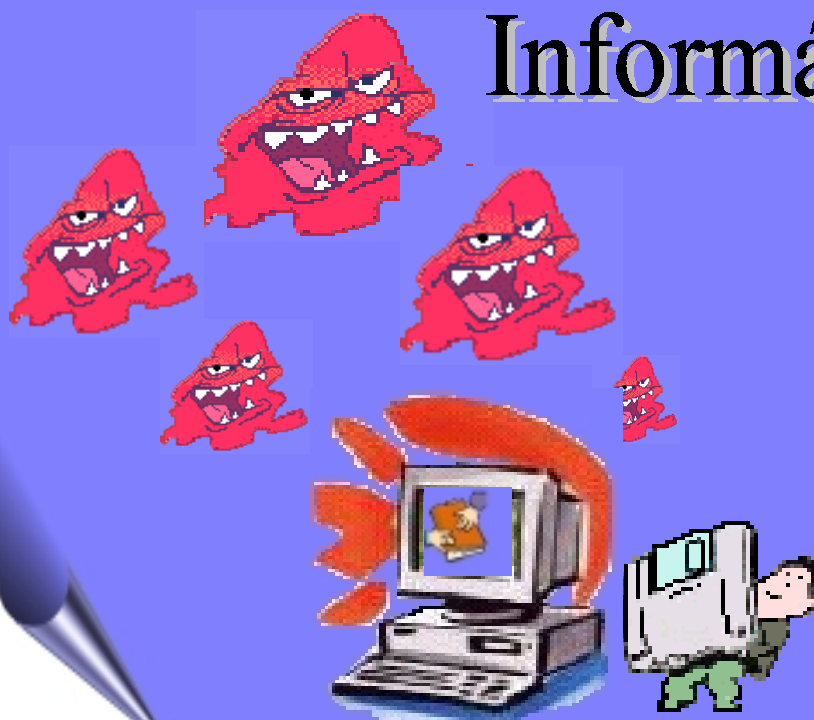




Instituto Nacional de Estadística e Informática
Sub - Jefatura de Informática

Auditoría para la Seguridad Informática



Colección Informática Fácil

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA^o

Elaborado por: SUB-JEFATURA DE INFORMATICA

Dirección Técnica de Desarrollo Informático.

Teléfono : 433-4223 - Anexos 181 - 315

TeleFax : 433-5568

Web : WWW.INEI.GOB.PE

Mail : POSTMAST@INEI.GOB.PE

Impreso en los Talleres de la Oficina de Impresiones de la Oficina Técnica de Difusión Estadística y Tecnología Informática del Instituto Nacional de Estadística e Informática (INEI)

Edición : 350 Ejemplares

Domicilio, Redacción y Talleres : Av. Gral. Garzón N° 658 - Jesús María

Orden : N° 912 - 99 - OI -OTDETI - INEI

Presentación

El Instituto Nacional de Estadística e Informática (INEI), como ente rector del Sistema Nacional de Informática, continuando con la publicación de la Colección «Informática Fácil», presenta su cuadrigésimo número titulado: « Auditoría para la Seguridad Informática ».

Los diferentes lectores, que buscan conocer conceptos sobre Los Virus y la Auditoría para la Seguridad Informática, tendrán a su alcance en esta publicación, la posibilidad de descubrir los conceptos fundamentales, además de poder ayudar a organizar el trabajo de los especialistas que se dediquen a la seguridad de la información.

El Instituto Nacional de Estadística e Informática INEI, pone a disposición de toda la Administración Pública y la sociedad en su conjunto, la presente colección de “Informática Fácil”.

Econ. Félix Murillo Alfaro
Jefe

INSTITUTO NACIONAL DE
ESTADISTICA E INFORMATICA

Indice

- LOS VIRUS Y LA AUDITORIA PARA LA SEGURIDAD INFORMATICA

Introducción.....	7
Historia.....	7
Amenazas.....	9
Pérdidas.....	9
Nuevos Riesgos.....	9

- AUDITORIA A LA SEGURIDAD INFORMATICA

Concepto	11
Objetivo.....	11
Funciones.....	11
¿A quiénes se realiza la Auditoría?.....	12
Etapas.....	12
Informe Conclusivo de los Resultados de la Auditoría.....	15

- CUESTIONARIO PARA LA AUDITORIA A LA SEGURIDAD INFORMATICA

Cuestionario Nro. 1.....	17
Cuestionario Nro. 2.....	28

- ANEXOS

Panda Software International

Firewalls- Seguridad Concentrada.....	37
Backups: Copias de Seguridad esenciales.....	38
Passwords, el primer punto a proteger.....	40
Seguridad Unix para usuarios Windows.....	42
Informe sobre la seguridad informática en las empresas.....	44
7,600 millones de dólares en pérdidas causadas por los virus	45

- BIBLIOGRAFIA

LOS VIRUS Y LA AUDITORIA PARA LA SEGURIDAD INFORMATICA

Introducción

Actualmente vemos cómo el avance de las tecnologías de la información han incrementado las pérdidas relacionadas con la Seguridad Informática, por las acciones de los virus.



Con la masificación de INTERNET y las nuevas generaciones de virus, se puede pronosticar que en el año 2000 existan aproximadamente 27,000 virus, incluyendo mutaciones y los virus de correo electrónico, que en estos últimos meses se han incrementado notablemente, como por ejemplo los virus CIH, Papa, Melissa, Explorer.zip, entre otros.

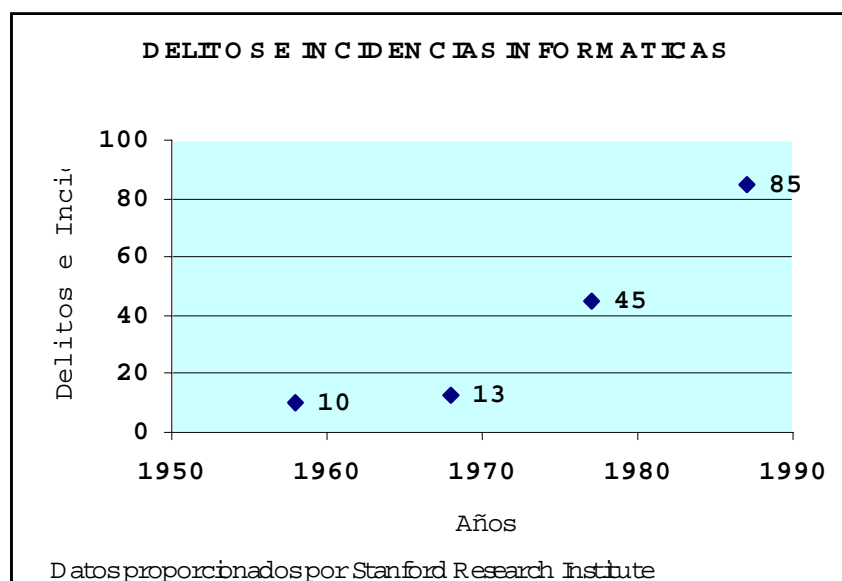
El aumento de la tasa de natalidad de los virus se convierte en un grave problema para todos los usuarios de computadoras y desarrolladores de los productos de software antivirus.

Historia

Los Incidentes y Delitos Informáticos muestran un incremento vertiginoso. El Stanford Research Institute (SRI) fue el primero en comenzar a compilar datos sobre Delitos e Incidentes Informáticos en el año 1958.

