irán dando.

Herramientas

Las herramientas básicas con las que puede operar un Programa de Seminarios por Intranet (PSI) son las siguientes:

- Página de Capacitación En Línea del E-Government

Por medio de esta página se realiza la publicación de cursos o seminarios, publicación de solicitudes de inscripción, condiciones para la misma, horarios y días de los mismos, requerimientos básicos, condiciones de pagos o exenciones, etc.

- Portal del Empleado del E-Government

Es el medio a utilizar para la difusión de alcance masivo para toda la APP acerca de cursos y seminarios a ser dictados interna o externamente.

- Correo electrónico

Por este medio se reciben las solicitudes de inscripción, se distribuyen las clases, se procesan las preguntas y/o comentarios, se organizan los debates que puedan surgir (por medio de las llamadas "mailing list"), etc.

Esta es también la herramienta básica e imprescindible con que debe contar cualquier colega para poder inscribirse en cualquiera de nuestros seminarios.

- La web

Este medio permite que cada inscripto a cada seminario tenga acceso en forma permanente a todas las clases de cada seminario. También permite disponer de un formato universal válido para cualquier plataforma y/o sistema operativo de los participantes, para la edición de las clases.

- Reuniones virtuales

Se propone utilizar el mecanismo popularizado con el nombre de "Chat". Para facilitar su utilización se puede implementar una interfase vía web, ofreciendo así la posibilidad de evitar tener que conocer el manejo de los programas específicos de "chat".

Se puede realizar también experiencias de video con programas mas sofisticados como el Netmeeting o similares.

Modalidades funcionales de los seminarios / cursos

- *A cargo de uno o mas responsables*

En la mayoría de los casos, el dictado de cada seminario estará a cargo de uno o dos responsables. En esos casos, los seminarios / cursos se estructurarán según alguna de las variantes instrumentales siguientes:

a) Como espacios abiertos de trabajo, con un programa temático general pero sin delimitación ni del tiempo de duración total del seminario / curso ni de la cantidad de clases que tendrá el mismo.

Es algunos casos pueden demorar meses y ser también un espacio de trabajo.

b) Como espacios mas acotados de trabajo, ajustándose más a un programa predefinido de clases.

c) Otros

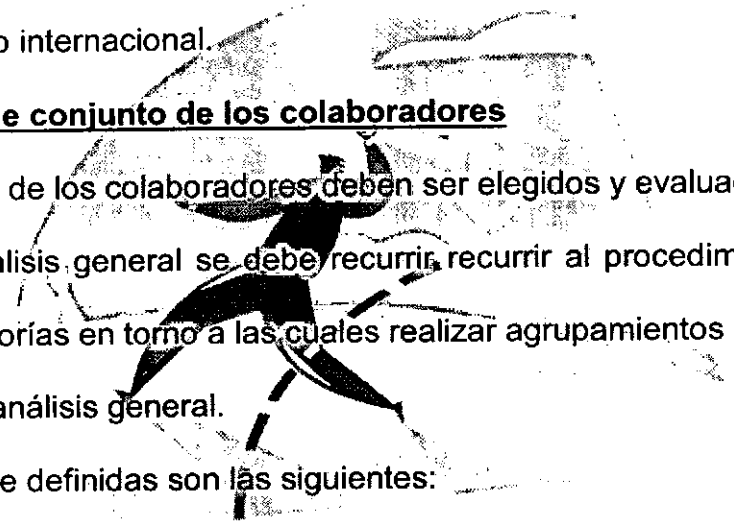
d) Otros seminarios, finalmente, se constituyen como una versión digital de un seminario dictado en tiempo real.

- *A cargo de un conjunto mayor de responsables*

El punto común en todos los casos de seminarios dictados por un conjunto mayor de responsables, debe ser el de ajustarse a un programa preestablecido temática y temporalmente. Ello por una cuestión casi obvia de organización.

No obstante ello, pueden variar en cuanto al origen y modo de estructuración.

- Puede ser la trascripción digitalizada de un seminario que se desarrolló en tiempo real, con unos meses de anticipación.
- Un primer intento puede agrupar a 3 o 4 responsables y si los resultados obtenidos son exitosos, puede hacerse una segunda versión con hasta 15 responsables.
- El éxito de experiencias de implementación de seminarios o cursos dictados por grupos de profesionales puede llevar a crear nuevos con invitados de nivel nacional y/o internacional.



Características de conjunto de los colaboradores

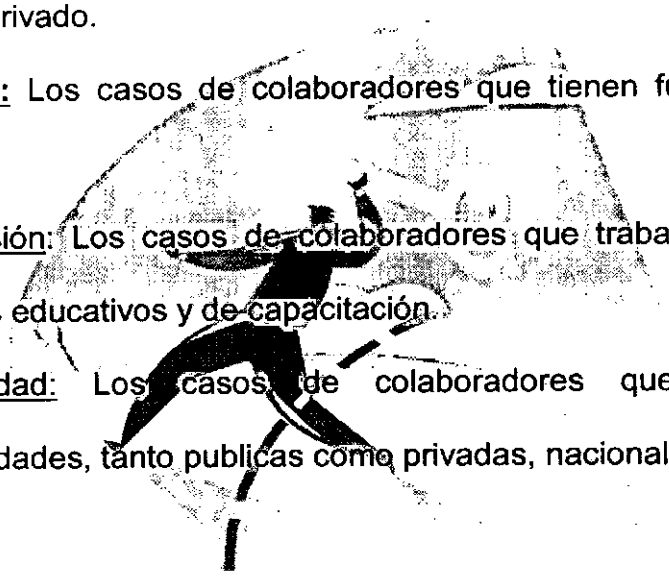
Todos y cada uno de los colaboradores deben ser elegidos y evaluados.

Pero para un análisis general se debe recurrir, recurrir al procedimiento de definir un conjunto de categorías en torno a las cuales realizar agrupamientos para, de ese modo, hacer factible un análisis general.

Las categorías que definidas son las siguientes:

- Asociaciones: Los casos de colaboradores que son miembros plenos de Instituciones o Asociaciones con o sin fines de lucro, con experiencias acabadas y exitosas en el dictado de cursos y/o seminarios.
- Admnistración Pública: Los casos de colaboradores que trabajan en administraciones públicas nacionales y provinciales, incluso en España la AP ha tenido una gran relevancia en los últimos años generando mucha información (www.map.es)
- ONG: Los casos de colaboradores que trabajan en Organizaciones no Gubernamentales y que pueden estar dedicados a trabajos de investigación y capacitación.

- Investigación: Los casos de colaboradores que trabajan en proyectos orgánicos de investigación
- Libros: Los casos de colaboradores que han publicado libros
- Organismos: Los casos de colaboradores que trabajan en organismos gubernamentales (justicia, organismos nacionales e internacionales, ministerios, gobierno, municipalidades, etc.)
- Privado: Los casos de colaboradores que trabajan en Organizaciones del ámbito privado.
- Revistas: Los casos de colaboradores que tienen funciones directivas en revistas.
- Supervisión: Los casos de colaboradores que trabajan en supervisión en servicios educativos y de capacitación.
- Universidad: Los casos de colaboradores que son docentes en Universidades, tanto publicas como privadas, nacionales o internacionales.



Funcionamiento General desde el punto de vista de los participantes

- *Procedimiento de inscripción*

La inscripción a cada uno de los seminarios / cursos que compondrán el programa será gratuita pero no libre.

El procedimiento será el siguiente.

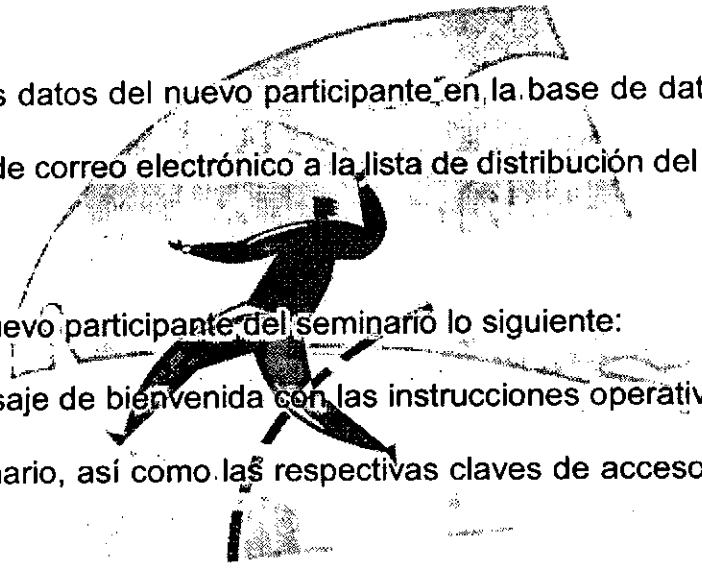
Cada interesado en inscribirse, en uno o varios seminarios / cursos, deberá enviar una solicitud a cada uno de ellos, con un conjunto de informaciones sobre su persona:

- ✓ Nombre y Apellido
- ✓ Dirección de Correo Electrónico
- ✓ Domicilio

- ✓ Lugar de trabajo (Repartición)
- ✓ Resumen de su Curriculum Vitae – Categoría, antigüedad, etc.
- ✓ Resumen de sus actuales actividades
- ✓ Motivos de interés en el seminario

Cada una de estas solicitudes será evaluada por los coordinadores y responsables de cada seminario / curso, quienes las aprobarán o rechazarán.

Una vez aprobada la solicitud de inscripción, el sistema debe realizar las siguientes operaciones.



1. Agregar los datos del nuevo participante en la base de datos del PSI, y agrega su dirección de correo electrónico a la lista de distribución del respectivo seminario / curso.
2. Enviar al nuevo participante del seminario lo siguiente:
   - un mensaje de bienvenida con las instrucciones operativas para participar en el seminario, así como las respectivas claves de acceso a la edición web del mismo.
   - las clases que se hubieran editado desde el comienzo del seminario hasta el momento de su inscripción.

- *Participación en cada seminario*

Como se señala mas arriba, las herramientas básicas de cada seminario son la página de Capacitación En Linea, el correo electrónico y la edición web.

Cada seminario es identificado con una palabra clave a partir de la cual se componen dos direcciones básicas:

- una dirección de correo electrónico (del tipo **palabra-clave@sanluis.gov.ar**)
- una dirección web (del tipo **http://wwww.sanluis.gov.ar/palabra-clave**)

La dirección de correo electrónico del seminario será la que opera como receptora de las solicitudes de inscripción a dicho seminario, así como de las posteriores preguntas y /o comentarios que quiera hacer cada participante a los coordinadores y responsables del seminario.

La dirección web define el sitio donde se encuentran editadas las clases del seminario, tanto en formato web como en formato de Word para Windows.

El acceso a dicho espacio se restringirá por password. Las claves de acceso serán suministradas a cada participante al momento de la aprobación de su solicitud de inscripción, en el mensaje de bienvenida.

De esta manera, cada participante dispone de un sitio en la Intranet al que puede acudir en cualquier momento a buscar cualquier clase, por los motivos que sean:

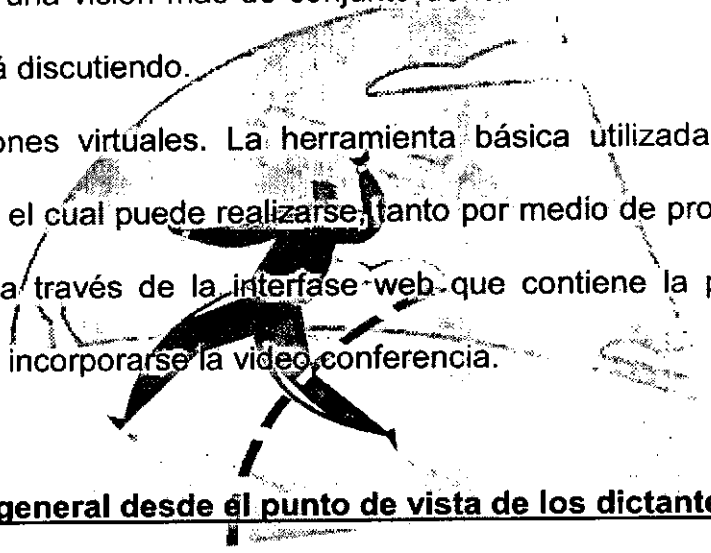
- pérdida de los archivos que se le enviaron por correo electrónico
- incompatibilidad de plataforma o de soft (es especialmente el caso de los usuarios de sistemas operativos anteriores a la versión en que se dicta el seminario / curso))
- necesidad de acceder a las clases del seminario desde una computadora que no sea la suya
- etc.

En síntesis, cada participante dispondrá de tres vías de participación básicas.

- Recibe las clases vía correo electrónico
- Dispone de un sitio web permanente donde encontrar las clases
- Dispone de una dirección de correo electrónico donde enviar sus preguntas y/o comentarios

A esta estructura básica, se agregan, según las necesidades de cada seminario en particular, las siguientes herramientas:

- Foro de discusión por correo electrónico (mailing list). A estas listas solo podrán suscribirse los participantes del respectivo seminario. Esta herramienta se utilizará básicamente para debates mas ágiles sobre temas puntuales y permitirá una comunicación directa entre los participantes del seminario.
- Foro de discusión vía web. Una herramienta similar a la anterior que, por un lado es menos ágil, pues requiere de navegación web, pero por el otro ofrece una visión mas de conjunto de los diferentes mensajes y de lo que se está discutiendo.
- Reuniones virtuales. La herramienta básica utilizada hasta ahora es el "chat", el cual puede realizarse, tanto por medio de programas específicos, como a través de la interfase web que contiene la página de gobierno. Puede incorporarse la video conferencia.



Funcionamiento general desde el punto de vista de los dictantes

Las tareas básicas desarrolladas por el coordinador o responsable de cada seminario son las siguientes.

- *Solicitudes de inscripción*

El sistema debe recibir todas las solicitudes de inscripción a cada seminario / curso, y las reenvía al responsable de cada uno de ellos.

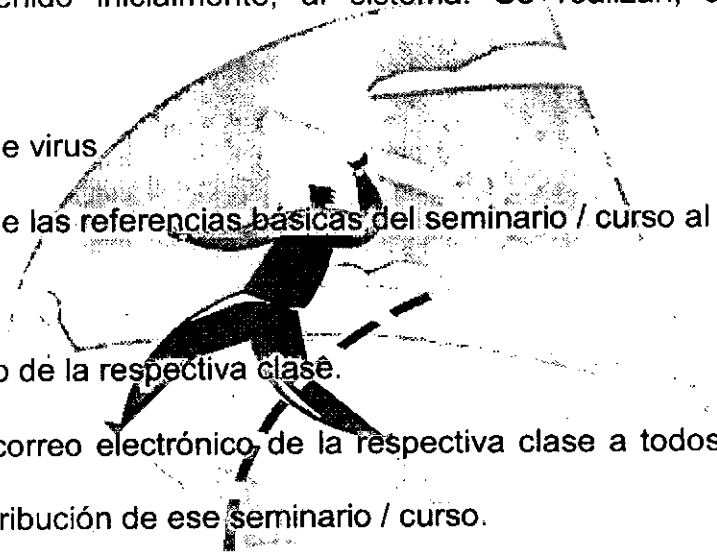
El responsable de cada seminario es el que aprueba o desaprueba cada solicitud, de acuerdo a ciertos criterios fijados con anticipación. En caso de considerarlo necesario, antes de expedirse, puede enviarle un mensaje al remitente de una solicitud de inscripción, requiriéndole una ampliación de la información que ha enviado.

Las solicitudes desaprobadas son desechadas y borradas.

Las solicitudes aprobadas son enviadas con el respectivo OK del responsable, all sistema, para su procesamiento (agregado del nuevo participante en nuestra base de datos, inclusión de su e-mail en la lista de distribución del respectivo seminario / curso, y envío al nuevo participante del mensaje de bienvenida con las instrucciones operativas y las clases editadas hasta ese momento).

- *Envío de Clases*

El responsable de cada seminario / curso envía las clases del mismo, según el cronograma convenido inicialmente, al sistema. Se realizan, a continuación, las siguientes tareas:



A. Chequeo de virus.
B. Agregado de las referencias básicas del seminario / curso al archivo de Word de cada clase.
C. Edición web de la respectiva clase.
D. Envío por correo electrónico de la respectiva clase a todos los incluidos en la lista de distribución de ese seminario / curso.

- *Respuestas a preguntas y/o comentarios*

El sistema recibe todas las preguntas y/o comentarios realizadas por cada participante de cada seminario, y las reenvía al respectivo responsable de cada seminario.

Se abren entonces las siguientes posibilidades.

Primero, en el caso de que se trate de un seminario cuyo dictado está a cargo de un conjunto de responsables, definir quien responde a la pregunta y/o comentario. Es el responsable y coordinador del seminario quien decide si responderá él mismo o delegará esa respuesta en alguno de sus colaboradores.

Segundo, el responsable del seminario también decide si la respuesta a la pregunta y/o comentario le es enviada en forma personal a quien la hizo o le es enviada a todos los participantes del seminario.

En el primer caso, él mismo se encarga del envío.

En el segundo caso, envía la respuesta al sistema, el cual se encarga de reenviársela a todos los incluidos en la lista de distribución de ese seminario.

El criterio para optar por una u otra alternativa consiste en la pertinencia que tenga la pregunta y/o comentario para el desarrollo general del seminario.

Por ejemplo, si se trata de una pregunta muy elemental, o de un simple mensaje de agradecimiento y/o felicitación, etc., entonces será mejor responder personalmente y no entorpecer el desarrollo del seminario con mensajes que, sin ningún tipo de desmerecimiento, no aportan gran cosa al mismo.

En cambio, aquellas preguntas y/o comentarios que aporten al desarrollo del seminario, convendrá reenviarlos a todos los participantes.

En resumidas cuentas, este tipo de funcionamiento es similar al de un foro moderado: solo son reenviados al conjunto de los participantes aquellas preguntas y/o comentarios que el responsable considere pertinentes.

