DEFINICIONES

FMVZ: Facultad de Medicina Veterinaria y Zootecnia.
CCFMVZ: Comité de Cómputo de la Facultad de Medicina Veterinaria y Zootecnia, órgano que observará la correcta aplicación de las políticas, el cual está integrado por:

- El Director, quien fungirá como presidente de dicho Comité,
- El titular de la Secretaría General,
- El titular de la Secretaría Administrativa,
- El titular de la División de Estudios Profesionales,
- El coordinador del programa de Maestría y Doctorado,
- El titular de la Secretaría de Educación Continua y Tecnología,
- El titular de la División del Sistema de Universidad Abierta,
- El titular de la Secretaría de Producción Animal,
- El jefe del Departamento de Cómputo, quién fungirá como Secretario Técnico de dicho Comité
- Un representante profesor del H. Consejo Técnico, y
- Un representante alumno del H. Consejo Técnico

ATI: Administrador de Tecnologías de Información. Responsable de la administración de los equipos de cómputo, sistemas de información y redes de telecomunicaciones de la FMVZ.
Administrador de la red de datos: Persona encargada de realizar proyectos, actualizar y mantener en funcionamiento eficiente la red de datos de la FMVZ.
Sistema de cómputo: Conjunto de elementos electrónicos que interactúan entre sí (Hardware) para procesar y almacenar información de acuerdo con una serie de instrucciones (Software).
Recurso informático: Cualquier componente físico o lógico de un sistema de información**.**
Usuario: Cualquier persona que haga uso de los servicios proporcionados por la FMVZ, responsables de los equipos de cómputo y sistemas de información.
Nombre de usuario: Conjunto de caracteres que identifican al usuario ante un recurso informático.
Contraseña: Conjunto de caracteres que permite el acceso de un usuario a un recurso informático.
TIC: Tecnologías de Información y Comunicaciones.
Seguridad en cómputo: Conjunto de recursos destinados a lograr que los activos de una organización sean confidenciales, íntegros, consistentes y disponibles a sus usuarios, autenticados por mecanismos de control de acceso y sujetos a auditoría.

ÁMBITO DE APLICACIÓN Y FINES

Estas políticas tienen por objeto establecer las medidas de índole técnica y de organización necesarias para garantizar la seguridad de las tecnologías de información y personas que interactúan, haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios de cómputo de la FMVZ.

Estas políticas definen ciertas medidas que establecen un límite entre lo que está permitido y prohibido a los usuarios dentro de la FMVZ. Para ello, se establece el principio básico de seguridad para la Facultad: "Lo que no se permite expresamente, será revisado por el CCFMVZ".

POLÍTICAS GENERALES DE SERVICIOS

1. La prioridad será mantener funcionando la infraestructura y los servicios de la red de cómputo (cableado estructurado, equipos de red y servidores) y los servicios en los Laboratorios de Cómputo Académico.
2. Los servicios a usuarios se prestarán principalmente por los Departamentos de Cómputo y de Apoyo Técnico en Cómputo.
3. El servicio de reparación a equipos de cómputo inventariados será realizado por la empresa contratada para ese fin.
4. Sólo se dará servicio a usuarios con software propietario legal.

POLÍTICAS GENERALES DE SOFTWARE

1. Se dará preferencia al uso de software libre sobre soluciones basadas en software propietario, a efecto de reducir costos innecesarios.
2. Cuando se requiera de software propietario, deberá ser legalmente adquirido.
3. No se deberá utilizar software propietario sin tener la licencia correspondiente.
4. El Departamento de Cómputo propiciará la compra de software propietario en volumen cuando éste sea de amplio uso entre el personal académico o administrativo.

POLÍTICAS GENERALES DE HARDWARE

1. El Departamento de Cómputo deberá contar con la tecnología de cómputo emergente (computadoras de escritorio, servidores, equipos activos de red, puntos de acceso inalámbrico, etc.), para evaluarla antes de aplicarla a nivel general en la FMVZ, con el fin de aprender a solucionar los problemas que puedan acarrear su uso.
2. A partir de los resultados de las evaluaciones realizadas y basados en recomendaciones del Consejo Asesor de Cómputo de la UNAM, el Departamento de Cómputo emitirá recomendaciones de hardware para los usos específicos de las diferentes áreas.
3. Para realizar la compra de equipo de cómputo (computadoras personales de escritorio, computadoras portátiles, servidores, impresoras y scanners), se considera lo siguiente:
    a) Para las adquisiciones realizadas con cualquier fuente presupuestal de la FMVZ (partidas centralizadas, presupuesto a ejercer anualmente o ingresos extraordinarios) el Departamento de Cómputo dará visto bueno únicamente en lo concerniente a las características técnicas del equipo a adquirir, con el fin de obtener los equipos con las mejores condiciones.

   b) Para las adquisiciones realizadas con fuentes de financiamiento externo a la FMVZ, se deberán informar al Departamento de Cómputo las características de los equipos adquiridos.
4. La adquisición de equipo nuevo deberá contar con la licencia respectiva de sistema operativo (Windows XP, Windows Vista, etc.)