Durante las 3 primeras décadas, las cantidades eran insignificantes: Año 1958 (10), 1968 (13), 1977 (45) hasta 1987, donde el total de incidentes ascendió a 85. A partir de ese año el SRI dejó de compilar estos datos, ya que no era capaz de reflejar los incidentes y delitos informáticos que ocurrían.





Las incidencias y delitos informáticos se deben principalmente a:

- La evolución de las tecnologías de información desde el procesamiento en lotes de trabajo (BATCH) en la década del 60, pasando por el entorno distribuido de los 70's, las redes de microcomputadoras en los 80's, hasta el ambiente cliente-servidor de los 90's.
- El uso generalizado del trabajo en redes de computadoras e INTERNET y el ambiente cliente-servidor. Las estadísticas muestran que en esta década el crecimiento de HOST conectadas a esta red se hace realmente notable, estimándose que a finales del año 1999 sobrepasarán los 80 millones.

1995

En 1995 el motivo fundamental de conectarse a INTERNET era la necesidad de los usuarios por tener acceso a diferentes tipos de información.

1996

En 1996 por el desarrollo de aplicaciones de negocios, teniendo en cuenta que la implementación de INTRANETS estimuló el desarrollo de sitios WEB.

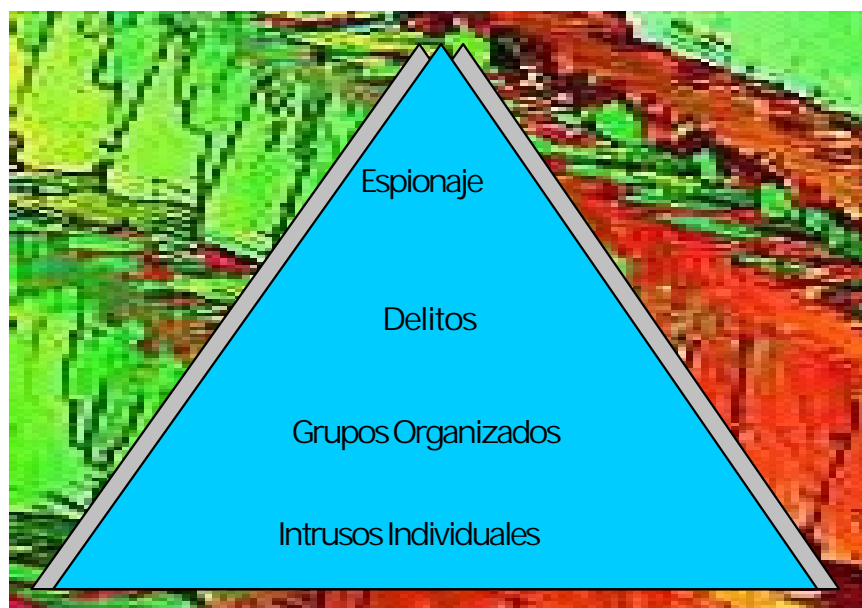
1998

A partir de 1998 el Comercio Electrónico es el principal motivo del crecimiento de INTERNET.

- Las nuevas tecnologías de la información introducen gran cantidad de amenazas y vulnerabilidades. El desarrollo de la Seguridad Informática resulta imprescindible.

Amenazas

El comportamiento de las Amenazas a la Seguridad de la Información arroja que la mayoría de los hechos son realizados por intrusos individuales. Un porcentaje corresponde a incidentes realizados por grupos organizados, otro porcentaje menor son delitos y la punta de la pirámide corresponde a casos de espionaje.



Pérdidas

En la mayoría de las empresas hay pérdidas de información por los siguientes motivos:



- Errores de los usuarios.
- Desastres naturales.
- Hardware.
- Virus informáticos.

Cabe resaltar que los virus son los causantes de la mayor parte de la pérdida de Información.

• Aparecen de 5 a 7 virus diariamente y el pronóstico para finales del año 2000 es que sobrepasen los 25,000 virus.



El acceso de tantos usuarios a INTERNET ha incrementado notablemente el riesgo de que una computadora sea infectada por un virus, debido a que se recibe o comparte información con mayor frecuencia.

Nuevos Riesgos

Con el incremento de microcomputadoras conectadas a INTERNET, destacan dos grandes tendencias que tendrán un fuerte impacto en la propagación de virus en los próximos años:

Primera Tendencia

Es el desarrollo y potencia de los sistemas integrados de mensajería como Lotus Notes y MS-Outlook, con los cuales cada vez es más fácil enviar archivos a otras personas. Además, permiten interfases de programación de aplicaciones (MAPI y Notes API), las cuales pueden utilizarse por otros programas, para enviar y procesar mensajes automáticamente.

Segunda Tendencia

Es el desarrollo de los llamados Sistemas Mobile- program como Java y Active X, que permiten mover un programa desde un servidor WEB y ejecutarlo en un cliente. Con la integración de Java en Lotus Notes y Active X en los Sistemas de mensajería de Microsoft, la amenaza aumenta.

El virus macro Share Fun demostró a principios de 1997, cómo era posible con macros de Word Basic, estando el MS-Mail activo, escoger del libro de direcciones, nombres a cuyas direcciones el virus envía un anexo infectado por él.

Existen diversos riesgos que de forma creciente se incorporan en los procesos automatizados, debido, entre otros factores, a la proliferación de usuarios y equipos informáticos, aumento en el nivel de autonomía de quienes tienen a su cargo el manejo técnico de éstos, el grado de vulnerabilidad ante insuficientes mecanismos de protección, seguridad física y lógica y conductas irresponsables o delictivas.

AUDITORIA A LA SEGURIDAD INFORMÁTICA

Concepto

La Auditoría a la Seguridad Informática es el proceso de verificación y control mediante la investigación, análisis, comprobación y dictamen del conjunto de medidas administrativas, organizativas, físicas, técnicas, legales y educativas, dirigidas a prevenir, detectar y responder a acciones que pongan en riesgo la confidencialidad, integridad y disponibilidad de la información que se procese, intercambie, reproduzca y conserve a través de las tecnologías de información.

Objetivo

El objetivo de la Auditoría a la Seguridad Informática es detectar fisuras o puntos vulnerables en el sistema informático que pongan en riesgo la seguridad de la información y de las tecnologías empleadas para su procesamiento, como base para la elaboración de un diagnóstico.



Funciones

- Analizar las políticas de Seguridad Informática adoptadas en la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información que en ella se procesa.
- Analizar y comprobar el funcionamiento y eficacia del Sistema de Medidas de Seguridad Informática implantado en la entidad.
- Detectar fisuras o puntos vulnerables en el funcionamiento del Sistema Informático y el Sistema de Medidas de Seguridad que puedan propiciar causas y condiciones para la comisión de delitos.

- Valorar la factibilidad del Sistema de Medidas de Seguridad, en correspondencia con la caracterización del Sistema Informático.

¿A quiéne se realiza la Auditoría?

La Auditoría a la Seguridad Informática se puede realizar a todos los Organos y Organismos de la Administración Central del Estado y sus dependencias, otras entidades



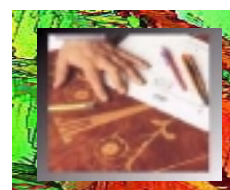
estatales, empresas mixtas, sociedades y asociaciones económicas que se constituyen conforme a la Ley, que utilicen Tecnologías de la Información, abarcando el control de aquello que actúa sobre una causa para reducir los riesgos o minimizar las causas de riesgo.