Como se desprende de todo lo visto hasta ahora, las comunicaciones de los responsables de cada seminario se circunscriben básicamente a los intercambios de mensajes con el sistema (salvo los casos en que el responsable considere necesario una comunicación directa con un solicitante de inscripción para requerirle una ampliación de la información, o los casos en que prefiera responder a una pregunta y/o comentario de un participante en forma individual).

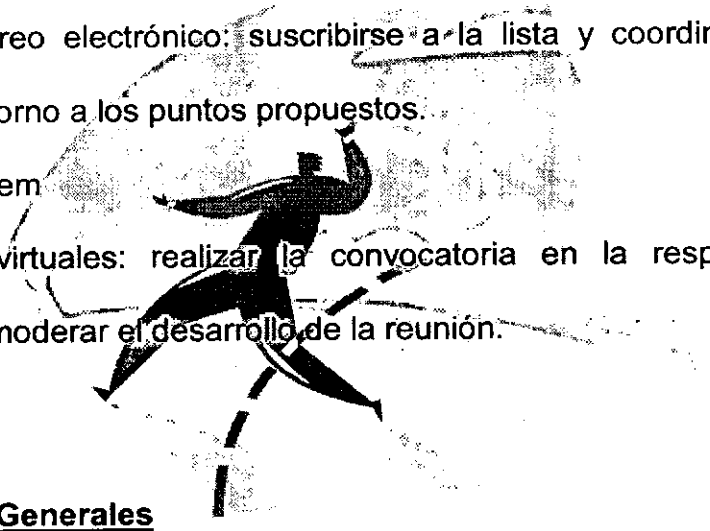
- *Coordinación de actividades extra*

Cuando la particularidad del seminario lo requiere, se pueden instrumentar las otras herramientas comentadas mas arriba:

- Foro de correo electrónico
- Foros web
- Reuniones virtuales

En cada caso, el responsable del seminario (o el colaborador en quien delegue esa tarea, en los casos de seminarios dictados por un conjunto de responsables), se hace cargo de la tarea de coordinación. La misma consistirá en:

- Foro de correo electrónico: suscribirse a la lista y coordinar y estimular los debates en torno a los puntos propuestos.
- Foro web: ídem
- Reuniones virtuales: realizar la convocatoria en la respectiva cartelera y coordinar y moderar el desarrollo de la reunión.



3.4. Pautas Generales

Las pautas que abajo se mencionan, son para el dictado de todo curso relacionado con capacitación o concientización y las cuales serán adoptadas por la Gerencia de Concientización Comunitaria:

Inscripciones:

Las mismas podrán ser realizadas personalmente, con un horario de atención limitado o por Internet (Intranet) las 24 horas a fin de lograr el mayor alcance posible para las mismas.

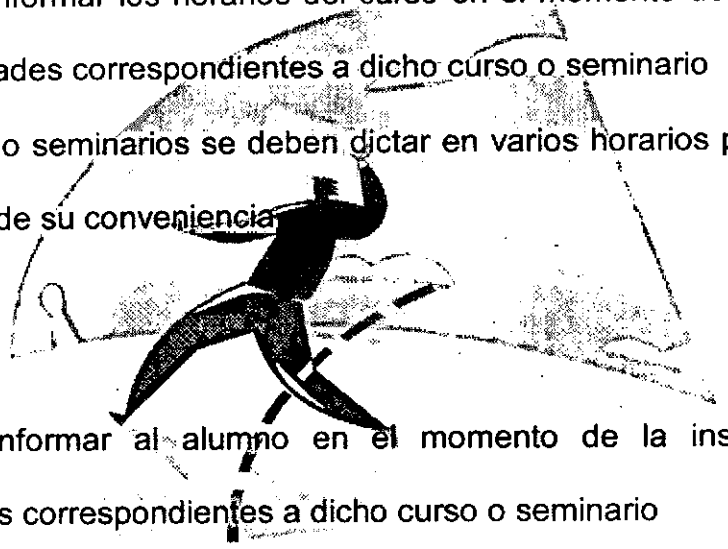
El Portal del Empleado, con sus ventanas de anuncios oficiales, debe ser el motor de información para que todos los usuarios sean informados de los cursos a dictarse.

Alumnos:

- En el momento de la inscripción, será informado acerca de la modalidad del curso (asistencia, examen, modalidad, etc)
- Se otorgará en forma personal, material de apoyo correspondiente al curso.

Horario

- Se deben informar los horarios del curso en el momento de la inscripción y en las publicidades correspondientes a dicho curso o seminario
- Los cursos o seminarios se deben dictar en varios horarios para que el alumno opte por el de su conveniencia



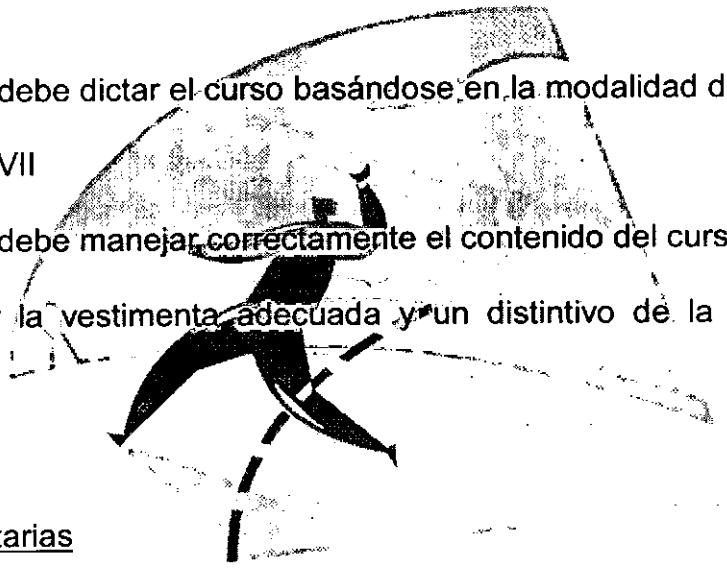
Duración

- Se debe informar al alumno en el momento de la inscripción y en las publicidades correspondientes a dicho curso o seminario
- La duración debe ser informada en cantidad de horas o clases y no en cantidad de tiempo
- Realizar descansos o recreos en cursos o seminarios cada 2 horas, para no lograr el cansancio o distracción de los alumnos.
- Siempre es recomendable que los cursos no sean de mas de 6 horas diarias porque pasado este período la atención decae gravemente. Por lo tanto debe iniciarse con los temas que puedan ser menos atractivos, dejando los mas llevaderos e interactivos para la segunda mitad del mismo.

Lugar

- Usar aulas que cumplan con los requisitos para el dictado de cursos (ambiente climatizado, limpieza, iluminación, medios audiovisuales, energía, escritorios o bancos para cada alumno, etc)
- Las aulas deben estar perfectamente señaladas para la fácil ubicación de la misma
- Las aulas deben estar aisladas a posible ruidos externos.

Profesor



- El profesor debe dictar el curso basándose en la modalidad descrita en el Anexo VI y Anexo VII
- El profesor debe manejar correctamente el contenido del curso
- Debe tener la vestimenta adecuada y un distintivo de la gerencia a la que pertenece

Campañas publicitarias

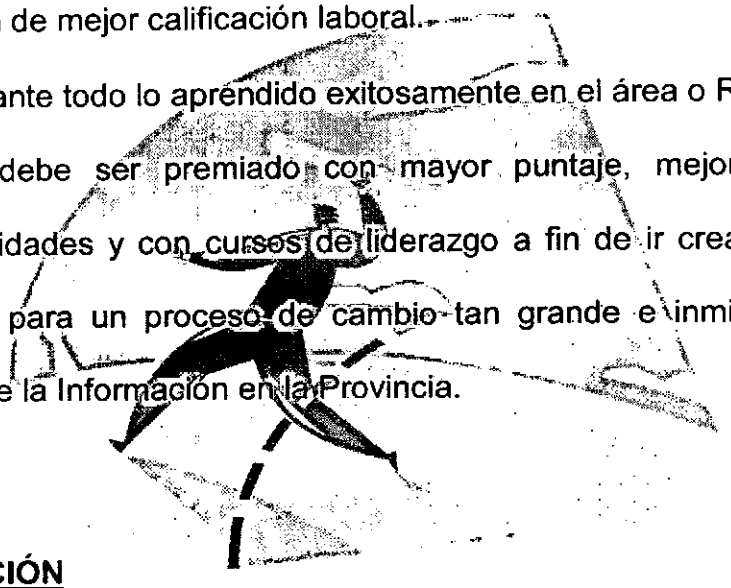
- Las campañas de capacitación o concientización que realice la Secretaría, deben estar acompañadas de campañas publicitarias en algunos medios de comunicación o audiovisuales

Certificaciones:

- Los cursos o seminarios deben contar con certificaciones de asistencia y/o aprobación, que puedan aumentar el bagaje del CV de quienes asistan, marcando la diferencia entre quienes se capacitan y quienes no. Además deben sumar puntaje para poder aspirar a mejoras en las categorías de la APP.

Resultados visibles y Valor agregado:

- Para que los cursos o seminarios no queden solo en una cursada deben proponerse metas a corto y mediano plazo a todos los concurrentes, como convertirlos en responsables de llevar a cabo actividades especiales en cada una de sus áreas, incluso sean portavoces de aquello que han aprendido.
- Si alguno de los mismos se califica adecuadamente por sus esfuerzos y logros, en próximos seminarios o cursos puede ser invitado a disertar, acerca de sus experiencias laborales, o modos de implementación, siendo también esto una certificación de mejor calificación laboral.
- Llevar adelante todo lo aprendido exitosamente en el área o Repartición a la que pertenece debe ser premiado con mayor puntaje, mejores condiciones y responsabilidades y con cursos de liderazgo a fin de ir creando los dirigentes adecuados para un proceso de cambio tan grande e inminente como es la Autopista de la Información en la Provincia.



4. RECOMENDACIÓN

"Las cualidades de la fuerza de trabajo serán el arma competitiva básica del siglo XXI, y las personas especializadas la única ventaja competitiva perdurable (...) las organizaciones serán redes finas de conocimiento que se limitan a conectar necesidades con recursos en cualquier lugar del planeta..." (Thurrow, L. "La guerra del siglo XXI", Ed. Vergara).

Se recomienda que las pautas generales para la concientización y la capacitación, sean adoptadas como estándares por la Secretaría de Estado de Tecnologías de la Información para todo seminario o curso a dictarse que tenga a cargo la Secretaría, para tener un acercamiento mas directo y mas amigable con el usuario, quien va a ser

el beneficiado con todo esto. En la elaboración de dichas pautas, se consultó con la Gerencia de Concientización Comunitaria.

5. BIBLIOGRAFÍA

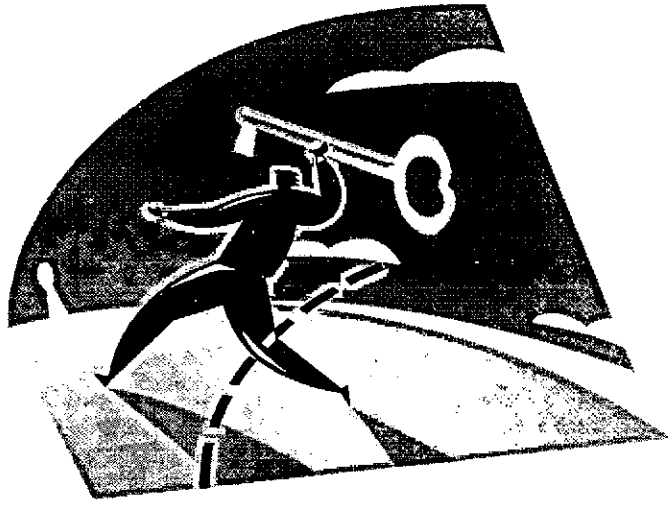
- Monografías.com – Sitio de monografías temáticas. Información publicada en www.monografias.com - Las consultadas fueron las siguientes:
    - Influencia de los Medios de Comunicación de Masas – Trabajo realizado por: Juan Ignacio Pontón. - ponton@dat1.net.ar
- Lafacu.com – Sitio de trabajos ordenados temáticamente – Información publicada en: www.lafacu.com - Las consultas fueron las siguientes:
    - Características de la publicidad exterior como medio publicitario
- Universidad Nacional de Tucumán – Comunicación para el Desarrollo. Información publicada en: www.geocities.com/Athens/Delphi/8644
- Ministerio de Administraciones Publicas - Pedagogía . Información publicada en: www.map.es/csi/caibi/ibfm/pedagogía
- La Bola – Sitio de información relacionada con la ingeniería del software – Publicada en: http://www.la-bola.com/abc9904.htm

Proyecto:

"POLÍTICAS DE MITIGACIÓN DE RIESGOS"

Objetivo específico:

PREVENCIÓN Y POLÍTICAS DE SEGURIDAD



ANEXO I

Actividad N°6

"DECRETO Nº 976-SGG-SETI-2001"

DECRETO Nº 976-SGG-SETI-2001

V I S T O:

El decreto N° 976-SGG-SETI-2001, en el que se ordena asignar una cuenta de correo electrónico, con una dirección electrónica a todos los Agentes de la Administración Pública Provincial, y

CONSIDERANDO:

Que la revolución de la información está transformándole mundo y en este proceso, está creando una sociedad global donde el papel preponderante está en las comunicaciones y las nuevas tecnologías que las facilitan

Que la Provincia ha reconocido la necesidad de participar en esta revolución de conocimiento

Que el uso del servicio de correo electrónico por los Agentes de la Administración Pública se ha transformado en una necesidad imprescindible para optimizar la calidad del trabajo en el Gobierno

Que el Gobierno debe establecer los lineamientos que regulen el uso racional de servicios de correo electrónico para hacer más eficiente la actividad diaria de la función pública, mejorando el desarrollo de las funciones del gobierno, a través de la definición de las facultades y responsabilidades de los usuarios funcionales, así como de las áreas de tecnología de información

Que es de interés para la Provincia aprovechar los servicios de correo electrónico en un marco de legalidad y transparencia, con normas claras y sencillas que aseguren el uso correcto del mismo.

Que la asignación de una cuenta de correo electrónico, con una dirección electrónica segura y reconocida a todos los Agentes de la Administración

Pública Provincial como "USUARIOS" del mismo, conlleva la responsabilidad de su utilización

Que es necesario establecer los términos de uso en el envío y recepción de los mensajes de correo electrónico, delimitando las responsabilidades que pudieran originarse mediante la utilización del mismo

Por ello y en uso de sus atribuciones,

EL GOBERNADOR DE LA PROVINCIA

D E C R E TA :

Art. 1°.- Establecer el presente reglamento de uso para los Agentes de la Administración Pública Provincial, los que en adelante serán denominados "USUARIOS" del "SERVICIO" de correo electrónico.

Art. 2°. DESCRIPCIÓN DEL SERVICIO

Todo Agente de la Administración Pública que desee una cuenta de correo electrónico, deberá solicitarla ante la Gerencia de Tecnologías de la Información, adjuntando copia de recibo de sueldo, constituyéndose como un "USUARIO" del servicio, es decir, con el derecho a usar normalmente del mismo.

3. OBLIGACIONES DEL USUARIO

Una vez verificada su condición de Agente de la Administración Pública, el usuario recibirá una cuenta y una contraseña al completar el formulario de registro, con sus datos personales y laborales completos.

El usuario es enteramente responsable de mantener la confidencialidad de la contraseña y cuenta, como también de todas las actividades que ocurran bajo la cuenta o contraseña del usuario.

4. CUENTA DE USUARIO, CONTRASEÑA Y SEGURIDAD

Como consecuencia de lo expresado precedentemente, el usuario se compromete a:

a) Notificar inmediatamente a la Gerencia de Tecnologías de la Información, de cualquier uso no autorizado de su cuenta, o de cualquier otra falla de seguridad.

b) Asegurarse de que su cuenta sea cerrada al final de cada sesión.

5. CONDUCTA DEL USUARIO

El usuario del correo electrónico, será responsable por todo el contenido que cargue, fije o envíe por correo electrónico.

6. LÍMITE A LA RESPONSABILIDAD POR PARTE DEL GOBIERNO.

El Gobierno de la Provincia, respecto del contenido fijado por medio del servicio de Correo Electrónico:

a) No garantiza la veracidad, integridad o calidad de dicho contenido

b) No se responsabiliza de los contenidos ofensivos, indecentes u objetables a los que, por usar el servicio puede quedar expuesto el Agente.

c) No se responsabiliza por errores u omisiones en algún contenido, por alguna perdida o daño de cualquier tipo que resulte del uso de algún contenido fijado, enviado por correo electrónico.

7. OBLIGACIONES DEL USUARIO

El usuario será el único responsable por las consecuencias que pueda acarrear la realización de las siguientes actividades:

Es responsabilidad del usuario no realizar las siguientes actividades:

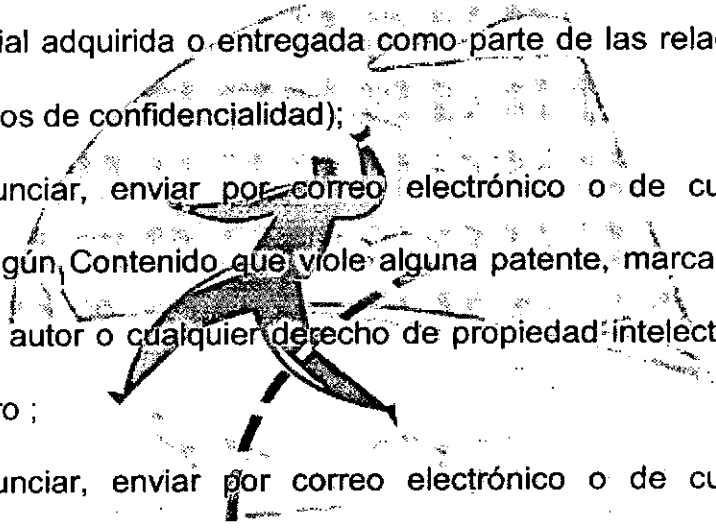
a. Cargar, anunciar, enviar por correo electrónico o de cualquier otra forma transmitir Contenido que sea ilegal, peligroso, amenazante, abusivo, hostigador, tortuoso, difamatorio, vulgar, obsceno, calumnioso, invasivo del derecho de privacidad, odioso, discriminatorio, o de cualquier otra forma ofensivo a terceros;

b. de ninguna manera dañar a menores de edad;

c. hacerse pasar por alguna persona o entidad, incluyendo, pero no limitado, a un funcionario o Agente del Gobierno, o hacer declaraciones falsas, o de cualquier otra forma falsificar su asociación a alguna persona o entidad.

d. falsificar encabezados o de cualquier otra forma manipular identificadores para desviar el origen de algún Contenido transmitido por medio del Servicio;

e. cargar, anunciar, enviar por correo electrónico o de cualquier otra forma transmitir algún Contenido del cual no tiene el derecho de transmitir por ley o bajo relación contractual o fiduciaria (tal como información interna, de propiedad y confidencial adquirida o entregada como parte de las relaciones de empleo o bajo contratos de confidencialidad);



f. cargar, anunciar, enviar por correo electrónico o de cualquier otra forma transmitir algún Contenido que viole alguna patente, marca, secreto comercial, derecho de autor o cualquier derecho de propiedad inteléctual ("Derechos") de algún tercero ;

g. cargar, anunciar, enviar por correo electrónico o de cualquier otra forma transmitir cualquier anuncio no solicitado o no autorizado, materiales promocionales, correo de solicitudes("junk mail", "spam"), cartas en cadena ("chain letters"), esquemas de pirámides ("pyramid schemes"), cuartos de compras "shopping rooms" o cualquier otra forma de solicitud, que están destinadas para tal propósito;

h. cargar, anunciar, enviar por correo electrónico o de cualquier otra forma transmitir algún material que contenga virus de software, o cualquier otro código de computadora, archivos o programas diseñados para interrumpir, destruir o limitar el funcionamiento de algún software o disco duro para computadora o equipo de telecomunicaciones;

i. interrumpir el fluido normal de diálogo, hacer que una pantalla se mueva más rápido de lo que otros usuarios pueden manejar, o de cualquier otra forma actuar de manera que afecte negativamente la habilidad de otros usuarios para vincularse en intercambios de tiempo reales;

j. interferir o interrumpir el Servicio, servidores, o redes conectadas al Servicio, o desobedecer cualquier requisito, procedimiento, política o regulación de redes conectadas al Servicio;

k. violar intencionalmente o no alguna ley local, estatal, nacional o internacional, incluyendo pero no limitado, a regulaciones promulgadas por la Comisión Nacional Bancaria y de Valores, la Comisión de Valores e Intercambio.

l. acechar o de cualquier otra forma hostigar a un tercero ; o colectar o guardar datos personales acerca de otros usuarios.

El usuario deberá ser siempre precavido a la hora de aportar cualquier información sobre la identificación personal referente a si mismo o a sus hijos a través del Servicio

7. TERMINACION

Cuando se compruebe uso indebido o falta de uso del servicio, el Gobierno de la Provincia podrá cancelar o discontinuar la cuenta asignada, sin perjuicio de toda otra acción que fuere necesario iniciar por el uso indebido del. Correo electrónico.

8 LIMITE DE LAS GARANTIAS

Será responsabilidad del usuario cualquier daño al sistema operativo de la computadora o pérdida de datos que resulte del material descargado.

9. PRÁCTICAS GENERALES ACERCA DEL USO Y RETENCIÓN

El Gobierno puede establecer prácticas generales y límites con respecto al uso del Servicio, incluyendo, pero sin limitarse a ello, el número máximo de días que los mensajes de correo electrónico, anuncios fijados en el boletín de mensajes u otros

contenidos cargados por el usuario. o por otros serán retenidos por el Servicio de Correo Electrónico, el número máximo de mensajes que puedan ser mandados o recibidos por una cuenta en el Servicio, el tamaño máximo de cualquier mensaje de correo electrónico que pueda ser mandado o recibido por una cuenta en el Servicio, el espacio máximo de disco que será asignado en los servidores del Gobierno para su beneficio y el número máximo de veces que usted podrá tener acceso al Servicio en un período de tiempo, así como la máxima duración de cada uno de los accesos. En virtud de lo anterior, el Gobierno no tiene responsabilidad u obligación legal por el borrado o falla al guardar mensajes u otras comunicaciones, o cualquier otro Contenido mantenido o transmitido por el Servicio, reservándose el Gobierno el derecho de **remover cuentas** que han estado inactivas por un período prolongado de tiempo y de **modificar estas prácticas generales y límites** en cualquier momento, a su solo arbitrio, sin necesidad de previa notificación.

El Gobierno no tiene obligación de supervisar los Servicios,. sin embargo, el Gobierno, se reserva el derecho de revisar los materiales enviados y de suprimir cualquier material a su única discreción. El Gobierno se reserva igualmente el derecho de denegarle en cualquier momento el acceso a cualquiera de los Servicios, sin previo aviso y por los motivos que sean.

10. MODIFICACIONES AL SERVICIO

El Gobierno tendrá el derecho de modificar, o discontinuar el Servicio de correo electrónico o cualquier parte del mismo, temporalmente, en cualquier momento, por lo que el Gobierno no será responsable hacia el usuario o terceras partes por ninguna modificación, suspensión, o interrupción del Servicio.

11. DERECHOS DE PROPIEDAD DE EL GOBIERNO

El Usuario acepta y acuerda que el Servicio y cualquier software necesario usado en conexión con el Servicio ("Software") contiene propiedad e información confidencial que se encuentra protegida bajo las leyes aplicables de propiedad intelectual y de otra naturaleza. Además, acepta y acuerda que el contenido, está protegido por los derechos de autor, marcas comerciales, marcas de servicio, patentes y otros derechos y leyes de propiedad.

Con excepción a lo expresamente autorizado por el Gobierno o los anunciantes, el usuario se compromete a no modificar, rentar, arrendar prestar, vender, distribuir o crear obras derivadas en base al Servicio o al Software, en todo o en parte.

El Gobierno le otorga un derecho y licencia personal, **no-transferible, y no-exclusiva** para usar el código objeto de su Software en una sola computadora; siempre y cuando no copie, modifique, haga una obra derivativa, haga ingeniería reversiva, haga ensamblaje reversivo, o de cualquier otra manera intente descubrir alguno de los códigos de configuración, venda, asigne, subarriende, otorgue un interés de seguridad o de cualquier otra forma transfiera algún derecho en el Software. El usuario no deberá modificar de ninguna manera el Software o a usar versiones modificadas del Software, incluyendo sin limitación, el propósito de obtener acceso no autorizado al Servicio. Se obliga, asimismo, a no entrar al Servicio por ningún otro medio que no sea la zona interfacial provista por el Gobierno para uso de entrada al Servicio.

12. NOTIFICACIÓN

Las notificaciones podrán ser enviadas por medio de correo electrónico o cualquier otro medio. El Servicio también puede proveer notificaciones de los cambios de los Términos y condiciones del Servicio, u otros asuntos, mostrándole avisos o enlaces a anuncios en el Servicio.

13. DERECHOS DE AUTOR Y AGENTES DEL DERECHO DE AUTOR

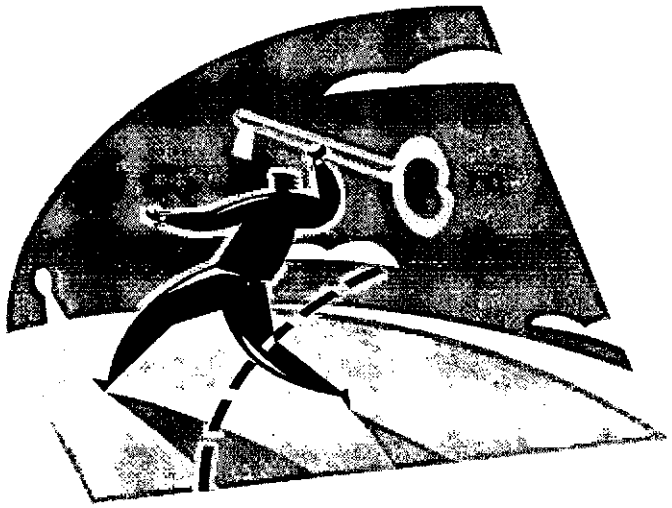
El Gobierno respeta el derecho de propiedad intelectual de terceros y requiere a sus usuarios que hagan lo mismo.

Proyecto:

"POLÍTICAS DE MITIGACIÓN DE RIESGOS"

Objetivo específico:

PREVENCIÓN Y POLÍTICAS DE SEGURIDAD



ANEXO II

Actividad N°6

PROYECTO DE DECRETO "USO DE INTENET"

PROYECTO DE DECRETO "USO DE INTENET"

V I S T O:

El decreto N° 000-GSSL-SETI-2001, en el que se ordena que el uso de la Intranet de gobierno es para uso exclusivo de trabajo dentro de la Administración Pública Provincial, y

CONSIDERANDO:

Que los problemas y peligros de la red (Intranet-Internet) son el tema de una amplia discusión pública y en muchas ocasiones esta discusión carece de la información necesaria acerca del Internet.

Que el manejo sin dificultades, el acceso aparentemente ilimitado al conocimiento y la alta flexibilidad comunicativa son temas que ejercen una fascinación casi mítica capaz de suscitar gran entusiasmo y temor a la vez.

Que determinados actos delictivos tales como la violación de barreras de seguridad, para acceder a datos secretos y privados, o la difusión de pornografía infantil, se prestan para una tematización espectacular a nivel público.

Que la Provincia ha reconocido la necesidad de participar en esta revolución de conocimiento

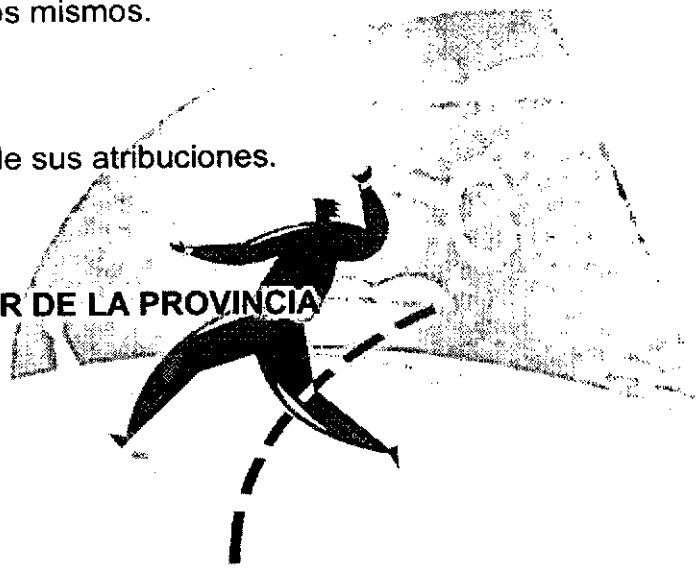
Que el uso del servicio de los servicios de red por los Agentes de la Administración Pública se ha transformado en una necesidad imprescindible para optimizar la calidad del trabajo en el Gobierno

Que el Gobierno debe establecer los lineamientos que regulen el uso racional de los servicios para hacer más eficiente la actividad diaria de la función pública, mejorando el desarrollo de las funciones del gobierno, a través de la

definición de las facultades y responsabilidades de los usuarios funcionales, así como de las áreas de tecnología de información

Que es de interés para la Provincia aprovechar los servicios de la red en un marco de legalidad y transparencia, con normas claras y sencillas que aseguren el uso correcto del mismo.

Que es necesario establecer los términos de uso en el manejo de los servicios de red, delimitando las responsabilidades que pudieran originarse mediante la utilización de los mismos.



Por ello y en uso de sus atribuciones.

EL GOBERNADOR DE LA PROVINCIA

D E C R E T A :

Art. 1°.- Establecer las restricciones necesarias para la navegación de los "USUARIOS" en la Intranet tanto como para Internet, en la Administración Pública Provincial.

Art. 2°. DESCRIPCIÓN DEL SERVICIO

Todo agente de la Administración pública que desee navegar en la Intranet de Gobierno y acceder al servicio de Internet, deberá solicitarlo ante la Gerencia de Servicios San Luis.

Art. 3° OBLIGACIONES DEL USUARIO

El usuario será el único responsable por las consecuencias que pueda acarrear la realización de las siguientes actividades:

Es responsabilidad del usuario no realizar las siguientes actividades:

a. Bajar Información que no este relacionada con fines de trabajo.

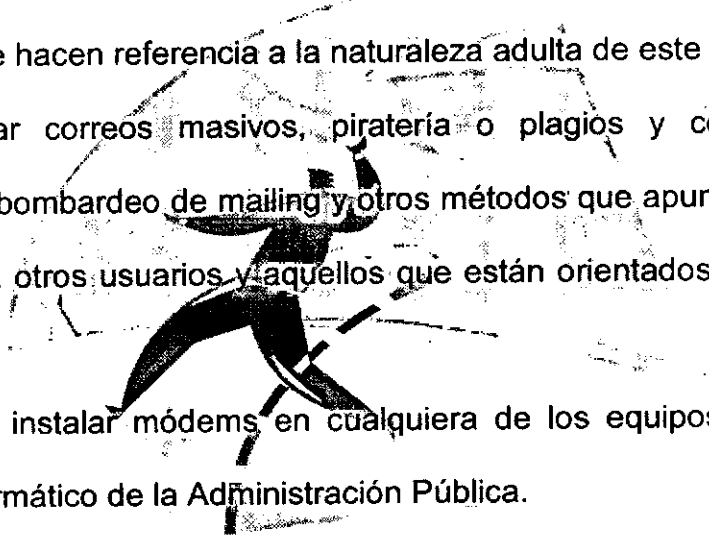
b. Usar la red para audio y video de sitios que lo permitan en línea.

c. Realizar trafico y descompresión de mp3.

d. Almacenar en la red, información que no este relacionada con temas laborales.

e. Cargar, enviar o levantar paginas de sitios pornográficos o que fomenten la delincuencia. La Secretaria se adhiere a las regulaciones y leyes Argentinas y de la EUA. Que hacen referencia a la naturaleza adulta de este material.

f. Realizar correos masivos, piratería o plagios y copias de software, spamming, bombardeo de mailing y otros métodos que apuntan a negar servicio o acceder a otros usuarios y aquellos que están orientados a la violación de la seguridad.



g. Usar e instalar módems en cualquiera de los equipos que conformen el parque informático de la Administración Pública.

h. Conectarse con módems a la Intranet de Gobierno que no estén autorizados por la Gerencia de Tecnologías de la Información.

i. Instalar redes internas sin la previa supervisión y aprobación de la Gerencia de Tecnologías de la Información.

j. No conectar las redes internas a la Intranet de gobierno.

El usuario deberá ser siempre precavido a la hora de aportar cualquier información sobre la identificación personal referente a si mismo o a sus hijos o parientes a través del servicio.

Art.5° CONDUCTA DEL USUARIO

El usuario de la intranet de Gobierno, será responsable por todo el contenido que maneje, difunda o envíe en la red.

Art 6° LIMITE A LA RESPONSABILIDAD POR PARTE DEL GOBIERNO

Art. 7° TERMINACIÓN

Cuando se compruebe uso indebido, el Gobierno de la Provincia podrá cancelar o discontinuar el servicio.

Art. 8° LIMITE DE LAS GARANTIAS

Será responsabilidad del usuario cualquier daño al sistema operativo de la computadora o pérdida de datos que resulte del material descargado o manipulado desde la red.

Art. 9° PRÁCTICAS GENERALES ACERCA DEL USO Y RETENCION

El Gobierno puede establecer prácticas generales y límites con respecto al uso del Servicio, como auditorias internas de los equipos de hardware, tanto en almacenamiento de contenido como de software utilizado.

El Gobierno no tiene obligación de supervisar los Servicios,. sin embargo, el Gobierno, se reserva el derecho de revisar la red, materiales enviados, almacenados y de suprimir cualquier material a su única discreción. El Gobierno se reserva igualmente el derecho de denegarle en cualquier momento el acceso a cualquiera de los Servicios, sin previo aviso y por los motivos que sean.

Art. 10°. MODIFICACIONES A LOS SERVICIOS

El Gobierno tendrá el derecho de modificar, o discontinuar los Servicios de redes o cualquier parte del mismo, temporalmente, en cualquier momento, por lo que el Gobierno no será responsable hacia el usuario o terceras partes por ninguna modificación, suspensión, o interrupción de los Servicios.

Art. 11°. DERECHOS DE PROPIEDAD DE EL GOBIERNO

El Usuario acepta y acuerda que el Servicio y cualquier software necesario usado en conexión con el Servicio ("Software") contiene propiedad e información confidencial que se encuentra protegida bajo las leyes aplicables de propiedad intelectual y de otra naturaleza. Además, acepta y acuerda que el contenido, está protegido por los derechos de autor, marcas comerciales, marcas de servicio, patentes y otros derechos y leyes de propiedad.

Con excepción a lo expresamente autorizado por el Gobierno o los anunciantes, el usuario se compromete a no modificar, rentar, arrendar prestar, vender, distribuir o crear obras derivadas en base al Servicio o al Software, en todo o en parte.

El Gobierno le otorga un derecho y licencia personal, **no-transferible, y no-exclusiva** para usar el código objeto de su Software en una sola computadora; siempre y cuando no copie, modifique, haga una obra derivativa, haga ingeniería reversiva, haga ensamblaje reversivo, o de cualquier otra manera intente descubrir alguno de los códigos de configuración, venda, asigne, subarriende, otorgue un interés de seguridad o de cualquier otra forma transfierá algún derecho en el Software. El usuario no deberá modificar de ninguna manera el Software o a usar versiones modificadas del Software, incluyendo sin limitación, el propósito de obtener acceso no autorizado al Servicio. Se obliga, asimismo, a no entrar al Servicio por ningún otro medio que no sea la zona interfacial provista por el Gobierno para uso de entrada al Servicio.