Etapas

Etapas para la realización de la Auditoría:

Planificación de la Auditoría

En esta etapa se planificará el trabajo a desarrollar, elaborando un cronograma con todos los pasos a realizar y los objetivos a lograr.



Desarrollo de la Auditoría

La Auditoría a la Seguridad Informática se divide a su vez en tres etapas:

- Investigación preliminar.
- Verificación de la seguridad informática aplicada.
- Comprobación con el empleo de herramientas informáticas.

Investigación Preliminar

Esta etapa persigue :

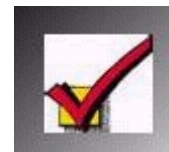
1. Conocer los objetivos y alcances del sistema de información establecido en la entidad objeto de auditoría.
2. Obtener la información necesaria sobre la caracterización (organización, recursos, personal, documentación existente sobre el objeto social, las dependencias y otros aspectos de interés a auditar).
3. Realizar una pormenorizada revisión de los resultados de auditorías informáticas y de seguridad anteriores o controles específicos de seguridad u otras actas o documentos, con el fin de obtener la mayor información en el menor tiempo posible sobre los principales problemas que han afectado esta entidad y que evidencien debilidades en el control interno.
4. Emplear el uso de cuestionarios para la recopilación de información, con el propósito de obtener una orientación general sobre la seguridad informática de la entidad.
5. Determinar los bienes informáticos más importantes para la entidad, de acuerdo a su costo beneficio.
6. Clasificación de los activos en función de su importancia y los problemas que trae a la entidad su revelación, modificación o destrucción.



7. Confeccionar tablas que permitan determinar dentro de los activos informáticos los riesgos existentes, ya sean de carácter administrativos, organizativos, técnicos, legales o específicamente informáticos, que determinen la vulnerabilidad de los activos.
8. Obtener los manuales de explotación y de usuario de los sistemas de las áreas o dependencias y efectuar un examen pormenorizado de éstos, para conocer el sistema y la auditabilidad para la seguridad del mismo.

Verificación de la Seguridad Informática Aplicada

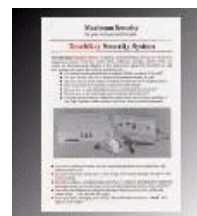
Esta etapa consiste, en la revisión y comprobación del cumplimiento de las normas y procedimientos de seguridad informática de la entidad.



Se utilizarán los cuestionarios como Herramienta de Auditoría a la Seguridad Informática, con el fin de obtener una orientación general sobre este tema.

Comprobación con el Empleo de Herramientas Informáticas

Muchos de los problemas y retos de la Auditoría a la Seguridad Informática parecen estar aún sin resolver. Según avanza la tecnología informática también tienen que cambiar y desarrollarse las técnicas de auditoría apropiadas para un determinado sistema, resultando inefectivas en otro más sofisticado.



Para el desarrollo de este enfoque, el Auditor a la Seguridad Informática necesita comprender suficientemente el sistema completo, para que le permita identificar y evaluar sus características esenciales de control.

Existe una amplia variedad de paquetes generalizados de auditoría a la seguridad que ayudan a la realización de las mismas, además de los programas generalizados disponibles. Muchos auditores diseñan sus propios procedimientos que se adaptan a las peculiaridades del sistema auditado.



Los diversos paquetes de programas de auditoría, entre los trabajos que llevan a cabo con más frecuencia, se encuentran, las muestras estadísticas o no, verificaciones matemáticas, examen de los riesgos, funciones de comparación, revisión analítica, chequeo de integridad de Base de Datos, etc.

Informe Conclusivo de los Resultados de la Auditoría

Se elabora un Informe Conclusivo donde se resume todo el desarrollo de la Auditoría a la Seguridad Informática, el cual debe contener los siguientes aspectos:

Objetivos Específicos de la Auditoría a la Seguridad Informática

Se explica en forma resumida la razón que persigue la aplicación de la Auditoría a la Seguridad Informática.

Objetivos a Controlar por la Auditoría a la Seguridad Informática

Se reflejan los objetivos controlados durante el proceso de la Auditoría a la Seguridad Informática.

Cronograma de Aplicación de la Auditoría a la Seguridad Informática

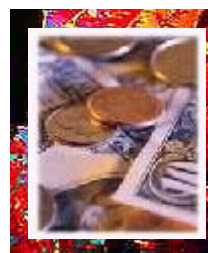
Se anexa el cronograma que se desarrolló en la Auditoría a la Seguridad Informática.

Desarrollo de la Auditoría a la Seguridad Informática

Se detalla la forma en que se aplicó la Auditoría, cada paso, control, verificación, entrevista, prueba o dinámica aplicada, así como los que intervinieron en el proceso de control y los resultados que se obtuvieron.

Valoración Resumen

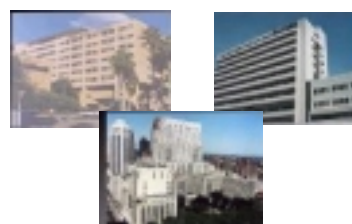
El objetivo de este aspecto es mencionar las medidas a adoptar con el fin de cubrir los riesgos potenciales. Es fundamental que el costo de estas medidas sea menor que el costo de la pérdida, ya que el objetivo final de un análisis de riesgos ha de ser la implantación de un sistema de seguridad, que persiga la reducción de la probabilidad de pérdida a un nivel aceptablemente bajo, dentro de un costo razonable.



Se debe exponer de forma clara, concisa y objetiva las deficiencias e incumplimientos que se comprueben, expresando siempre que sea posible la regulación, norma o procedimiento que se incumplió o violó.

Siempre que se realice un diagnóstico, deben incluirse las proposiciones necesarias para subsanar y erradicar las deficiencias o incumplimientos que se señalan.

Una vez que se ha terminado el informe, éste debe discutirse en la entidad auditada con la Dirección del Centro, la cual debe elaborar un plan de medidas para dar respuesta a las recomendaciones planteadas y fijar fecha para el análisis del mismo.



CUESTIONARIO PARA LA AUDITORIA A LA SEGURIDAD INFORMATICA

Cuestionario Nro. 1

ESTRUCTURA DE GESTION

	SI	NO
1. Existe un plan de seguridad informática aprobado por la entidad.	<input type="checkbox"/>	<input type="checkbox"/>
2. Se chequea adecuadamente el plan de seguridad informática	<input type="checkbox"/>	<input type="checkbox"/>
3. Existe un plan de contingencias	<input type="checkbox"/>	<input type="checkbox"/>
4. Existe un responsable de Seguridad Informática	<input type="checkbox"/>	<input type="checkbox"/>

POLITICAS DE SEGURIDAD

	SI	NO
1. Están definidas las Políticas de Seguridad Informática	<input type="checkbox"/>	<input type="checkbox"/>

CATEGORIZACION DE LA INFORMACION

	SI	NO
1. Se tiene la lista interna de clasificación de la información	<input type="checkbox"/>	<input type="checkbox"/>
2. Existe identificada la información sensible	<input type="checkbox"/>	<input type="checkbox"/>
3. Existe sistema de Control a la información clasificada	<input type="checkbox"/>	<input type="checkbox"/>
4. Existe sistema de Control a la información sensible	<input type="checkbox"/>	<input type="checkbox"/>