Art. 12°. NOTIFICACIÓN

Las notificaciones podrán ser enviadas por medio de correo electrónico, Mesa de Ayuda o cualquier otro medio. El Servicio también puede proveer notificaciones de los cambios de los Términos y condiciones del Servicio, u otros asuntos, mostrándole avisos o enlaces a anuncios en el Servicio.

Art. 13°. DERECHOS DE AUTOR Y AGENTES DEL DERECHO DE AUTOR

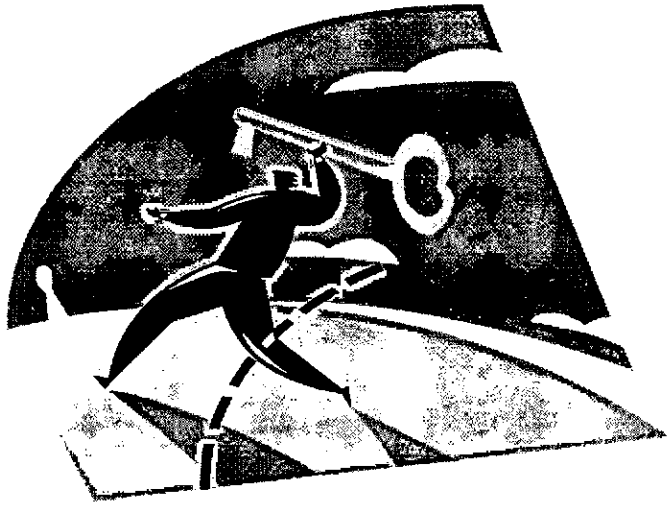
El Gobierno respeta el derecho de propiedad intelectual de terceros y requiere a sus usuarios que hagan lo mismo.

Proyecto:

"POLÍTICAS DE MITIGACIÓN DE RIESGOS"

Objetivo específico:

PREVENCIÓN Y POLÍTICAS DE SEGURIDAD



ANEXO III

Actividad N°6

PROYECTO DE DECRETO "REFERENTES INFORMÁTICOS"

PROYECTO DE DECRETO "REFERENTES INFORMÁTICOS"

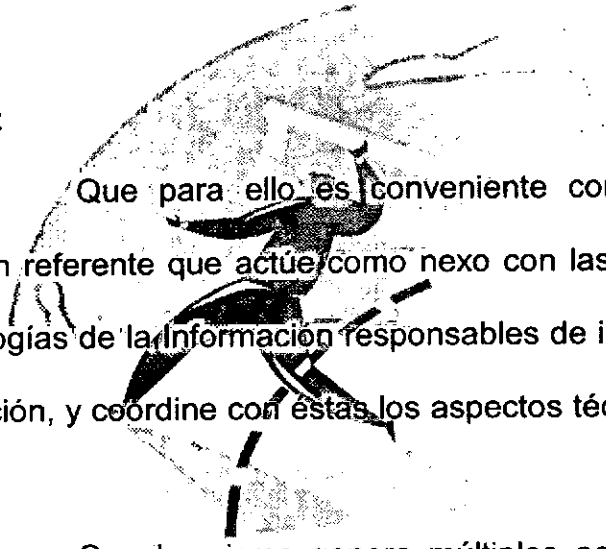
DECRETO Nº -SGG-SETI-2001.

SAN LUIS,

V I S T O :

La necesidad de continuar con el avance de la puesta en producción del Sistema de Información Provincial que conforman las aplicaciones que corren sobre la Intranet de Gobierno.; y;

CONSIDERANDO:



Que para ello es conveniente contar en cada Ministerio y Secretarías con un referente que actúe como nexo con las áreas de la Secretaría de Estado de Tecnologías de la Información responsables de implementar la mencionada puesta en producción, y coordine con éstas los aspectos técnicos para el desarrollo de sistemas propios;

Que la misma genera múltiples acciones, tanto relacionadas con los equipos informáticos, como con los recursos Humanos a afectar;

Que no es posible desarrollar una labor eficiente y ágil a la altura que los proyectos de Reinvención del estado y Autopista de la Información exigen, si no se cuenta con responsables por área capaces de coordinar las acciones emergentes, una acción eficiente y ágil si no se cuenta con responsables por área que lideren en las mismas las referidas acciones;

Por ello y en uso de sus atribuciones;

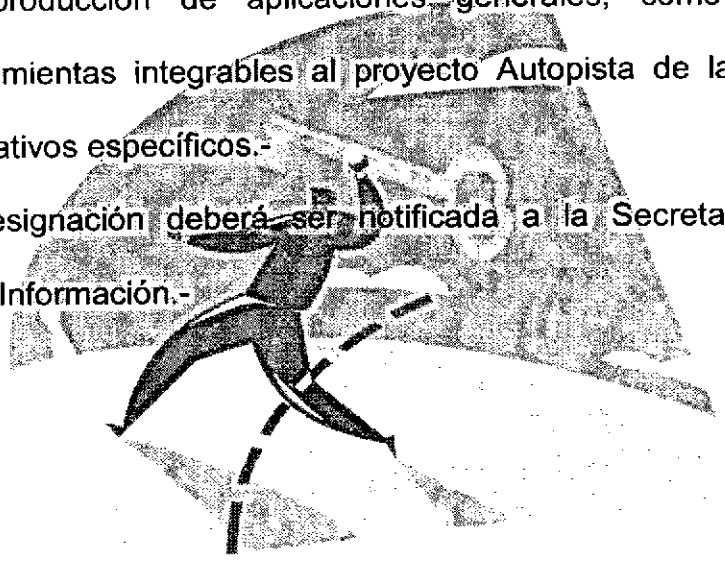
EL GOBERNADOR DE LA PROVINCIA

DECRETA

Art. 1°.- Cada Ministerio y Secretaría deberá designar, dentro de su plantel de personal, en un plazo no mayor a cinco (5) días, un "referente informático".-

Art. 2°.- Serán funciones del mismo:

a. Impulsar la adopción de aplicativos específicos y generales en el área en que ha sido designado.-
b. Actuar como nexo con la áreas de la Secretaría de Estado de Tecnologías de la Información, para coordinar con éstas, tanto la puesta en producción de aplicaciones generales, como la adopción de herramientas integrables al proyecto Autopista de la Información para aplicativos específicos.-



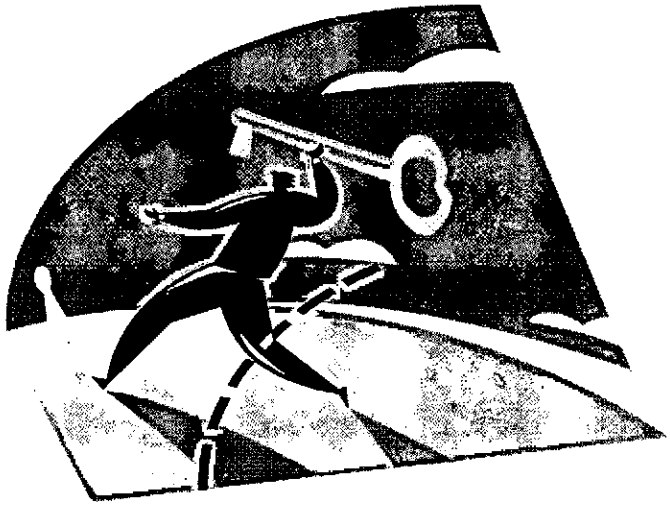
Art. 3°.-.Dicha designación deberá ser notificada a la Secretaría de Estado de Tecnologías de la Información.-

Proyecto:

"POLÍTICAS DE MITIGACIÓN DE RIESGOS"

Objetivo específico:

PREVENCIÓN Y POLÍTICAS DE SEGURIDAD



ANEXO IV

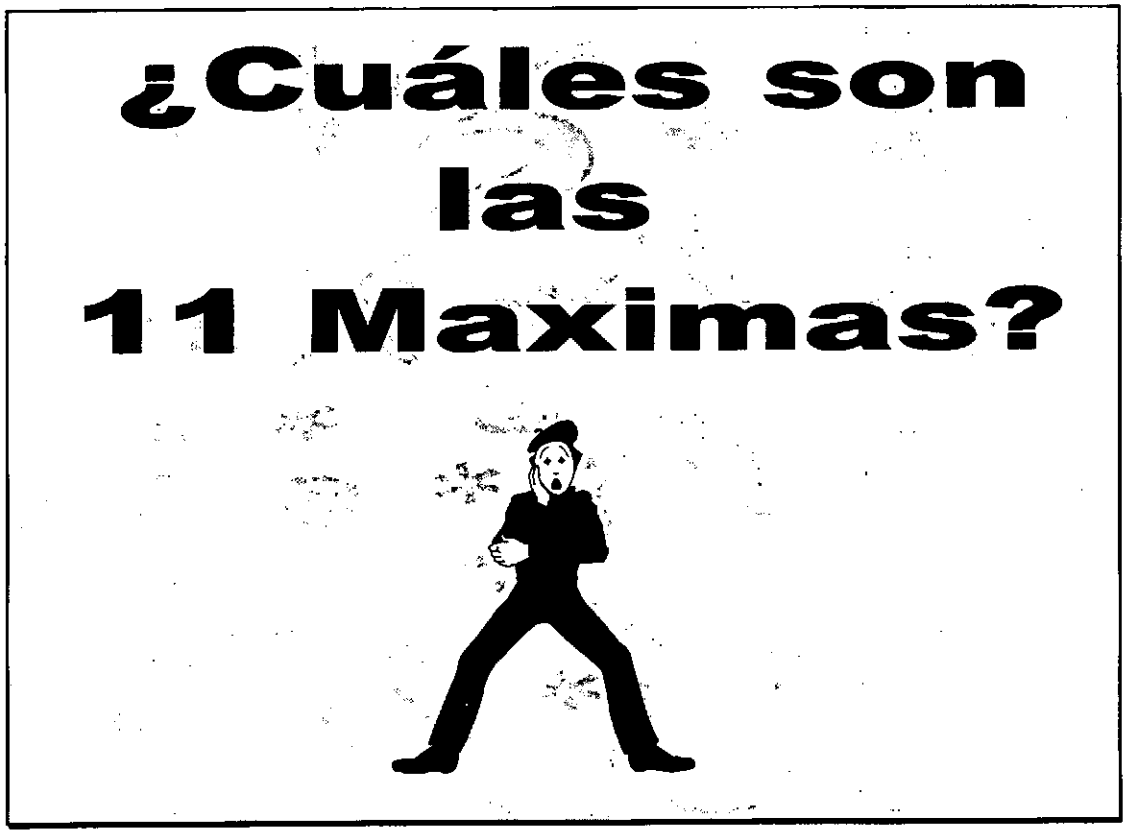
Actividad N° 7

CAMPAÑAS REALIZADAS

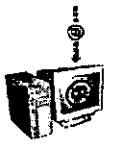
CAMPAÑAS REALIZADAS

1. Campaña sobre seguridad

- Medio utilizado: **Diapositiva, Afiche y Archivo para el envío por correo electrónico**

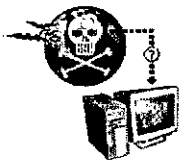


1. Utilizá ANTIVIRUS y actualizalo siempre



2. Aseguráte de que esté siempre activo

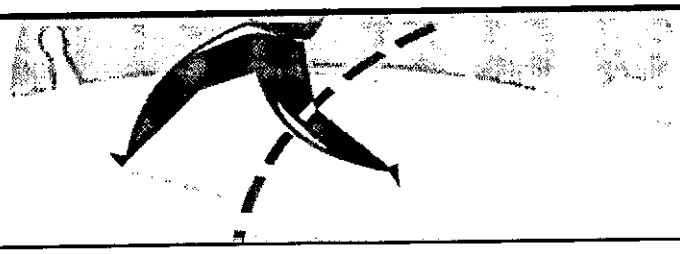
3. Usalo siempre antes de abrir los mensajes de correo electrónico



4. No descargues programas de Internet de lugares que no sean seguros

Autopista de la Información

Secretaria de Estado de Tecnología de la Información
Gerencia de Servicios San Luis



5. Analizá SIEMPRE los diskettes que vayas a utilizar en tu PC.

6. Sacá los diskettes de la PC cuando la arranques o la apagues

7. Analizá siempre el contenido de los archivos comprimidos (Zipeados)

8. Utilizá siempre las opciones de SEGURIDAD de los programas en tu PC

Autopista de la Información

Secretaria de Estado de Tecnología de la Información
Gerencia de Servicios San Luis

9. Todas las semanas, como mínimo, realizá copias de seguridad (Backup) de la información de tu PC

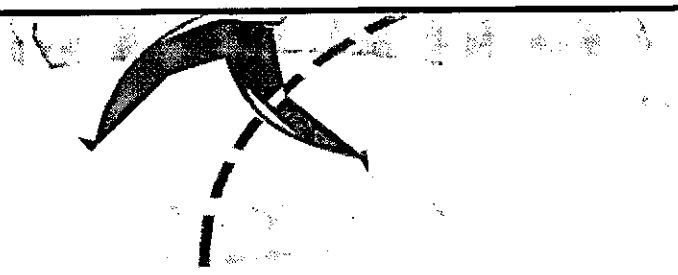
10. Mantenéte informado acerca de todas las novedades en estos temas.

11. Utilizá siempre SOFTWARE LEGAL

Para más información dirigite a la Gerencia de Servicios San Luis en el 2 piso del Edificio Administrativo, Entrada por Rivadavia o llamá al 451076 Mesa de Ayuda.

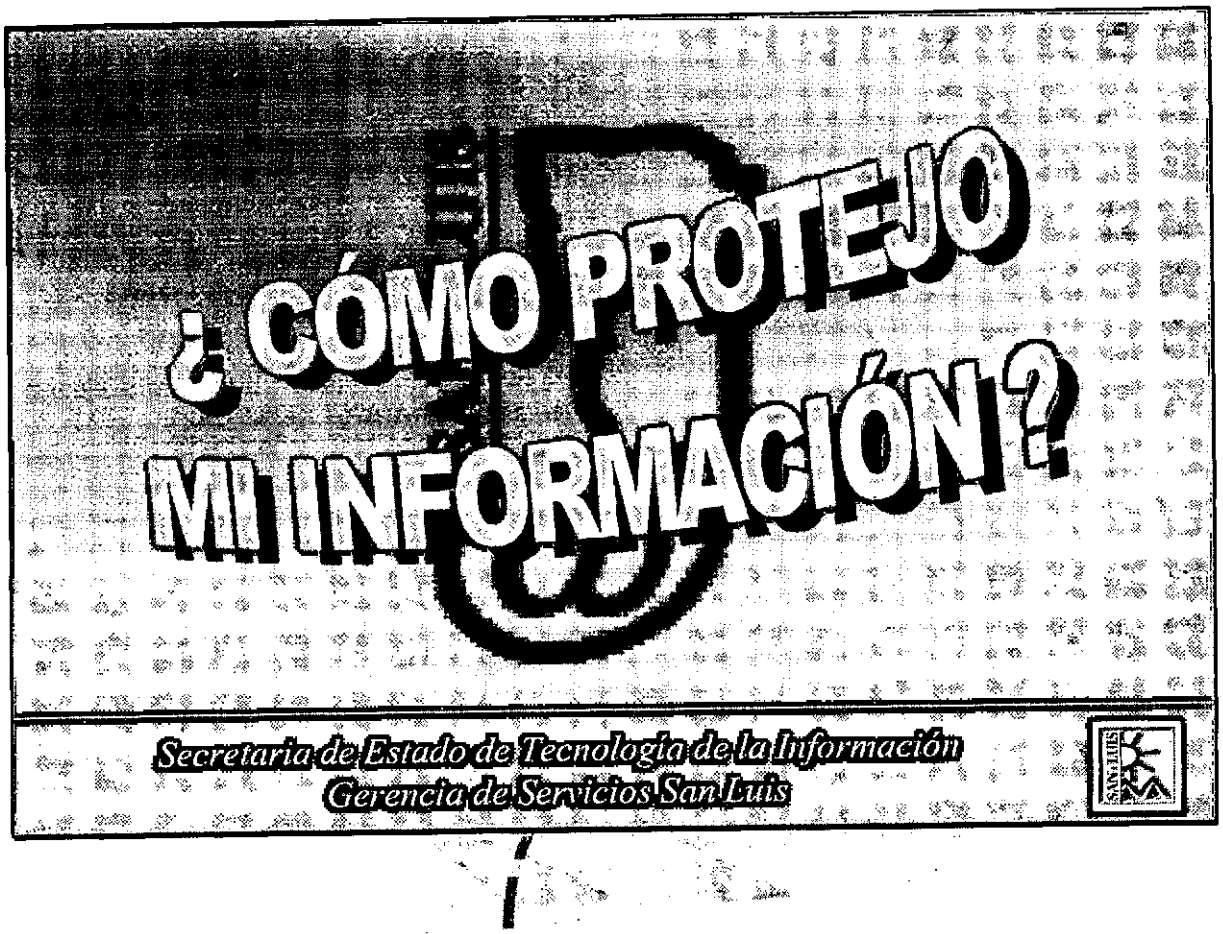
Autopista de la Información

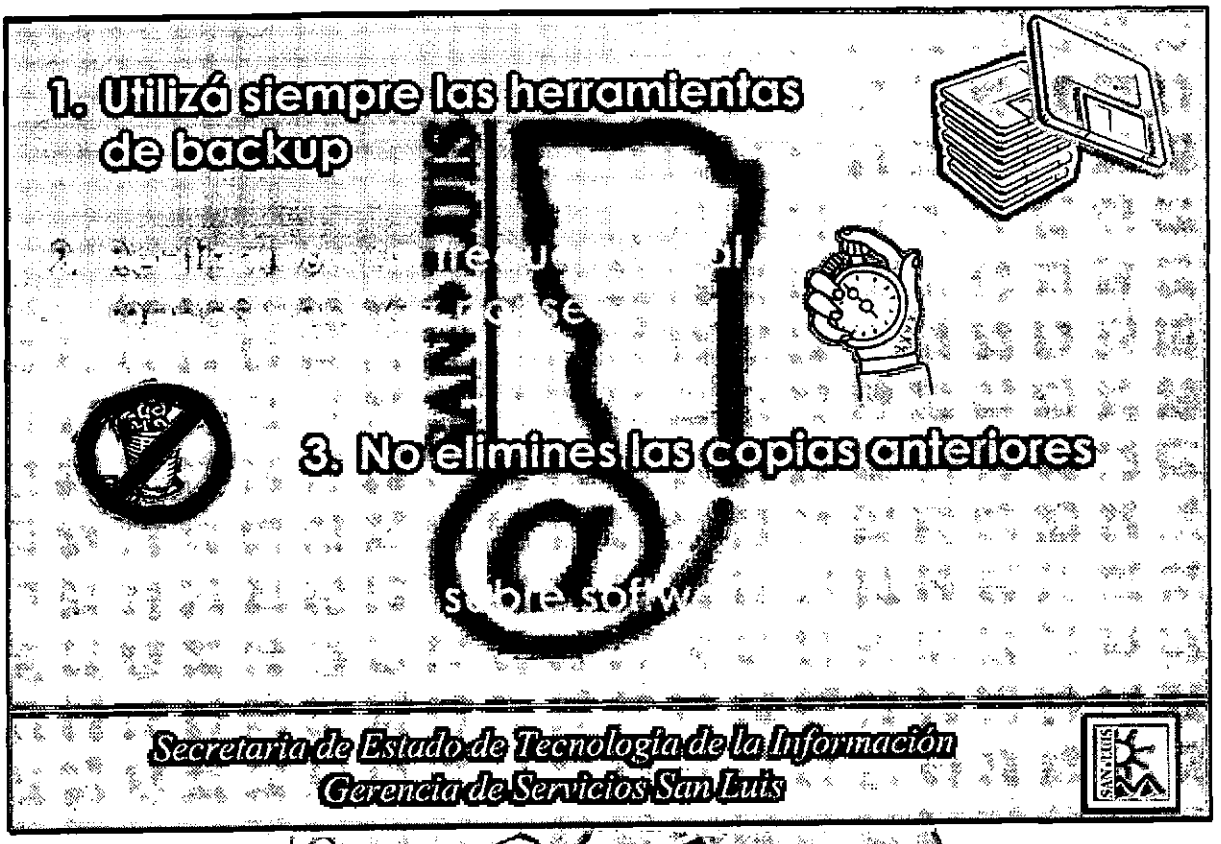
Secretaria de Estado de Tecnología de la Información
Gerencia de Servicios San Luis