PERSONAL

	SI	NO
1. Está definida la asignación de responsabilidades generales y particulares atendiendo al funcionamiento de los equipos		
2. Existen medidas para garantizar la confiabilidad del personal que tiene acceso a las tecnologías de información		
3. Se evalúa el cumplimiento de las normas de seguridad establecidas para sus funciones		
4. Se tienen definidos los conocimientos técnicos que requiere un individuo para:		
• Concretar una amenaza		
• Responder a acciones malintencionadas		
5. Existe un convenio entre el personal y la entidad para cumplir las medidas de Seguridad Informática		

RESPONSABILIDADES

	SI	NO
1. Están definidas las responsabilidades del personal dentro y fuera de la entidad en función de la Seguridad Informática		

MEDIDAS FISICAS

	SI	NO
1. Están definidas las áreas vitales y reservadas		
2. Existe sistema de detección contra intrusos		
3. Existe sistema de detección contra incendio		
4. Existe un procedimiento para otorgar la autorización de acceso		
5. La posición de las computadoras propician compartir la información ante la entrada de un visitante al local		
6. La ubicación de las microcomputadoras es la factible a la captación de emisiones electromagnéticas:		
• El local colinda con viviendas particulares, sedes diplomáticas u otras en distancias menores a los 1,000 metros		
• El local tiene grandes ventanales de cristal que posibilitan la visibilidad de la información con poca interferencia o atenuación de emisiones electromagnéticas		
• Condiciones ambientales que propician el deterioro acelerado de las tecnologías o información contenida en las mismas		



• En la Auditoría se tiene que verificar si la ubicación de las computadoras y las condiciones ambientales son las adecuadas.



PROTECCION FISICA A LAS TECNOLOGIAS



	SI	NO
1. Existen varias personas que trabajan con una misma tecnología		
2. Por la función y/o ubicación a la que está destinada la tecnología se aplican medidas de protección física directamente a los equipos tales como cerraduras de disquetes, cerradura de encendido del procesador, etc.		
3. Los ficheros contentivos de información clasificada están señalizados de forma clara, visible y legible para los usuarios		
4. Los soportes magnéticos que contienen información clasificada están debidamente señalizados con la categoría de la información de mayor valor registrada en el mismo		
5. Los soportes magnéticos que contienen información clasificada son controlados y custodiados en las oficinas o por las normas de control, elaboradas al efecto		
6. Se identifican los soportes que contienen información sensible o de valor para la entidad o para un área de trabajo		
7. Los soportes magnéticos que contienen información sensible o de valor para la entidad o un área de trabajo se conservan en lugares adecuados y con la seguridad requerida		
8. Se destruye la información clasificada o sensible contenida en los soportes magnéticos a través de sobre escritura o mediante la aplicación de campo magnético u otros		



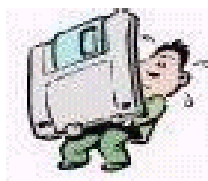
MEDIDAS DE SEGURIDAD TECNICA O LOGICA*Protección de entrada a las tecnologías de información*

	SI	NO
1. Hay un mecanismo para la protección de computadoras mediante el password del Setup		
2. Tienen asignado protectores de pantalla		
3. Existen mecanismos de control de passwords		

Protección a nivel de Sistema Operativo

	SI	NO
1. ¿Qué Sistema Operativo (S.O.) utiliza:		
  <ul style="list-style-type: none"> • D.O.S. • Windows 3.x • Windows 95 • Windows 98 • Windows NT • Otros 		
2. Cuenta con la documentación necesaria relacionada con los S.O. puestos en explotación		
3. Existe identificación y autenticación de usuarios a nivel de S.O. (licencias)		
4. Existen cuentas de equivalencia de supervisor en el caso de S.O. de redes		

MEDIDAS DE SEGURIDAD TECNICA O LOGICA

Protección a nivel de aplicaciones

	SI	NO
1. Indique:		
• Sabe en qué paquete de programas están desarrolladas las aplicaciones		
• Cuentan con la documentación necesaria relacionada con estas aplicaciones para su correcta explotación		
• Documentación sobre el uso de la aplicación		
• Documentación del código fuente		
• Sabe los códigos de programas de las aplicaciones que permanecen en el disco. Ejemplo: Códigos fuentes, ejecutables, etc.		
2. Está establecido un procedimiento para el cambio de los passwords en las aplicaciones		
3. Están establecidos los niveles de acceso de los usuarios en las Aplicaciones que lo requieran		
4. Tienen implementado mecanismos o herramientas que permitan suspender la sesión de trabajo de un usuario, cuando éste demore un tiempo dentro de la aplicación sin realizar acción alguna		



CONTROL DEL USO DE LOS RECURSOS Y DE LA INFORMACION

	SI	NO
1. Tienen implementados mecanismos para la protección de la información a nivel de S.O.		
2. Existe ambiente de red		
3. Sabe la cantidad de usuarios que están conectados		
4. Se restringe el nivel de acceso a la información de los usuarios		
5. Están establecidos todos los niveles de seguridad posibles para la protección de dispositivos, directorios, ficheros, etc.		
6. Existen procedimientos de enfrentamiento ante la detección de anomalías		

CONTABILIDAD DE LAS ACCIONES

	SI	NO
1. Tienen habilitados los mecanismos de contabilidad de las acciones de los usuarios		
2. Se registran las acciones de los usuarios		

AUDITORIA

	SI	NO
1. Se tienen el registro de las actividades de los usuarios en las aplicaciones		

CORTA FUEGO PARA CONEXION A INTERNET

	SI	NO
1. Tiene conexión a INTERNET		
2. Sabe el tipo de conexión a Internet que tiene su empresa		
3. Se adoptó alguna estructura de seguridad		
4. Se emplean mecanismos de filtrado		
5. Se realizó análisis de riesgo para protegerse de intrusos a través de INTERNET		
6. Tienen implementado algún mecanismo de seguridad		
7. Existen medidas para el control del uso del Correo Electrónico		



SISTEMA DE BACKUPS

	SI	NO
1. Se ha realizado un estudio de las características de backups de acuerdo al tipo de información		

MANTENIMIENTO Y REPARACION DE LA TECNOLOGIA DE INFORMACION

	SI	NO
1. Sabe dónde se realiza el mantenimiento de los equipos		
2. Sabe quién realiza el mantenimiento de los equipos		
3. Existe algún mantenimiento que sea necesario realizar fuera de la Entidad		

CONTROL DEL USO, TRASLADO Y ENTRADA DE LAS TECNOLOGIAS DE INFORMACION

	SI	NO
1. Sabe a qué entidad se le compran las tecnologías de información		
2. En caso de que las tecnologías de información provengan del exterior son sometidas a chequeos especializados		
3. Se realiza algún chequeo en la entidad a la máquina que reciben a nivel de:		
• Hardware		
• Software		

PRUEBA DE INSPECCION

	SI	NO
1. Están identificados los mecanismos de seguridad instalados	<input type="checkbox"/>	<input type="checkbox"/>
2. Se tiene establecida la frecuencia de inspección a cada mecanismo	<input type="checkbox"/>	<input type="checkbox"/>
3. Están definidas las medidas a desencadenar en el caso de que se detecten problemas	<input type="checkbox"/>	<input type="checkbox"/>
4. Existe un registro de incidencias de este tipo	<input type="checkbox"/>	<input type="checkbox"/>
5. El personal designado ha sido preparado para llevar a cabo las inspecciones	<input type="checkbox"/>	<input type="checkbox"/>
6. Se contempla entre el listado de responsabilidades, al personal vinculado a esta actividad	<input type="checkbox"/>	<input type="checkbox"/>