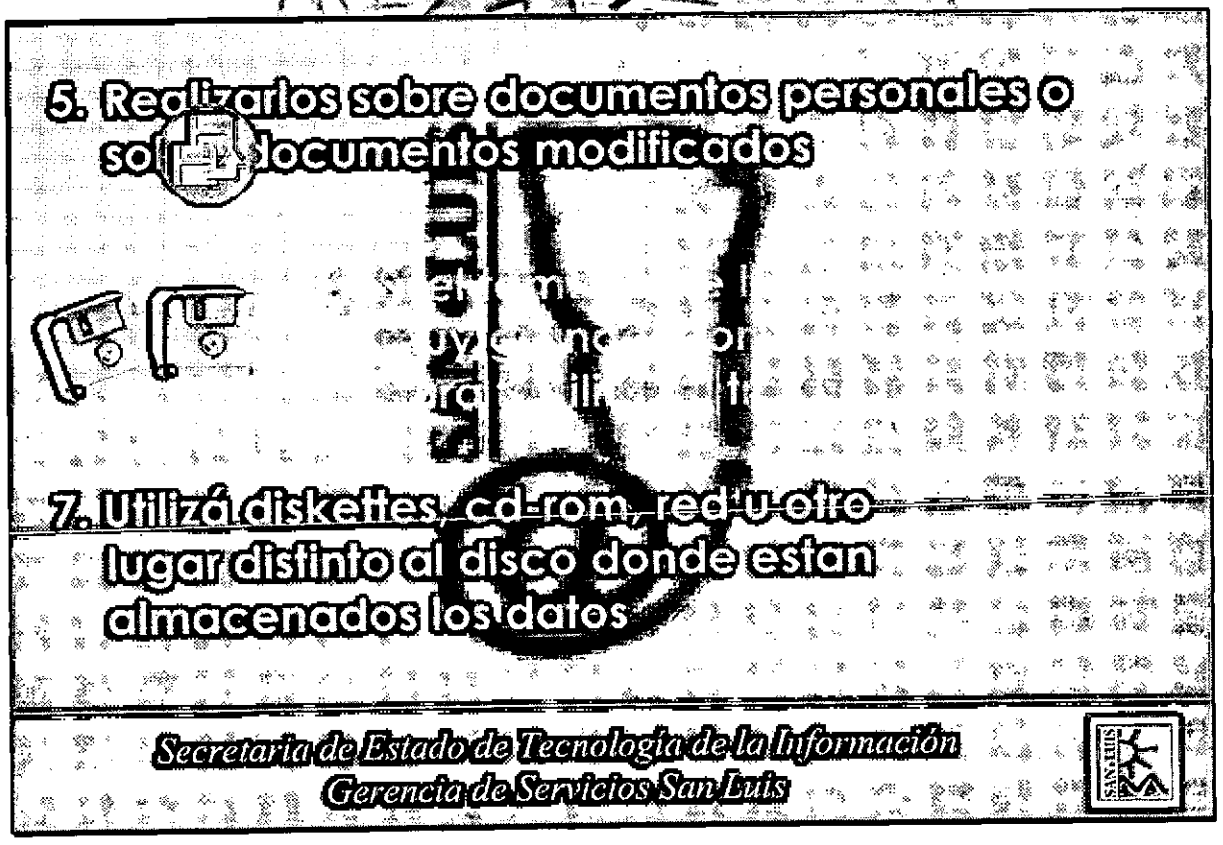


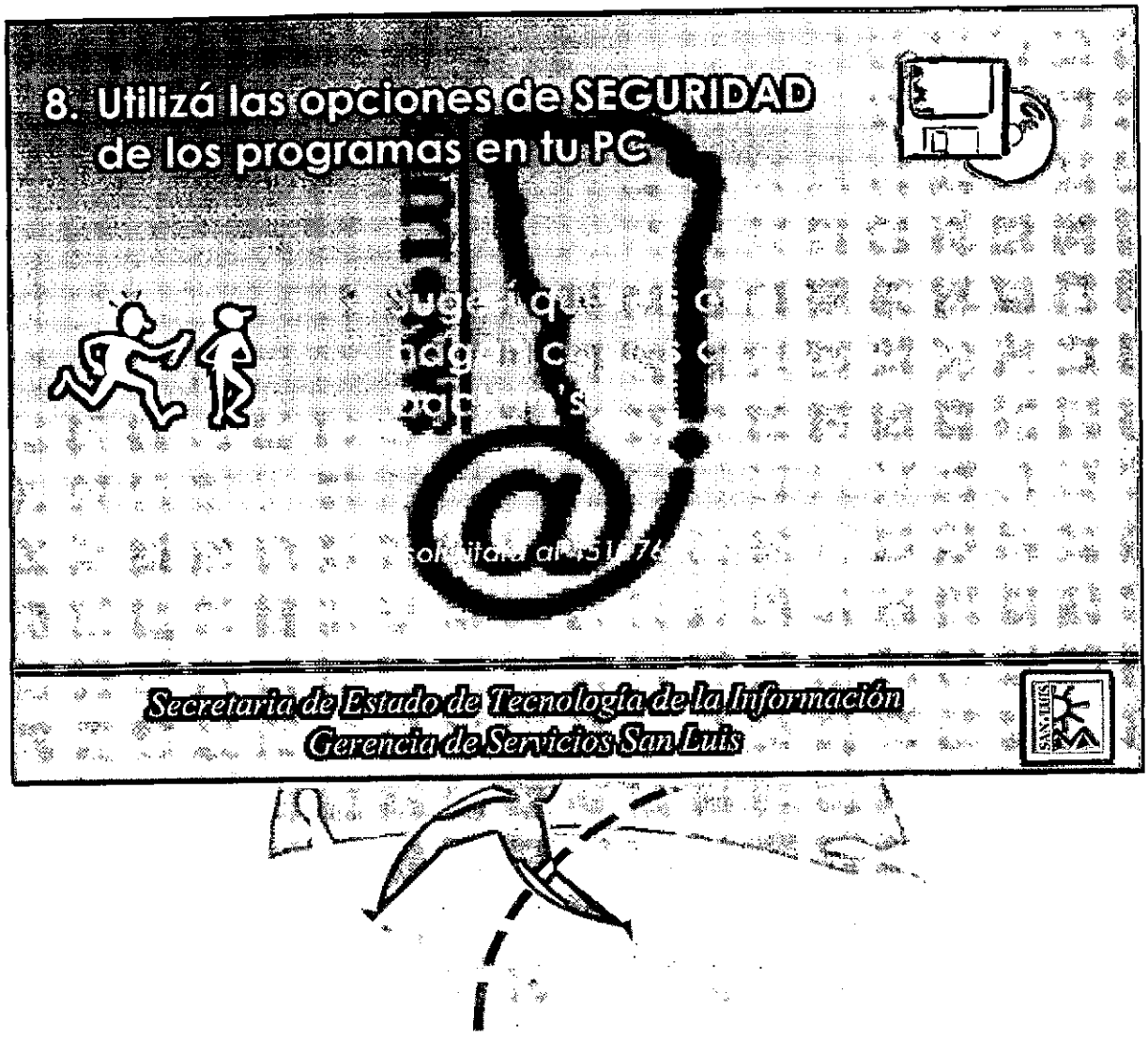
2. Campaña sobre Backup

- Medio utilizado: **Diapositiva**



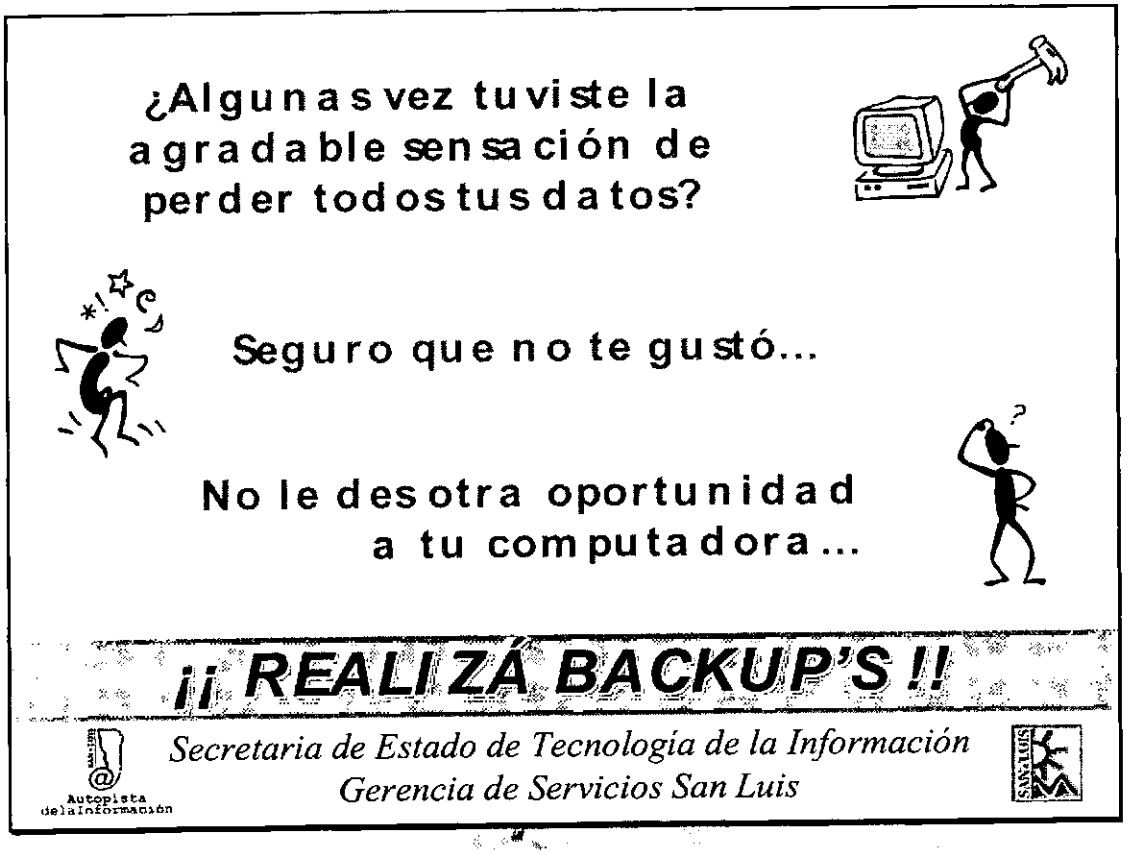

1. Utilizá siempre las herramientas de backup
3. No elimines las copias anteriores
Secretaría de Estado de Tecnología de la Información
Gerencia de Servicios San Luis


5. Realizarlos sobre documentos personales o
documentos modificados
7. Utilizá diskettes, cd-rom, red u otro lugar distinto al disco donde estan almacenados los datos
Secretaría de Estado de Tecnología de la Información
Gerencia de Servicios San Luis


8. Utilizá las opciones de SEGURIDAD
de los programas en tu PC
Secretaría de Estado de Tecnología de la Información
Gerencia de Servicios San Luis

3. Campaña sobre Backup

- Medio utilizado: **Afiche**

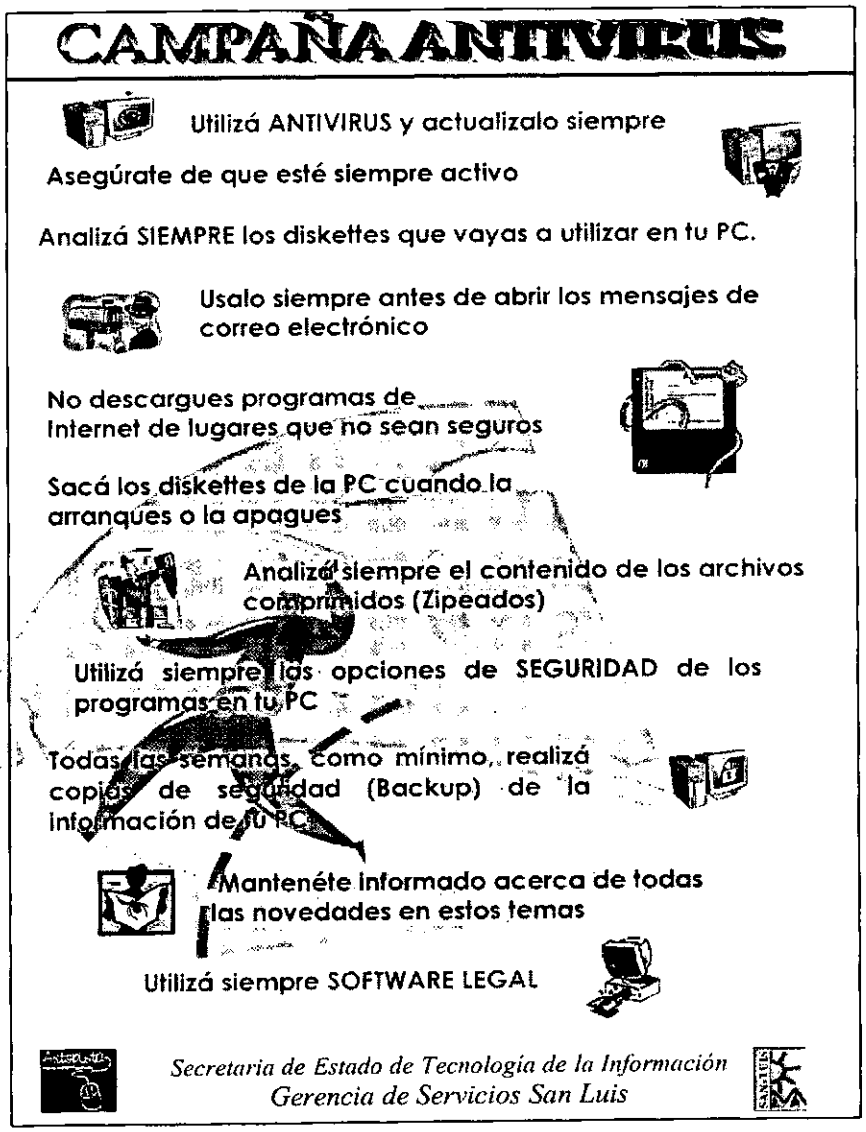


4. Campaña sobre Backup

- Medio utilizado: **Afiche**

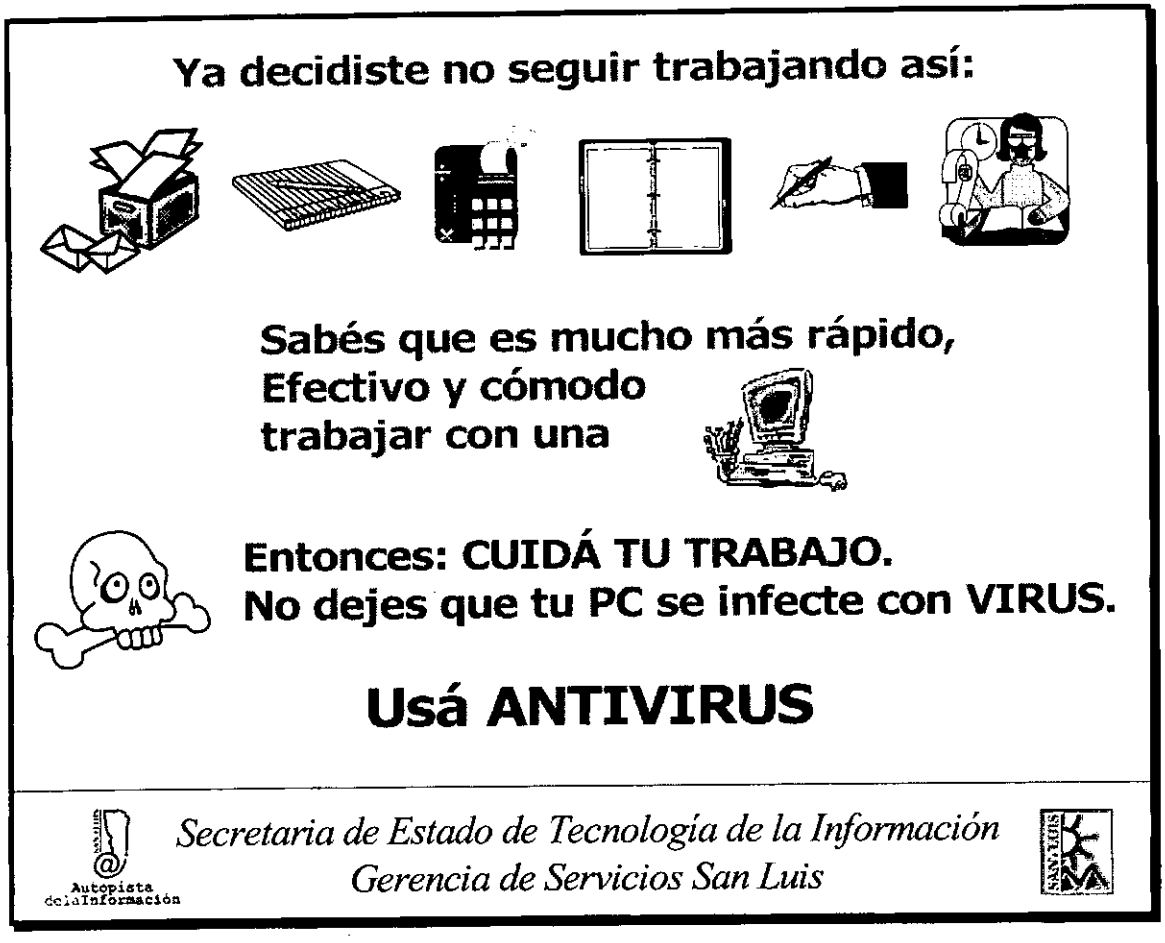
5. Campaña sobre Antivirus

- Medio utilizado: **Afiche y folleto**



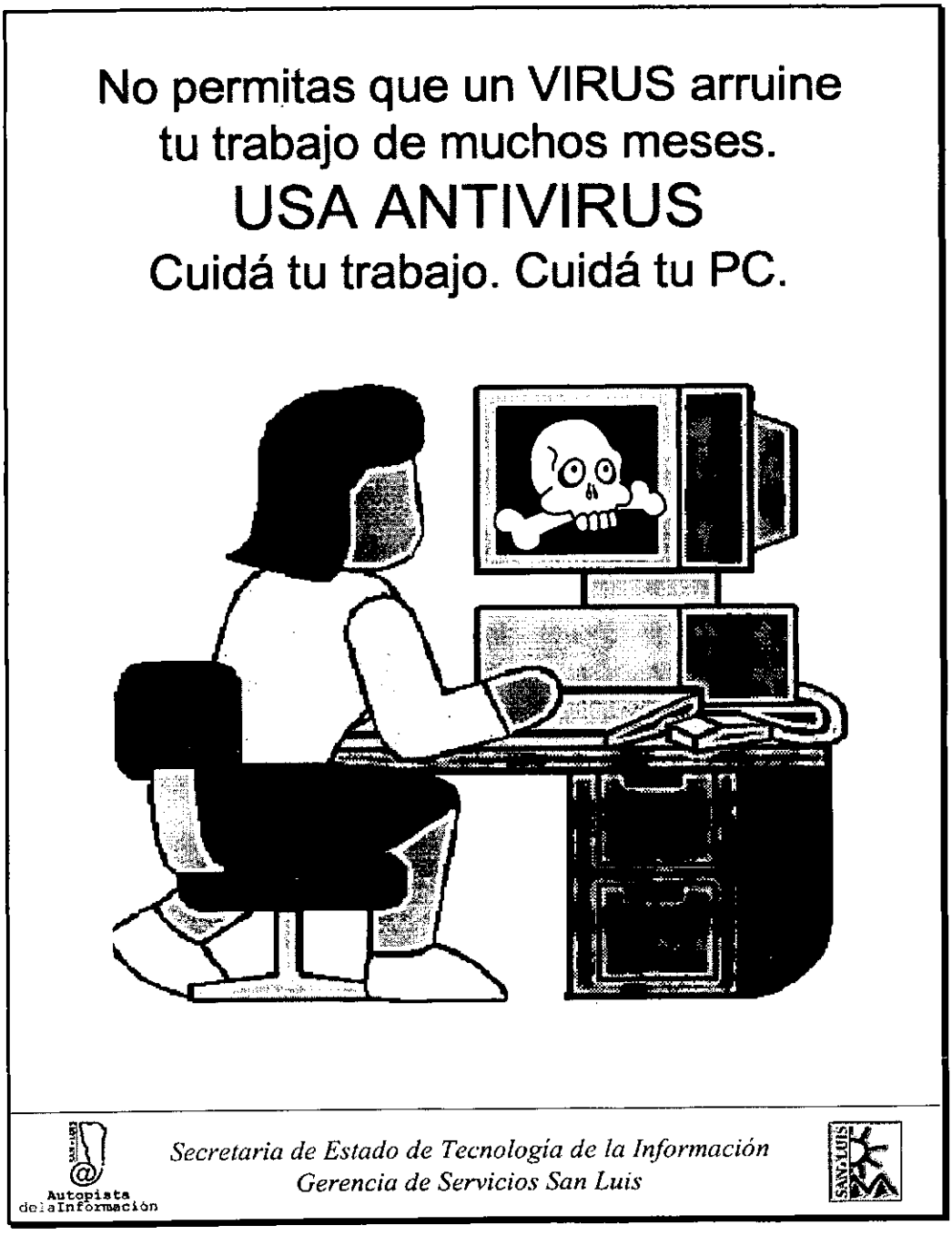
6. Campaña sobre Antivirus

- Medio utilizado: **Afiche**



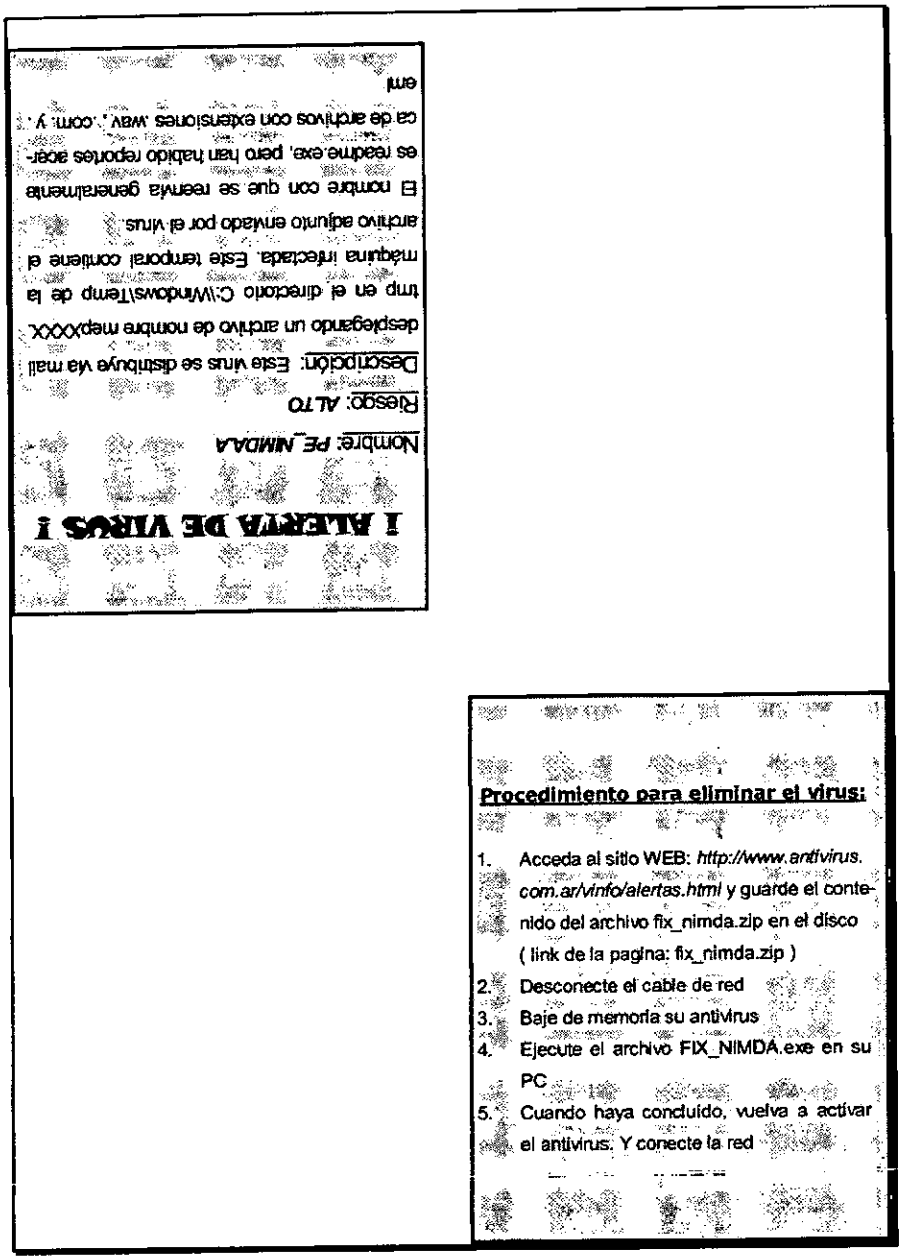
7. Campaña sobre Antivirus

- Medio utilizado: **Afiche**



8. Campaña sobre Antivirus

- Medio utilizado: **Folleto**



¡ ALERTA DE VIRUS !

Nombre: *PE_NIMDA.A*

Riesgo: *ALTO*

Descripción: Este virus se distribuye vía mail desplegando un archivo de nombre mepXXXX.tmp en el directorio C:\Windows\Temp de la máquina infectada. Este temporal contiene el archivo adjunto enviado por el virus.

El nombre con que se reenvía generalmente es readme.exe, pero han habido reportes acerca de archivos con extensiones .wav, .com, y .eml

Procedimiento para eliminar el virus:

1. Acceda al sitio WEB: *http://www.antivirus.com.ar/vinfo/alertas.html* y guarde el contenido del archivo fix_nimda.zip en el disco (link de la pagina: fix_nimda.zip)
2. Desconecte el cable de red
3. Baje de memoria su antivirus
4. Ejecute el archivo FIX_NIMDA.exe en su PC
5. Cuando haya concluido, vuelva a activar el antivirus. Y conecte la red

9. Campaña sobre Backup

- Medio utilizado: **Folleto**

BACKUP'S

¿Qué es?

Es guardar la información necesaria e importante que está en la PC e un lugar distinto, para no perderla en el caso de rotura de l computadora

Las 8 máximas:

1. Utiliza siempre las herramientas de backup
2. Realízalos con frecuencia, al menos una vez por semana
3. No elimines las copias anteriores
4. No los realices sobre software ya instalado
5. Realizarlos sobre documentos personales o sobre documentos modificados
6. Si el tamaño de la información es muy grande, comprimí los archivos para facilitar el traspaso
7. Utiliza las opciones de SEGURIDAD de los programas en tu PC
8. Sugerí que tus compañeros que hagan copias de seguridad o backup's

¿Donde realizarlos?

- Diskettes
- ZIP
- CD-ROM

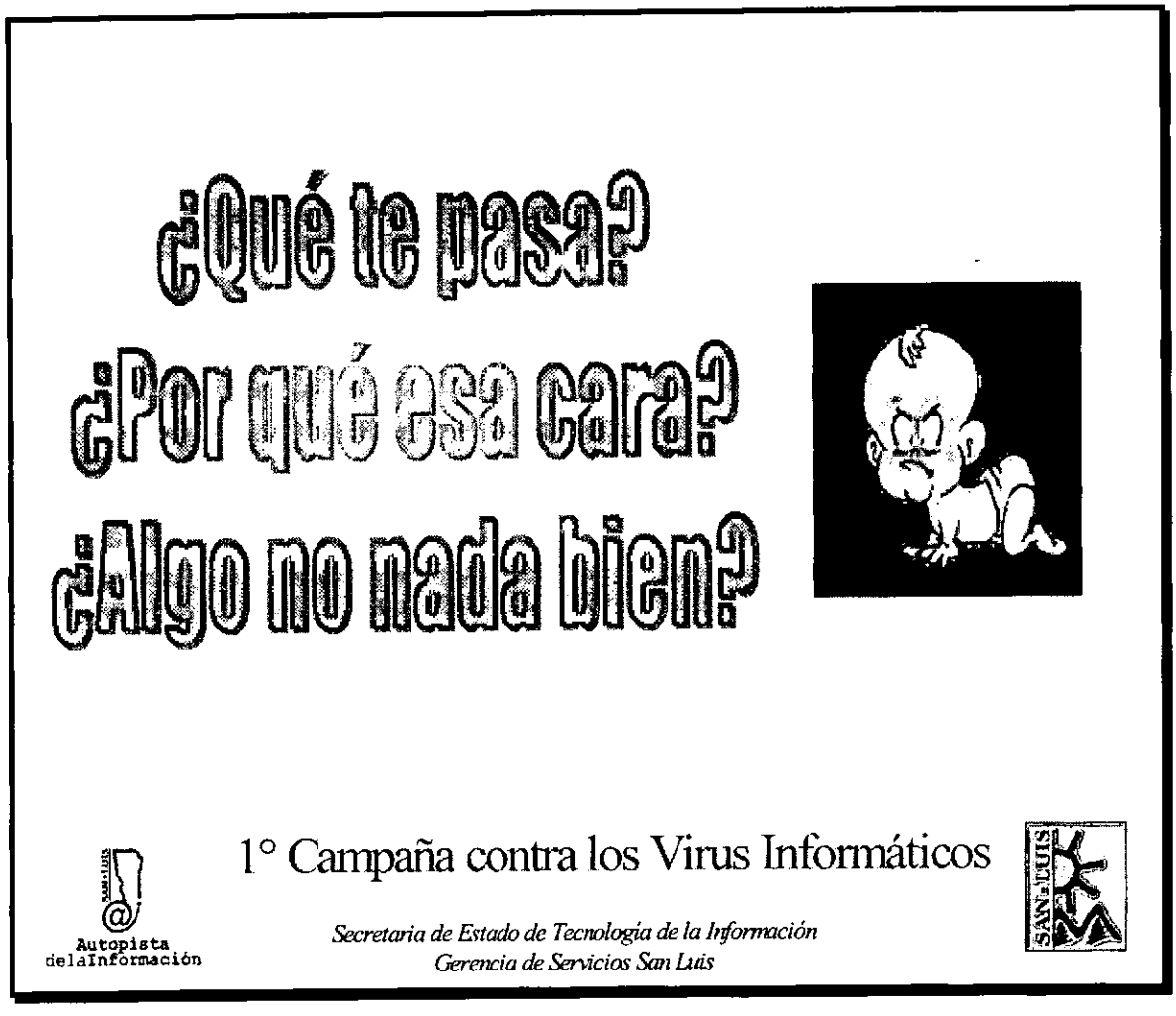
NOTA: Se recomienda utilizar el CD-ROM para realizar backup debido que los tamaños de información son demasiado grandes para utiliza Diskettes o ZIP

Formas de realizarlos

- Normal
- Comprimido

10. Campaña sobre Virus

- Medio utilizado: **Protector de pantalla**



11. Campaña sobre Virus

- Medio utilizado: **Protector de pantalla**

12. Campaña sobre Virus

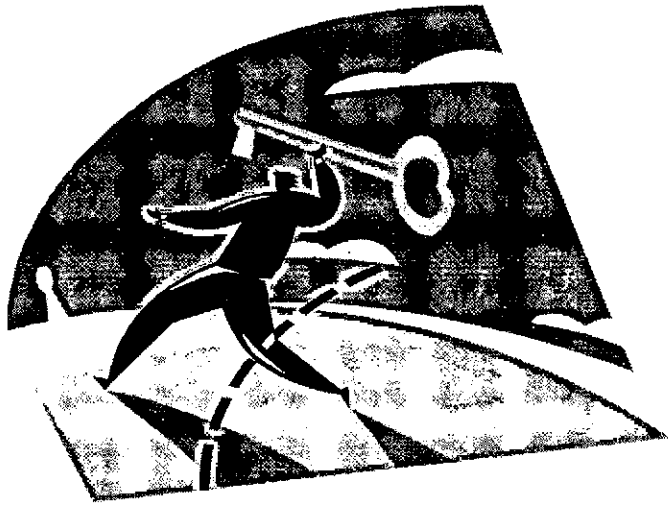
- Medio utilizado: **Protector de pantalla**

Proyecto:

"POLÍTICAS DE MITIGACIÓN DE RIESGOS"

Objetivo específico:

PREVENCIÓN Y POLÍTICAS DE SEGURIDAD



ANEXO V

Actividad N° 7

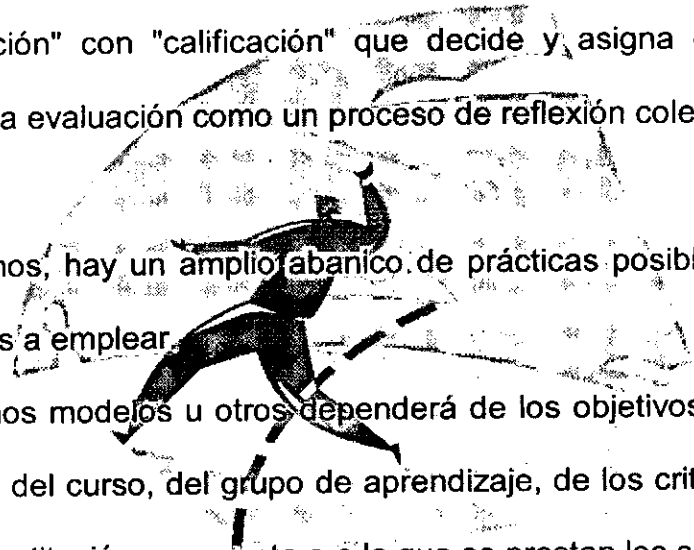
EVALUACIÓN DE LA FORMACIÓN

EVALUACIÓN DE LA FORMACIÓN

"1. EL CONCEPTO DE EVALUACIÓN EN LA FORMACIÓN

La evaluación es una parte integrante del proceso de aprendizaje, con la que se trata de verificar o comprobar en qué medida se han cumplido los diferentes objetivos de dicho proceso.