AUDITORIA

	SI	NO
1. Existen planificadas auditorías internas y/o externas	<input type="checkbox"/>	<input type="checkbox"/>
2. Tiene una guía de auditoría de Seguridad Informática	<input type="checkbox"/>	<input type="checkbox"/>
3. Existe un expediente único de auditoría y controles	<input type="checkbox"/>	<input type="checkbox"/>
4. Se realizan análisis de las trazas de auditoría instaladas	<input type="checkbox"/>	<input type="checkbox"/>
5. Cuentan con las herramientas necesarias para realizar auditorías	<input type="checkbox"/>	<input type="checkbox"/>
6. Se ha establecido que se analicen y tomen medidas a partir de los resultados de auditoría en la máxima instancia de dirección	<input type="checkbox"/>	<input type="checkbox"/>
7. Los ficheros de auditoría cuentan con la seguridad necesaria contra ataques diversos	<input type="checkbox"/>	<input type="checkbox"/>

MEDIDAS EDUCATIVAS Y DE CONCIENTIZACION

	SI	NO
1. Tienen implementadas medidas educativas y de concientización		
2. Tienen definidos programas de preparación		

MEDIDAS PARA LA APLICACION DE SANCIONES

	SI	NO
1. Se implementan sanciones administrativas al personal que viola la seguridad informática		



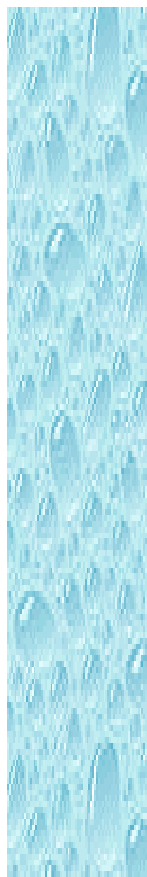
Cuestionario Nro. 2

POLITICAS DE SEGURIDAD



1. ¿Se realizó algún análisis de riesgo y de vulnerabilidad para la elaboración del Plan de Seguridad Informática?. Mostrar los resultados en caso afirmativo
2. ¿Cuál es la estructura de gestión adoptada?
3. ¿Cuáles son las políticas definidas en función de la Seguridad Informática?

MEDIDAS FISICAS



1. ¿Están definidas las áreas vitales y reservadas?
2. ¿Cuáles son las áreas vitales definidas y dónde se encuentran?
3. ¿Cuál es el estado constructivo de los locales en cuanto a:
 - Comprobar vías de acceso.
 - Comunicación con el exterior.
 - Condiciones de privacidad, para la compartición del trabajo y la información.
 - Condiciones de la red eléctrica y aterramiento.
 - Estado de los cierres de puertas y ventanas.
 - Dispositivos de sellaje o control técnico de acceso a los locales.
4. ¿Cómo se puede identificar el personal con acceso, según el tipo de autorización?
5. ¿Quién autoriza el acceso?
6. ¿Cómo se controla en las vías de acceso perimetral la documentación de autorización?



7. ¿Cuál es el régimen de autorización para el traslado o entrada de tecnologías de información hacia un local específico?

PROTECCION FISICA A LAS TECNOLOGIAS



1. En caso de usar tecnologías de forma compartida, ¿qué controles existen sobre la utilización de las mismas?
2. ¿Cuáles son los procedimientos establecidos para la conservación de los soportes magnéticos?
3. ¿Quién controla la aplicación de estos procedimientos?

MEDIDAS DE SEGURIDAD TECNICA O LOGICA

Protección de entrada a las tecnologías de información



1. Tienen asignado password.
- 2.Cuál es la política implementada para la gestión de las claves de acceso:
 - Utilizan los mecanismos de asignación, confección y control de claves.
 - Las claves de acceso son escogidas por el usuario o asignada por el administrador.



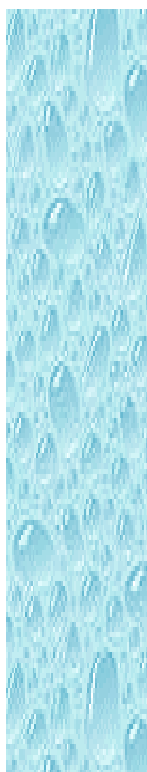
- ¿Qué longitud tienen las claves y cómo están conformadas?
- ¿Quién actualiza las claves, con qué periodicidad y quién controla este aspecto?

Protección a nivel de Sistema Operativo



1. En caso de tecnologías de uso compartido, ¿están definidos todos los usuarios de forma independiente?
2. ¿Quién tiene asignado cuenta de supervisor y quién autoriza la asignación de estas cuentas?
3. ¿Quién conoce las claves de supervisor?

Protección a nivel de aplicaciones



1. ¿Cómo se realiza el control de las modificaciones a las aplicaciones?
2. Mencione las aplicaciones que han sufrido modificaciones.
3. ¿Dónde se conserva la documentación actualizada?
4. ¿Quién instala, brinda mantenimiento y actualiza los programas o aplicaciones?
5. Relacione por cada aplicación los códigos de programas que permanecen en el disco.
6. Relacione para cada aplicación los mecanismos de seguridad implementados, tales como:
 - Autenticación e identificación de usuarios.
 - Asignación única de passwords a los usuarios.



- ¿Está reglamentada la protección y el tipo de acceso que se debe otorgar a cada tipo de usuario?.
 - ¿Dónde se guardan las claves de los usuarios?
 - ¿Se emplean mecanismos de encriptamiento para la salvaguarda de las mismas?.
7. ¿Con qué periodicidad se cambian las claves?
 8. ¿Quién controla el cambio de los passwords?
 9. ¿Cómo están implementados los mecanismos o herramientas que permitan suspender la sesión de trabajo de un usuario, cuando éste demore un tiempo dentro de la aplicación sin realizar acción alguna?
 10. ¿Cómo se realiza técnicamente la actualización de los niveles de acceso de los usuarios dentro de la aplicación?
 11. ¿Qué criterios utilizan para otorgar el acceso?

CONTROL DEL USO DE LOS RECURSOS Y DE LA INFORMACION



1. ¿Cuáles son los mecanismos empleados a nivel de Sistema Operativo para la protección de la información?
2. ¿Qué política se sigue para establecer los niveles de acceso?
3. Mencione otros mecanismos de seguridad empleados, tales como:
 - Asignación de tiempo de máquina.
 - Cantidad de intentos permisibles en el login.
 - Asignación de máquinas a determinadas cuentas.
 - Protección a nivel de directorios y archivos.



4. En el caso de chequeo interactivo:
 - ¿Qué chequeos de integridad se realizan a los datos?
 - ¿Qué acciones se realizan cuando es violado el chequeo de validación de los datos?
 - ¿Se registran en la Base de Datos los artículos que no cumplen los requisitos de validación?
5. En caso de chequeo batch:
 - ¿Cómo se realiza el mismo?
 - ¿Se tiene en cuenta la información existente o se adicionan los artículos sin chequeo de correspondencia previa?
6. ¿En qué consiste el chequeo de integridad?
7. ¿Quién realiza el control sobre el crecimiento de las BD?
 - En qué consiste este control.
 - Con qué periodicidad se realiza el mismo
8. Mencione los mecanismos de identificación de los ficheros.
9. Qué mecanismos de monitoreo tienen establecidos a nivel de Sistema Operativo tales para chequear:
 - Las actividades de los usuarios.
 - Los recursos empleados por los usuarios.
 - El acceso a la información.
 - Los procesos activos.
 - Usuarios conectados, etc.
10. ¿Quién se encarga de realizar el monitoreo y con qué frecuencia se realiza?