Existen distintas concepciones y prácticas de evaluación. Desde la concepción que identifica "evaluación" con "calificación" que decide y asigna el profesor, hasta la consideración de la evaluación como un proceso de reflexión colectiva de todo el grupo de aprendizaje.



Ente estos extremos, hay un amplio abanico de prácticas posibles de evaluación, de modelos y técnicas a emplear.

La elección de unos modelos u otros dependerá de los objetivos que se persigan, de las características del curso, del grupo de aprendizaje, de los criterios del profesor, de las normas de la institución que presta o a la que se prestan los servicios de formación, así como de los instrumentos de evaluación a los que se tenga acceso.

2. LA EVALUACIÓN EN EL PROCESO DE APRENDIZAJE

La evaluación puede realizarse en diferentes momentos a lo largo del proceso de aprendizaje, no solamente al final del mismo.

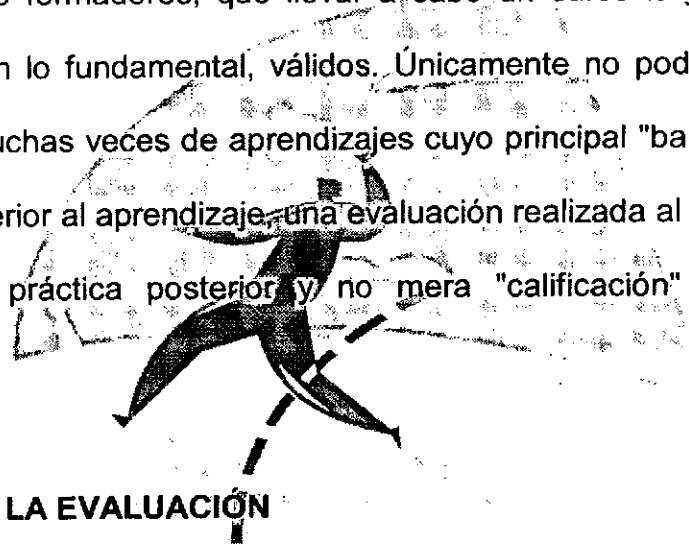
A este respecto, se pueden diferenciar tres tipos de evaluación:

- **DIAGNÓSTICA:** Nos permite conocer el nivel de conocimientos y habilidades que de entrada tienen los alumnos.

- **FORMATIVA:** Evaluación continua durante el desarrollo de la acción formativa que nos permite comprobar el grado en que los alumnos van consiguiendo los objetivos.
- **SUMATIVA:** Evaluación final del rendimiento de los alumnos.

Pues si bien es útil esta diferencia en cuanto al "cuando" de la evaluación en el proceso de aprendizaje, hemos de tener en cuenta que las condiciones de los procesos de formación con trabajadores adultos pueden hacer variar en algo estos planteamientos.

Si tenemos, como formadores, que llevar a cabo un curso largo, los criterios antes expuestos son, en lo fundamental, válidos. Únicamente no podemos perder de vista que al tratarse muchas veces de aprendizajes cuyo principal "banco de pruebas" es la práctica real posterior al aprendizaje, una evaluación realizada al final del mismo puede ser útil para la práctica posterior y no mera "calificación" del rendimiento del aprendizaje.



3. ACTORES DE LA EVALUACIÓN

El sujeto de la evaluación, es decir, quien la realiza, es uno de los datos clave que diferencia unos modelos de evaluación de otros.

La evaluación puede ser realizada por el profesor - hacia cada alumno individualmente o hacia el grupo -, por los alumnos - individualmente o en grupo -, así como puede tener lugar por parte de todo el grupo de aprendizaje - profesor y alumnos -.

Cada una de ellas son, por su alcance y contenido, diferentes:

- Hablaremos de "evaluación externa" en aquellos casos en que el docente utiliza un conjunto determinado de técnicas para evaluar la consecución de los objetivos programados, y como consecuencia de la información obtenida toma las decisiones pertinentes.

- Hablaremos de "evaluación interna" en aquellos casos en que es el propio alumno quien valora sus niveles de
- Realización, adquisición o ejecución de ciertas tareas u objetivos.

Esta división se conoce también con las denominaciones de heteroevaluación y autoevaluación, según que la evaluación la lleve a cabo una persona distinta al alumno (generalmente el profesor), o sea el alumno mismo el que la realice.

Teniendo esto en cuenta, y añadiendo la variable de si la evaluación individual o grupal, tenemos como posibles las siguientes prácticas de evaluación

Autoevaluación:	
Individual (cada sujeto evalúa su aprendizaje).	*Grupal* (el grupo, en conjunto, evalúa su proceso de aprendizaje como tal grupo).

Heteroevaluación:	
Individual (el profesor evalúa a cada sujeto).	*Grupal* (el profesor evalúa al grupo como colectivo de aprendizaje).

4. NECESIDAD DE LA EVALUACIÓN EN LA FORMACIÓN

- En el proceso de formación no se puede abordar un nuevo punto si el punto anterior no ha sido superado plenamente por los alumnos. Por tanto, el profesor precisa conocer el estado de formación de los distintos alumnos con relación a los objetivos - metas que han de alcanzar. Además esto ha de realizarse en cada momento del proceso de enseñanza para poder clasificar los contenidos a impartir de forma progresiva y segura.

- En toda acción formativa, por ser una situación de comunicación, es necesario que el profesor reciba toda la información posible de parte del alumno para poderle transmitir los contenidos con eficacia según su situación y condiciones concretas. Para esto, es necesario que conozca el grado de eficacia de sus comunicaciones, el grado de comprensión de las mismas por parte del alumno, las actitudes implicadas en ellos, etc. para que, según los datos recibidos en la "retroinformación", pueda introducir los cambios y reajustes en la función emisora.
- El profesor necesita controlar y autocontrolarse, en una acción reflexiva. Ello, para conocer sus aciertos y errores, encontrando las causas a las que se puedan atribuir tales efectos, causas que determinadas por un diagnóstico acertado, motivarán la búsqueda de las medidas correctoras oportunas.
- Es necesario conocer el grado de aprovechamiento de cada alumno, para poder emitir sobre él, un juicio objetivo y justo, con vistas a futuras acciones.
- El *conocimiento* de los resultados por el mismo alumno es autoestimulante para su participación en el aprendizaje.
- A lo largo del curso es necesario, dentro del marco de una enseñanza individualizada, detectar los alumnos con deficiencias para precisarlas y corregirlas.
- Por último, en un marco más amplio, es necesaria la evaluación para determinar la eficacia de un programa, así como de todas y cada una de las unidades que lo integran. De ellas, se obtendrán los aspectos positivos y negativos del sistema de instrucción, proporcionando los datos que permitan corregir y superar constantemente el programa.

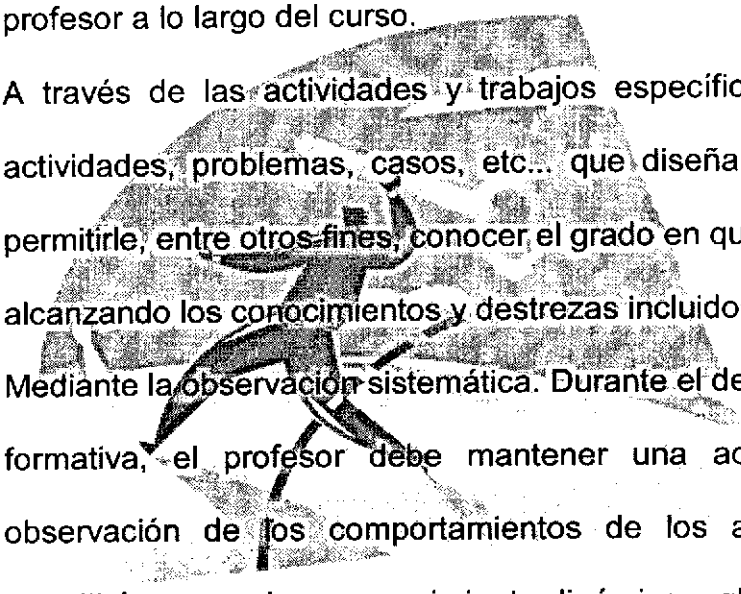
5. DESARROLLO DE LA EVALUACIÓN FORMATIVA

La **evaluación formativa** se realiza de las siguientes formas:

A. A partir de las manifestaciones espontáneas de los alumnos en el curso. Dependiendo de la calidad y la cantidad de estas intervenciones, el formador podrá valorar el grado de conocimientos y profundización en los temas de los alumnos, sus intereses y motivaciones, etc...

B. A partir de las respuestas a las preguntas de todo tipo que realiza el profesor a lo largo del curso.

C. A través de las actividades y trabajos específicos en el aula. Las actividades, problemas, casos, etc... que diseña el formador deben permitirle, entre otros fines, conocer el grado en que los alumnos están alcanzando los conocimientos y destrezas incluidos en los objetivos.



D. Mediante la observación sistemática. Durante el desarrollo de la acción formativa, el profesor debe mantener una actitud constante de observación de los comportamientos de los alumnos, lo que le permitirá conseguir un conocimiento dinámico y global de los mismos. Los requisitos de una buena observación son:

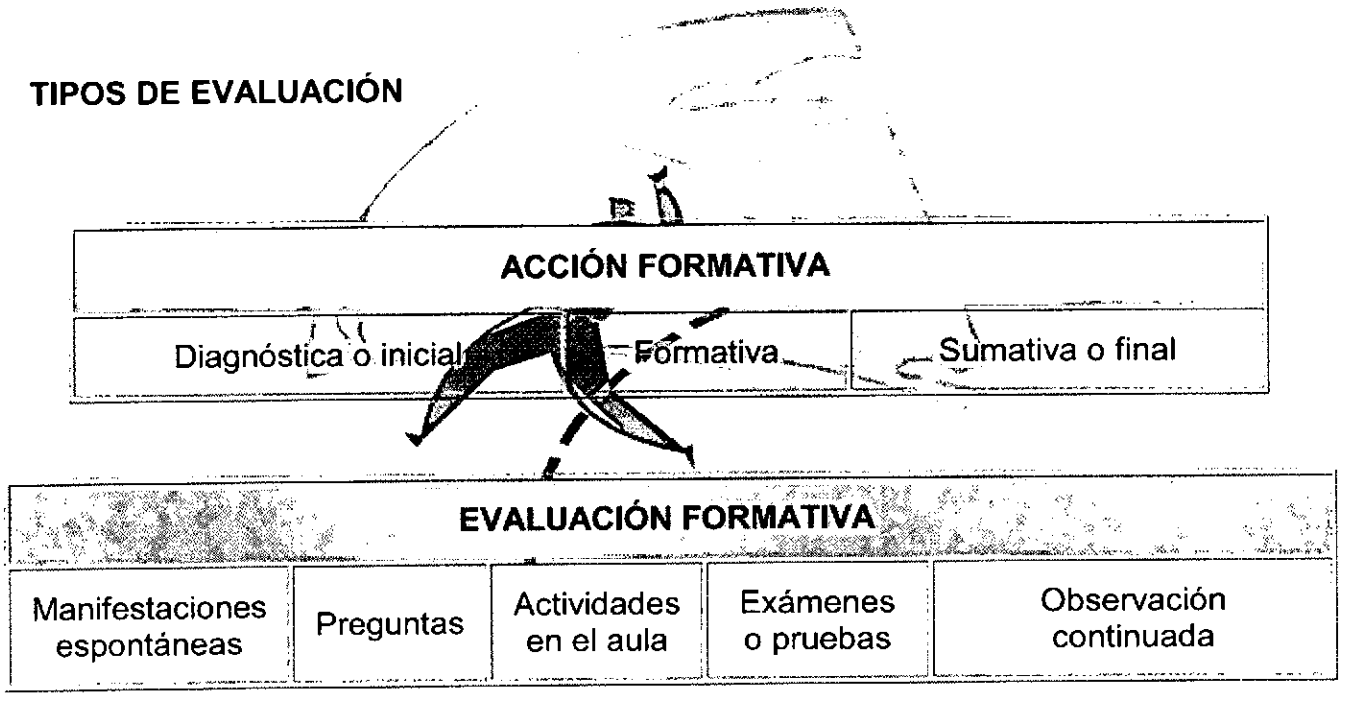
   - Ha de ser continua y sistemática.
   - Exige tiempo y un gran esfuerzo por parte del docente.
   - Planeada de antemano: el formador debe saber lo que tiene que valorar y lo que carece de importancia
   - Debe ser objetiva y, por tanto, evitar el subjetivismo, el efecto halo, el dogmatismo, el predominio de estereotipos, etc...

E. Mediante la realización de exámenes o pruebas (periódicas, prácticas, objetivas, etc...)

La evaluación formativa permite:

- Comprobar el logro de los objetivos planeados y determinar las causas de lo no planeado.
- Realimentar y modificar el programa sobre la marcha.
- Mantener el interés constante por cada alumno y la preparación continua de las clases.
- Obtener información y datos que no se pueden conseguir en la evaluación final.

TIPOS DE EVALUACIÓN



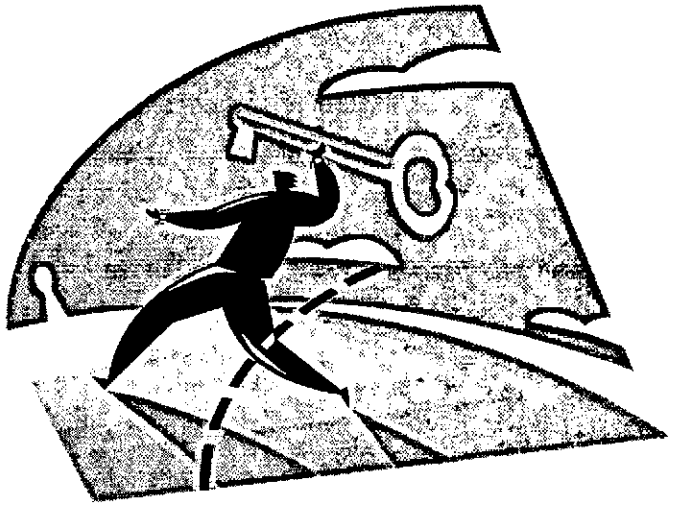
Información publicada en el Ministerio de Administraciones Publicas de España en la dirección de Internet: *www.map.es/csi/caibi/ibfm/pedagogia/documento8.html*

Proyecto:

"POLÍTICAS DE MITIGACIÓN DE RIESGOS"

Objetivo específico:

PREVENCIÓN Y POLÍTICAS DE SEGURIDAD



ANEXO VI

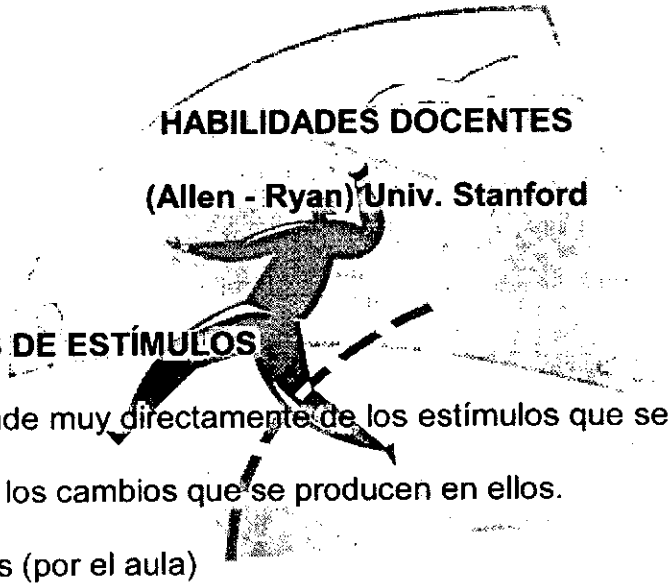
Actividad N° 7

HABILIDADES DOCENTES EN LA IMPARTICIÓN DE UNA CLASE

HABILIDADES DOCENTES EN LA IMPARTICIÓN DE UNA CLASE

"En cualquier tipo de relación entre profesor y alumnos, se ponen en juego tres factores esenciales:

- Seguridad científica del docente
- Transparencia didáctica
- Cercanía emocional entre docente y discentes



1 - VARIACIONES DE ESTÍMULOS

La atención depende muy directamente de los estímulos que se reciben, pero no de su intensidad sino de los cambios que se producen en ellos.

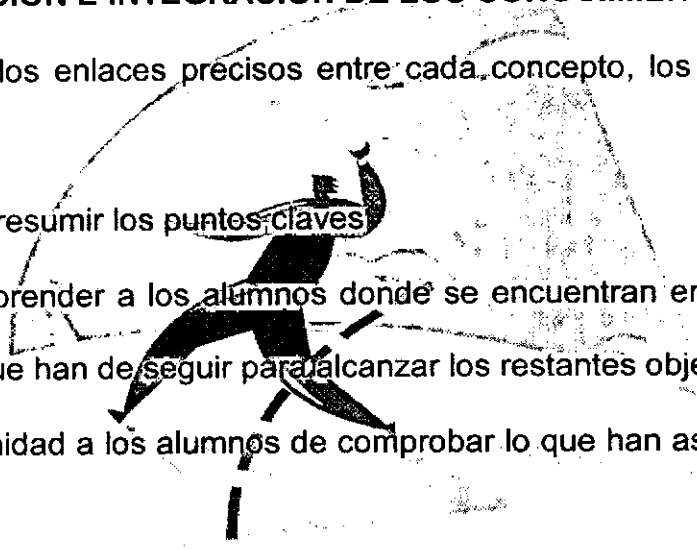
A. Movimientos (por el aula)
B. Gestos (expresividad y dinamismo)
C. Focalizaciones (sobre un punto, concepto ...)
D. Interacciones (profesor - alumno; profesor - grupo; alumno - alumno)
E. Pausas (silencios)
F. Cambios de canales sensoriales (oral - visual ...)