14. ¿Cuáles son las anomalías que pueden presentarse con mayor probabilidad?
15. ¿Cuáles son los procedimientos de enfrentamiento ante la detección de anomalías?

CONTABILIDAD DE LAS ACCIONES



1. ¿Qué datos se guardan en el registro del sistema?
2. ¿Con qué periodicidad se vacían estos registros?
3. ¿Se realizan salvadas de los mismos?.
4. ¿Quién analiza la información que se obtiene con la contabilidad de las acciones de los usuarios?
5. ¿Cada qué tiempo se realiza este análisis?.

AUDITORIA



1. ¿Qué información de la actividad de los usuarios se almacena en las aplicaciones?
2. ¿Qué protección tienen estos archivos?
3. ¿Se realiza backups de estos archivos?.
4. ¿Se tiene periodicidad e historia de los backups?.

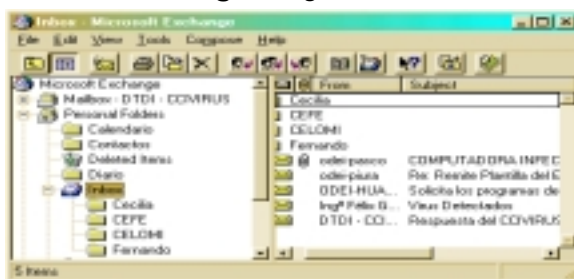
La Auditoría de la Información, es importante para revisar qué tipo de seguridad tiene la empresa o institución para garantizar su información.



CORTA FUEGO PARA CONEXION DE INTERNET



1. ¿Qué mecanismos de filtrado emplean para el acceso a los servicios?
2. ¿Qué análisis de riesgos se realizó para protegerse de intrusos a través de INTERNET?
3. ¿Qué servicios tiene habilitados?
4. ¿Qué medidas de seguridad tienen establecidas en los servicios habilitados?
5. Si tiene habilitado el servicio de Correo Electrónico:
 - ¿Quiénes están autorizados para emplear el mismo?
 - ¿Quién autoriza?
 - ¿Cómo es el procedimiento para solicitar el servicio?
 - ¿Qué medidas tienen establecidas para el uso del Correo Electrónico?
 - ¿Se registran los usuarios con acceso al mismo?, ¿qué información se registra?
 - Se realiza análisis del uso del Correo Electrónico, teniendo en cuenta la información del proveedor del servicio.
6. Cuando se detectan anomalías en los servicios de INTERNET, ¿a quién se informa?, ¿qué procedimientos se siguen?, ¿están establecidos?



SISTEMA DE BACKUPS

1. ¿Qué mecanismos de backups se han implementado?
2. ¿Con qué periodicidad se realizan los mismos?
3. ¿En qué soportes se realiza?
4. ¿Cuántos backups se realizan?
5. ¿Dónde se guardan los backups?
6. ¿Quién controla el funcionamiento de los mismos?
7. ¿Quién se responsabiliza con la información guardada?

**MANTENIMIENTO Y REPARACION DE LA TECNOLOGIA DE INFORMACION**

1. ¿Dónde se realiza el mantenimiento de los equipos y quién lo realiza?



ANEXOS

Panda Software International



FIREWALLS SEGURIDAD CONCENTRADA

Los sistemas informáticos de las empresas suelen estar formados por redes interconectadas entre sí, que permiten la compartición de los recursos entre todos los usuarios. Este conjunto de hardware, software y datos debe estar fuertemente protegido ante las amenazas externas.

Los Firewalls o cortafuegos, son barreras que concentran la seguridad de parte de una red en un punto. Se sitúan entre los encaminadores y pasarelas que unen unas redes con otras. Esto permite que, enfocando en ese punto políticas fuertes de seguridad, la red que queda tras esa barrera esté protegida ante el ataque de usuarios externos.



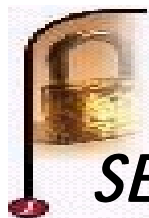
La función de los firewalls consiste en vigilar el tráfico de información, tanto entrante como saliente, a través del filtrado de los datos que viajan entre las redes. También se ocupan de identificar convenientemente a los usuarios externos que quieran conectarse a la red. Podemos pensar que su función es como la de un guardia de seguridad en un gran edificio: situado en la puerta, controlará todo el tráfico de personas, evitará que entren individuos sospechosos, y pedirá identificación a aquellos usuarios que quieran entrar a los departamentos privados.

Esta necesidad se hace aún más patente cuando la red está conectada a Internet, donde las posibilidades de un ataque se multiplican, ya que estamos hablando de millones de ordenadores que pueden, cuando menos, presentarse delante de nuestra supuesta puerta principal. Por norma general, los firewalls están formados por sistemas hardware o software, y en la mayoría de las ocasiones se trata de un compendio de ambos.



Esta solución se presenta como todo un estándar en cuanto a la seguridad de las redes, y su implantación queda complementada con un sistema antivirus que soporte distribución, monitorización, configuración, programación y actualización, de forma centralizada.

Panda Software International

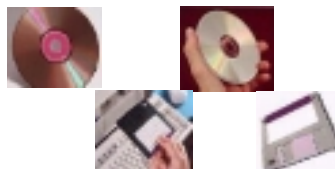


BACKUPS: COPIAS DE SEGURIDAD ESENCIALES

Firewalls, herramientas de cifrado, antivirus, o parches a los sistemas operativos, son algunas de las medidas y utilidades que a diario, y en mayor o menor medida, utilizamos para garantizar la seguridad de nuestros sistemas. Sin embargo, no debemos olvidar uno de los pilares básicos en los que debe basarse toda política de seguridad que se precie: las backups o copias de seguridad.

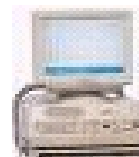
Ante desastres naturales, robo físico, o vandalismo informático, las copias de seguridad se presentan como una de las medidas más útiles para poder recuperar, mediante su restauración, la información vital de los sistemas y evitar la pérdida total de nuestros datos.

Cintas magnéticas, discos ópticos, discos duros, o el tan socorrido, pero cada vez menos útil, disquete, son algunos de los dispositivos empleados para realizar las copias de seguridad. El más utilizado tradicionalmente, la cinta magnética, ha sido desbancado por otros que permiten un acceso directo a la información y conllevan otras ventajas. No obstante, el acceso secuencial de las cintas magnéticas no impide que cumplan perfectamente con su misión, característica que se suma a la ventaja que supone el que se trate de uno de los soportes más baratos.

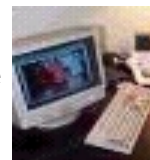


Cuando el usuario va a planificar la política de copias de seguridad de su equipo informático, debe tener en cuenta los siguientes consejos:

- Configurar el sistema para que realice las copias de seguridad de forma automática.
- Llevarlas a cabo en las horas en las que la actividad sea mínima. Esto nos permitirá asegurarnos de que hay pocos ficheros abiertos y que, por lo tanto, salvaguardamos la mayor parte de la información.
- Hacer una primera copia de seguridad de todo el sistema y repetirla cuando existan cambios importantes (actualizaciones, parches, o instalación de nuevo software).



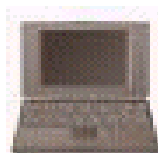
- Realizar, periódicamente, copias de seguridad incrementales, de forma que sólo se vayan guardando los cambios introducidos desde la última copia. Al evitar tener que realizar copias globales se agiliza el proceso.



- Escoger un sistema de rotación de cintas, que vendrá marcado por el número de copias que queremos guardar.
- Guardar las copias de seguridad en lugares seguros, como las cajas herméticas creadas con tal fin, y, si es posible, en ubicaciones diferentes donde se encuentran los sistemas salvaguardados. Aunque no siempre es posible, lo mejor sería que se hallaran en localizaciones muy distantes para evitar que ambas, copias de seguridad y sistemas, resulten afectadas si se produce un desastre natural.



- Probar el sistema de forma completa, lo que también incluye restaurar las copias de seguridad. En cualquier caso, el usuario no podrá asegurarse de que la metodología elegida funciona adecuadamente hasta que simule una pérdida de datos que, además de servirle como práctica, le ayudará a descubrir los problemas que pueden presentarse en un caso real.



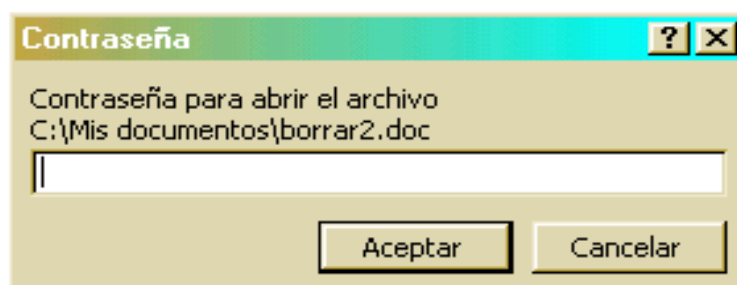
Panda Software International



PASSWORDS, EL PRIMER PUNTO A PROTEGER

En muchas ocasiones se efectúan grandes inversiones tratando de proteger los sistemas informáticos de la empresa: se instalan firewalls, servidores seguros, etc. Pero todo ello puede quedar al descubierto si se descuida un punto primordial: los passwords.

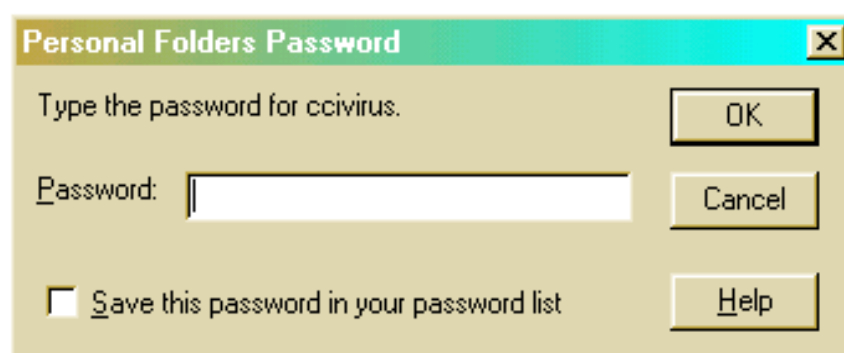
El primer punto en el que se basa la seguridad de un sistema son los passwords. Para entrar en un ordenador o servicio hay que introducir, por regla general, un nombre de usuario y una palabra clave. Si descuidamos este aspecto, toda protección adicional que se instale en el sistema no tendrá sentido.



Puede resultar chocante comprobar cómo una compañía puede invertir miles de dólares en instalar un eficaz firewall, para después ver que las contraseñas de acceso al sistema son tan simples como repetir el nombre de usuario o, incluso, que se mantienen los passwords que se crean por defecto en el sistema. El atacante no tendrá que saltarse ninguna medida de protección, bastará con que sea lo suficientemente “astuto” como para probar diversas combinaciones de login/ password y conseguirá entrar en el sistema con pleno derecho.

Por ello, es fundamental que ningún password sea obviado, que no contenga nombres de personas, lugares, fechas, etc. En definitiva, el password debe ser una combinación de números, letras y signos de puntuación, sin ningún sentido evidente.

La mayor parte de los sistemas operativos incluyen opciones (o existen paquetes adicionales) que posibilitan controlar este tipo de acciones, así como obligar a que el password sea de una determinada longitud. Otra medida que se puede tomar pasa por efectuar un cambio periódico de la clave, cada 15 días o una vez al mes, en consecuencia con la sensibilidad de los datos afectados.



Sin duda obligar a los usuarios a recordar cadenas de letras, números y signos puede ser algo caótico y hasta imposible de conseguir. Por ello, se les debe dotar de un medio para generar passwords complicados y de forma sencilla, incluso para los más inexpertos.

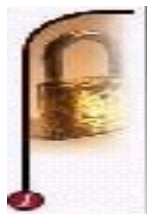
Un buen truco consiste en utilizar las iniciales de una canción, pasaje de un libro, refrán, etc. Por ejemplo, partiendo de un típico refrán



como "Quien a buen árbol se arrima, buena sombra le cobija", podríamos conseguir un password como **"qabasabslc"**, con una longitud adecuada y sin duda, imposible de encontrar en ningún diccionario. Si a esta password le cambiamos alguna letra de minúscula a mayúscula y algún carácter por un número o código similar y que nos recuerde al original (sustituir la l por un 1, la o por un 0, la b por un 6, etc.) podemos conseguir una clave con un alto grado de seguridad. Nuestro ejemplo podría quedar en algo como **"qabasA6s1c"**, una clave que, sin duda, no es difícil de recordar pero que es ciertamente difícil de descifrar por alguien que no sea el propio usuario que la ha creado.



Panda Software International



SEGURIDAD UNIX PARA USUARIOS WINDOWS

Virus, agujeros en los navegadores o agujeros en el sistema operativo, son algunos de los problemas de seguridad con los que tenemos que enfrentar a diario los usuarios de Windows, el sistema operativo más extendido. Sin embargo, el usuario doméstico debe ser consciente de las características de la seguridad de otros sistemas, como Unix, ya que, aunque en principio pueda parecer que no nos afecta, forman en realidad parte importante de nuestro entorno.

Con la entrada de Internet los usuarios domésticos hemos pasado a interactuar con un conjunto de sistemas muy heterogéneos, aunque no seamos conscientes, donde los sistemas Unix pasan a ser un punto en el que se suele concentrar parte de nuestra seguridad. Una de las razones, es que la mayoría de los proveedores de Internet utilizan esta plataforma para los servidores que nos identifican y dan acceso a la Red.



Cada vez que accedemos a Internet debemos proporcionar los datos de nuestra cuenta al proveedor. El nombre de usuario y contraseña permiten al servidor identificarnos como usuarios registrados y darnos acceso a Internet, así como a nuestro buzón de correo electrónico. Estos datos son muy importantes para nuestra seguridad y si llegara a manos de un tercero, éste podría hacerse pasar por nosotros, acceder a Internet con nuestra cuenta y utilizar a su antojo nuestro correo.