2 - SENSIBILIZACIÓN COMO TÉCNICA INTRODUCTIVA

A. Lograr nivel de atención suficiente
B. Creación de clima de interés y expectación por el tema

- Presentar de forma clara y precisa los objetivos que deben ser logrados en la sesión.
- Breve recapitulación de la lección anterior o materia que ha de servir de soporte a lo que se explicará a continuación
- Recurrir a lo anecdótico
- Presentar problemas o experiencias motivadores

3 - RECAPITULACIÓN E INTEGRACIÓN DE LOS CONOCIMIENTOS



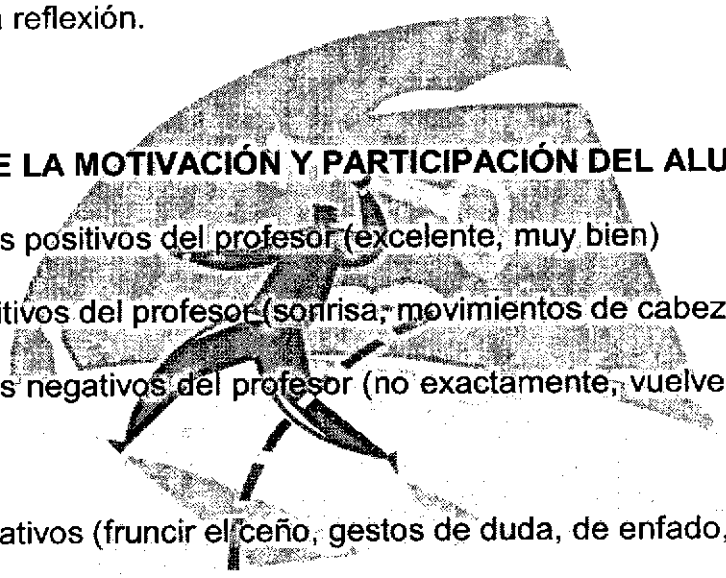
- Establecer los enlaces precisos entre cada concepto, los anteriores y los que seguirán.
- Destacar y resumir los puntos claves
- Hacer comprender a los alumnos donde se encuentran en cada momento y la dirección que han de seguir para alcanzar los restantes objetivos
- Dar oportunidad a los alumnos de comprobar lo que han asimilado y valorar sus logros
- Al finalizar la lección o al considerar logrados los objetivos parciales en el transcurso de la misma, deben realizarse estas recapitulaciones

4 - USO DEL SILENCIO E INDICACIONES NO VERBALES

- El silencio tiene un extraordinario poder para captar la atención, crear expectación, favorecer la reflexión y obligar a hablar.
- El uso del silencio se complementa con el recurso gestual que suple con ventaja, en ocasiones, a la palabra.
- Los puntos no verbales pueden ser:
    - Faciales: sonrisa, fruncir el ceño, etc...

- Movimientos de cuerpo: dirigiéndote a un alumno, etc...
- Movimientos de cabeza: de afirmación, negación, duda, etc...
- Gestos con las manos: indicando a un alumno que debe responder, continuar, escuchar, etc...

- El uso del silencio e indicaciones no verbales constituye un recurso que debidamente complementado con otros como la formulación de preguntas, tiene como finalidad lograr una mayor participación de los alumnos a la vez que dar ocasión a la reflexión.



5 - REFUERZO DE LA MOTIVACIÓN Y PARTICIPACIÓN DEL ALUMNO

A. Comentarios positivos del profesor (excelente, muy bien)
B. Gestos positivos del profesor (sonrisa, movimientos de cabeza)
C. Comentarios negativos del profesor (no exactamente, vuelve a reflexionar sobre ello, etc...)
D. Gestos negativos (fruncir el ceño, gestos de duda, de enfado, etc...)

NOTA:

Tan peligroso es abusar de los refuerzos, positivos o negativos, como no incluirlos en nuestro repertorio verbal o gestual.

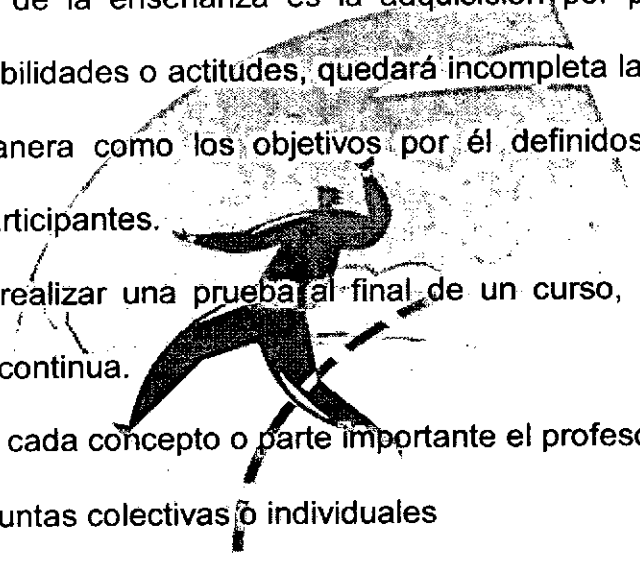
6 - SECUENCIALIDAD

A. Ordenar los conceptos de modo que cuando aparezca uno nuevo, los alumnos sean capaces de dar el "salto" que su asimilación exige.
B. Evitar a toda costa los "saltos atrás" que provocan la desconexión con la marcha del tema.

C. Evitar "saltos paralelos" interrumpiendo la explicación para comentar aspectos no específicos del tema. En caso de precisar, para el desarrollo de la lección, otros datos o conceptos, deben ser presentados a priori y establecer clara la separación y diferenciación entre estos y el tema de estudio. Una vez comenzada la lección debe ser explicada sin disgresiones.

7 - CONTROL DE LA COMPRENSIÓN

Si el fin esencial de la enseñanza es la adquisición por parte de los alumnos de conocimientos, habilidades o actitudes, quedará incompleta la acción del profesor si no comprueba la manera como los objetivos por él definidos son alcanzados por la totalidad de los participantes.



No es suficiente realizar una prueba al final de un curso, sino que es precisa una retroalimentación continua.

Tras el estudio de cada concepto o parte importante el profesor puede.

- Hacer preguntas colectivas o individuales
- Proponer la aplicación y reflexión sobre ejemplos o problemas, comprobando como son resueltos
- Pidiendo que descubran las situaciones de la vida real en que esos conceptos tienen validez o aplicabilidad...

Con esto se consigue:

- Provocar la reflexión de los alumnos respecto a los puntos más importantes
- Estimular la participación e imprimir un mayor dinamismo en clase

El control con fines evaluadores tendría otros objetivos muy distintos y un tratamiento diferente. En la situación de clase el alumno debe expresarse con toda libertad para

que la retroacción señalada sea eficaz. Por ello es conveniente diferenciar perfectamente las acciones de control de la comprensión, de las de evaluación. "

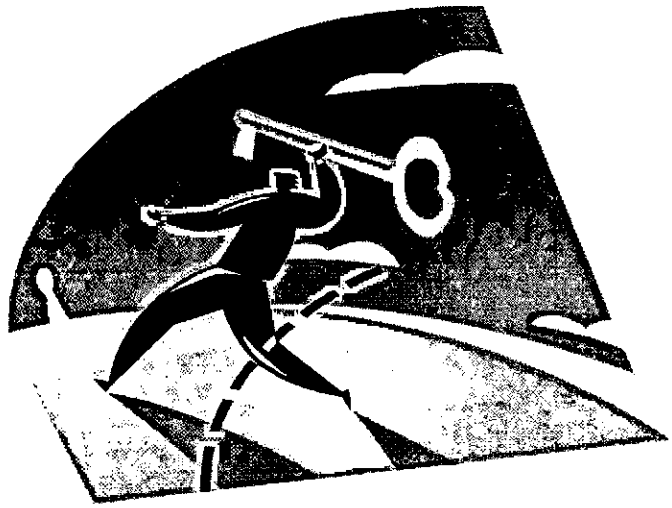
Información publicada en el Ministerio de Administraciones Publicas de España en la dirección de Internet: www.map.es/csi/caibi/ibfm/pedagogia/documento5.html

Proyecto:

"POLÍTICAS DE MITIGACIÓN DE RIESGOS"

Objetivo específico:

PREVENCIÓN Y POLÍTICAS DE SEGURIDAD



ANEXO VII

Actividad N° 7

EL LENGUAJE VERBAL Y NO VERBAL

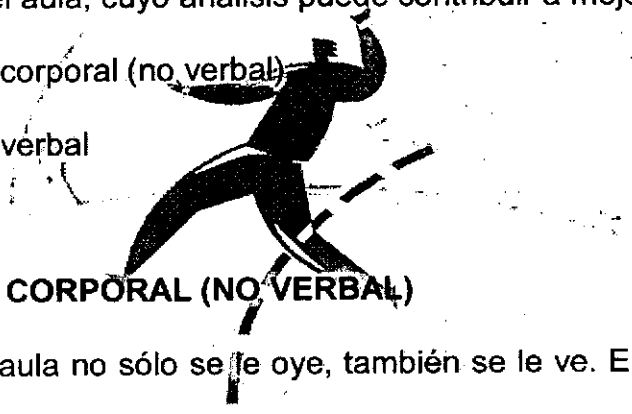
EL LENGUAJE VERBAL Y NO VERBAL

"Hablar ante un grupo de personas con naturalidad y soltura no es una tarea fácil.

No es suficiente con emplear los términos y recursos del lenguaje coloquial, sino que se hace necesario utilizar una serie de estrategias que refuerzan y complementan nuestro mensaje, al mismo tiempo que atraen y mantienen la atención de los interlocutores.

A continuación se desarrollan algunos de los elementos que intervienen en la comunicación en el aula, cuyo análisis puede contribuir a mejorarla:

1. El lenguaje corporal (no verbal)
2. El lenguaje verbal



1. EL LENGUAJE CORPORAL (NO VERBAL)

Al formador en el aula no sólo se le oye, también se le ve. En ocasiones, lo que se ve ayuda y refuerza lo que se dice, pero no siempre es así. A veces, el docente realiza una serie de gestos que no tienen sentido en el conjunto del mensaje y que dificultan o distraen la comunicación.

> Por ejemplo: mover en exceso las manos y los brazos puede llegar a marear al público. Por el contrario, tener todo el tiempo las manos en los bolsillos transmite una sensación de aburrimiento.

Muchos de estos hábitos gestuales y posturas no obedecen a un objetivo determinado, sino que en la mayoría de las ocasiones ocultan el temor y la tensión que provoca hablar ante un público.

El lenguaje del cuerpo debe servir para establecer y conservar el contacto con el auditorio, empleando todos aquellos recursos que lo favorecen y evitando lo que puede perturbarlo.

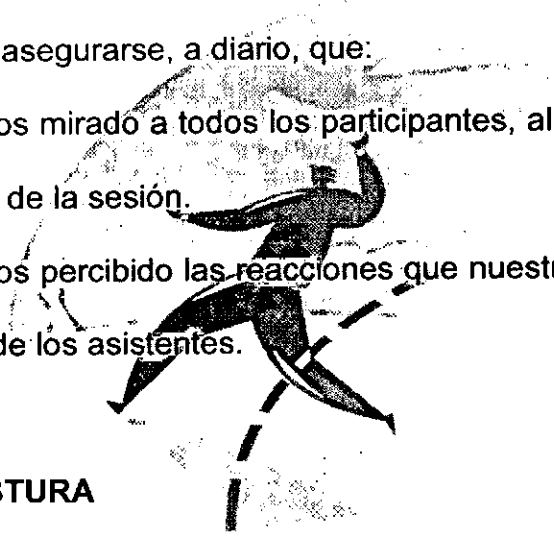
1.1 LA MIRADA

El contacto visual se establece antes que el auditivo.

Es importante mirar a todo el grupo antes de empezar a hablar y a lo largo de las sesiones de formación.

Ello implica asegurarse, a diario, que:

a. Hemos mirado a todos los participantes, al menos en alguna ocasión a lo largo de la sesión.
b. Hemos percibido las reacciones que nuestras palabras provocan en cada uno de los asistentes.



1.2 LA POSTURA

La postura que se adopte debe estar de acuerdo con lo que queremos decir.

Esta postura debe ser.

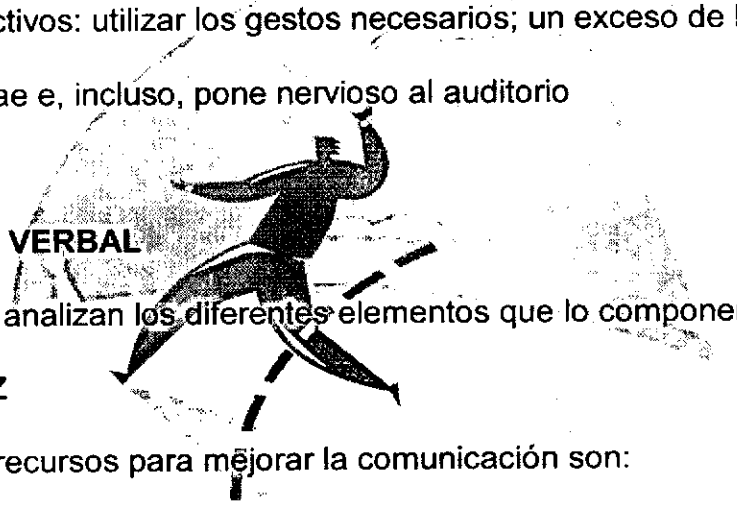
- natural: el formador debe sentirse cómodo, sin forzar posturas que le causen tensión, lo que captaría rápidamente el grupo.
- variable: mantener una misma postura todo el tiempo (por ejemplo: permanecer sentados detrás de la mesa durante varias horas) puede resultar monótono, o indicar falta de flexibilidad o apertura.
- respetuosa con el grupo, aunque exista confianza.

1.3 LOS GESTOS

Los gestos acompañan a la expresión verbal. Expresamos con todo nuestro cuerpo pero fundamentalmente con las manos, rostro, brazos, cabeza y hombros.

Los gestos deben ser.

- visibles: no esbozados sino realizados en su integridad para que puedan ser percibidos íntegramente por los alumnos.
- amplios: porque estamos ante un grupo de personas y debemos asegurarnos que todos los captan.
- selectivos: utilizar los gestos necesarios; un exceso de los mismos satura, distrae e, incluso, pone nervioso al auditorio



2. EL LENGUAJE VERBAL

A continuación se analizan los diferentes elementos que lo componen:

2.1 LA VOZ

- Los recursos para mejorar la comunicación son:
- Hablar con voz clara y fuerte.
- Vocalizar y pronunciar adecuadamente.
- No bajar la intensidad al final de las frases porque pierden significado.

2.2 RESPIRACIÓN

Conviene respirar con frecuencia mientras se habla. Para conseguirlo, es importante no utilizar frases demasiado largas, y realizar pausas y silencios a lo 1argo de la locución.

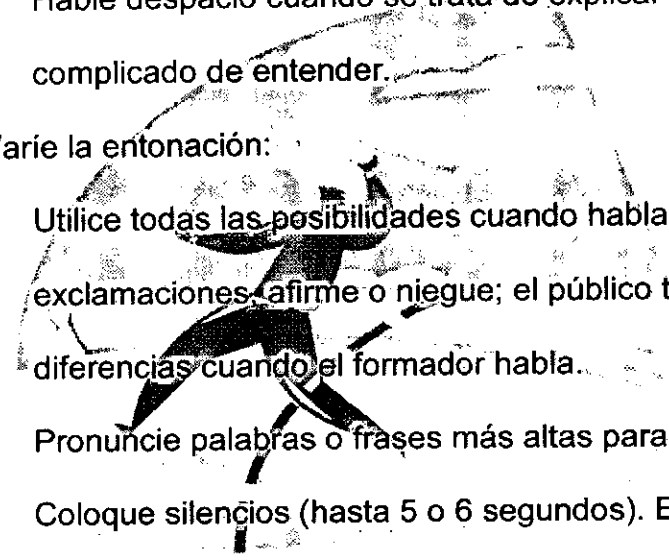
2.3 LOCUCIÓN

Atraiga la atención mientras se habla,

Se trata, ante todo, de romper la monotonía y hacer que el auditorio se interese por lo que se está diciendo.

Recursos:

1. Cambie el ritmo del discurso:
   - Si la atención del grupo disminuye, hable más deprisa o más lentamente.
   - Hable despacio cuando se trata de explicar algo difícil o complicado de entender.
2. Varíe la entonación:
   - Utilice todas las posibilidades cuando habla: interrogue, haga exclamaciones, afirme o niegue; el público tiene que captar estas diferencias cuando el formador habla.
   - Pronuncie palabras o frases más altas para atraer la atención.
   - Coloque silencios (hasta 5 o 6 segundos). Estos silencios tienen la finalidad de:
     - Dejar que los alumnos asimilen lo que acaban de oír, relajando un poco la atención.
     - Llamar la atención de los participantes.
     - Permitir al formador organizar sus ideas.



2.4 VOCABULARIO

El lenguaje debe adaptarse al grupo de alumnos.

Características:

- *variado*: rico en términos, con sinónimos y sin caer en frases hechas y tópicos.
- *preciso*: utilizar los términos adecuados para cada cosa, explicándolos cuando sean desconocidos para los alumnos.
- *adaptado*: al auditorio, con empleo de términos comunes pero sin caer en la vulgaridad o en la pedantería.

2.5 ESTILO

Es la manera personal de expresarse.

Características :

- natural : coloquial.
- estilo periodístico: frases cortas y concisas.
- personal: cada docente tiene que desarrollar con el tiempo un estilo propio de expresión, de acuerdo con su personalidad"

Información publicada en el Ministerio de Administraciones Publicas de España en la dirección de Internet: *www.map.es/csi/caibi/ibfm/pedagogia/documento6.htm*