Los sistemas Unix son conscientes de la importancia de estas cuentas, por lo que utiliza un sistema de cifrado para salvaguardar estos datos. Las contraseñas de los usuarios son almacenadas en un fichero llamado etc/passwd. Debido a su contenido, este fichero es uno de los más codiciados por los crackers y hackers. Unix, como primera medida de seguridad, almacena las contraseñas cifradas, de manera que si un cracker o hacker consigue el archivo, no tenga, en principio, acceso a estas claves.



Sin embargo, los crackers suelen utilizar una técnica, denominada 'ataque por fuerza bruta' o 'diccionario', que consiste en cifrar todas las palabras de un diccionario y ver si coinciden con la contraseña cifrada de algún usuario.

Lo hacen de esta forma ya que no es posible obtenerla de otro modo, debido a que el algoritmo que utiliza Unix para cifrar no permite la operación inversa.

Consciente del modo en que se producen este tipo de ataques, el usuario doméstico debe tener un cuidado especial al elegir la contraseña. La elección debe realizarse pensando que debe ser una combinación de números, signos y letras, de manera que no se encuentren en un hipotético diccionario que un cracker pueda utilizar para averiguar nuestra clave. Debemos evitar el utilizar palabras comunes, nombres propios, marcas, combinaciones del nombre de usuario, alias, etc.

Cecilia, Fernando

Silvana, Gonzalo - Patty, Alex - Margarita, Jimmy

***Ana, Francisco - Josésino, Carol - Sandra, Eduardo- Jaqui, Toño
Sergio, - Miller - Dávila - Agustín, Sara- Antonieta, Frank- Paola,
Shawn - Antonina, Frank - Patty, Jorge - Oscar - Betsy, José -
Pierito - Cecy, Nando.***

Una buena contraseña debe mezclar letras mayúsculas y minúsculas, dígitos y caracteres de puntuación. Su longitud debe superar los seis caracteres, y al mismo tiempo, debemos tratar que sean fáciles de recordar. Una buena elección nos permite que, aunque un atacante consiga el fichero de passwords de nuestro proveedor de Internet, nuestra seguridad sea realmente difícil de vulnerar.

Panda Software International



INFORME SOBRE LA SEGURIDAD INFORMATICA EN LAS EMPRESAS

Un 77 % de las empresas tienen, a lo largo del año, algún tipo de incidencia o problema relacionado con virus informáticos. Este es uno de los datos proporcionados en el último estudio sobre seguridad informática, publicado en el número de Julio de la prestigiosa revista Information Security. El estudio, realizado entre los meses de Abril y Mayo del presente año, es el resultado de una encuesta en la que han participado 745 lectores de la revista Information Security, una muestra que incluye administradores de sistemas, responsables y ejecutivos en tecnologías de la información, redes informáticas y administración de datos. El informe ha sido patrocinado por la Asociación Internacional de Seguridad Informática (ICSA) y SAIC, empresa dedicada a soluciones de seguridad.

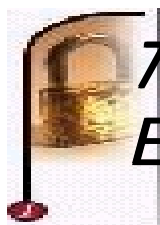
El objetivo de la encuesta es evaluar el estado de la seguridad informática desde el punto de vista de sus responsables, calibrar la vulnerabilidad y eficacia de los productos comerciales relacionados con dicha área, y profundizar en los crecientes problemas asociados a los agujeros de seguridad.



Los ataques por virus siguen siendo el principal problema de las empresas en lo que a seguridad se refiere, y el número de incidencias debidas a código maligno sigue aumentando. Un 77 % de las empresas encuestadas ha sufrido a lo largo del pasado año algún tipo de incidencia o problema relacionado con virus informáticos. Las soluciones antivirus, que se pueden encontrar en más de un 90% de las empresas, son los más empleados en el área de seguridad, aunque este año ha cobrado especial importancia la inversión en firewalls y software de control de acceso, debido sobre todo a la potenciación de la seguridad en Internet.

Estudios anteriores reflejaban que el mayor riesgo a la seguridad provenía de los abusos de los propios empleados o de empleados descontentos. Este tipo de accesos "desde dentro" se llegaba a cifrar hasta en un 80%. Según este nuevo informe, se vuelve a demostrar, por un amplio margen, que este tipo de accesos no autorizados sigue afectando a la mayor parte de las compañías por encima de cualquier otro tipo de riesgo. También se produce un aumento en el número de casos de accesos externos no autorizados. El porcentaje de empresas que habían sufrido alguna intrusión de hackers durante el año 1998 se situaba en un 12%, mientras que en el presente estudio el porcentaje se eleva al 23% de las empresas, es decir, casi el doble.

Panda Software International



7,600 MILLONES DE DOLARES EN PERDIDAS CAUSADAS POR LOS VIRUS

Según la consultora Computer Economics, en el primer semestre del año los virus han causado a las empresas unas pérdidas por valor de 7,600 millones de dólares en todo el mundo. Según la consultora norteamericana, los principales enemigos de este año tienen nombres de gusanos, I-Worm, ExploreZip y Melissa, ya que éstos han protagonizado los mayores índices de ataques y de pérdidas para las empresas.

Computer Economics eSite
The Authority on Technology Value

Estos 7,600 millones de dólares representan los gastos por pérdidas en productividad y costos de reparación declarados por las 185 compañías que han sido objeto del estudio de Computer Economics y que representan cerca de 900.000 usuarios internacionales.

Esta cifra contrasta con la ofrecida el año pasado por la misma consultora y que situaba las pérdidas de todo el año por encima de los 1,500 millones de dólares. En el estudio de 1998 no sólo se incluyeron las pérdidas por virus, sino también las debidas a intrusiones en los sistemas informáticos por hackers y usuarios maliciosos. Computer Economics hace hincapié en que las cifras de pérdidas en este primer semestre del año son ya cinco veces superiores a los totales del pasado año y sólo en cuanto a virus se refiere. Incluso, se estima que estos números son conservadores e inferiores a los reales, ya que la mayor parte de las compañías tienden a minimizar los gastos y las incidencias producidas, a fin de no provocar una mala imagen entre sus clientes.

En cuanto a la prevención contra los ataques por virus y gusanos, Michael Erbschloe, vicepresidente de investigación de Computer Economics, recomienda una mayor atención a las políticas de seguridad informática de las empresas: "La prevención contra estos ataques sólo se puede llevar a cabo destinando fondos y personal adecuado a los programas de seguridad informática de la empresa. De estos programas, son muy pocos los que cumplen con los recursos necesarios y la mayoría de las empresas tendrán que doblar el presupuesto destinado al área de seguridad informática para hacer frente a este tipo de ataques".

BIBLIOGRAFIA



Modelo de la Metodología para la realización de Auditorías a la Seguridad Informática.

Agradecimiento Especial a:

Ing. Jesús Zaldivar Vázquez

Ing. Lucila Vázquez Noa

Ministerio del Interior

CUBA



Incidencia de los Virus en la Seguridad Informática

Agradecimiento Especial a:

Lic. José Bidot Pelaéz

Director del Laboratorio Latinoamericano de Protección
contra Virus Informáticos UNESCO

CUBA



Proceedings of the Seventh International Virus Bulletin Conference 1997



Proceedings SECURMATICA' 97 .
(ANSEI, España)



Proceedings Segunda Conferencia de Seguridad Informática.
(ALAPSI, México)



<http://www.computereconomics.com>



<http://www.pandasoftware.es/>