POLÍTICAS GENERALES DE SEGURIDAD

1. El Departamento de Cómputo establecerá los mecanismos de hardware y software necesarios para salvaguardar el funcionamiento de la red de telecomunicaciones y la información en los equipos de cómputo de uso común.
2. Todas las computadoras que utilizan el sistema operativo Microsoft Windows deberán contar con el sistema de protección antivirus recomendado por el Departamento de Cómputo.
3. Todas las computadoras que funcionen bajo el sistema Linux/UNIX deberán acatar las configuraciones de acceso desde y para el exterior dictadas por el Departamento de Cómputo.
4. No se permitirá la instalación y uso de software que viole los derechos de autor al permitir descargar audio, video y software propietario (por ejemplo: Ares, Kazaa, Gator, AudioGalaxy, LimeWire, etc.).
5. Las computadoras de particulares que deseen conectarse a la red de la FMVZ deberán cumplir con las políticas de seguridad y los procedimientos dictados por el Departamento de Cómputo.
6. Respecto a la seguridad física:
   a) Mantener las computadoras alejadas del fuego, humo, polvo y temperaturas extremas.
   b) Colocar las computadoras fuera del alcance de rayos solares, vibraciones, insectos, ruido eléctrico (balastros, equipo industrial, etc.), agua, etc.
   c) Todos los servidores deberán ubicarse en lugares de acceso físico restringido.
   d) El lugar donde se instalen los servidores deberá contar con una instalación eléctrica adecuada, con tierra física y un sistema de energía ininterrumpible de cuando menos 30KVA.
   e) El lugar donde se instalen los servidores deberá contar con aire acondicionado. La capacidad de éste será calculada acorde al espacio destinado para dicho fin.
   f) En los lugares donde se encuentren equipo de cómputo queda prohibido fumar e ingerir bebidas y alimentos.
   g) Los Laboratorios de Cómputo Académico deberán tener la orientación y visto bueno del H. Cuerpo de Bomberos de la UNAM respecto de la colocación y manejo de extintores.
   h) Los racks de comunicaciones deberán ser closets de comunicaciones cerrados con ventilación, a los cuales sólo personal del Departamento de Cómputo tendrá acceso.

i) Todo cableado estructurado de datos que se pretenda instalar en la FMVZ deberá contar con el visto bueno por escrito del Departamento de Cómputo.
j) Todo cableado que se pretenda modificar deberá contar con un estudio previo de vialidad estructural y de crecimiento con visto bueno por escrito del Departamento de Cómputo.

7. Respecto a cuentas de usuario:
   a) Estarán conformadas por nombre de usuario y contraseña. Las cuentas deben ser otorgadas únicamente a usuarios legítimos. Se consideran usuarios legítimos a aquellos usuarios quienes hayan realizado el trámite de registro correspondiente y que:
      I. Sean miembros vigentes de la comunidad de la Facultad de Medicina Veterinaria y Zootecnia (alumnos, académicos y personal administrativo)
      II. Participen en proyectos especiales y tengan la autorización del representante del área.
   b) La asignación de cuentas la hará el ATI.
   c) El ATI podrá deshabilitar las cuentas que no se utilicen en un periodo de seis meses.
   d) Las cuentas y contraseñas son personales e intransferibles.
8. Respecto a contraseñas de usuario:
   a) La longitud de una contraseña deberá siempre ser verificada al ser construida. Todas las contraseñas deberán contar con al menos seis caracteres, que podrán ser los siguientes: **a-z, A-Z, 0-9** y caracteres especiales tales como *** + $ % / \ # ¡ ! ¿ ?.**
   b) Todas las contraseñas elegidas por los usuarios deben tener la complejidad necesaria para que sean difíciles de deducir. No deben ser utilizadas palabras que aparezcan en el diccionario, secuencias conocidas de caracteres, datos personales ni acrónimos.
   c) La comunicación de la contraseña se realizará de manera personal y no se podrá informar a otra persona que no sea el interesado.
   d) No se podrán informar contraseñas vía telefónica.
   e) Las contraseñas deberán cambiarse cada seis meses.
   f) Los usuarios no deben construir contraseñas idénticas o muy parecidas a contraseñas anteriores.
9. Respecto a los niveles de acceso de las cuentas de usuario:
   a) Se definen dos niveles de acceso a los equipos de cómputo: con privilegios y sin privilegios. Las cuentas de usuario con privilegios tendrán acceso a instalación de hardware o software, eliminación de hardware o software, etc., este tipo de cuentas se proponen para todos los funcionarios y para aquellos usuarios que el titular de la coordinación, secretaría, departamento académico o administrativo crea conveniente. Las cuentas de usuario sin privilegios sólo podrán hacer uso del software y hardware ya instalado en el equipo de cómputo, podrán crear, modificar y eliminar archivos creados en su cuenta. Este tipo de cuenta se ha ideado principalmente para

colaboradores de las distintas áreas y usuarios temporales (por ejemplo, estudiantes de posgrado, residentes, prestadores de servicio social).

POLÍTICAS DE USO ADECUADO

1. Políticas permisivas:

a) Alumnos:

I. Realizar sus tareas con fines académicos y asociadas con los programas académicos de la FMVZ.
II. Utilizar los servicios de Internet con fines académicos únicamente.
III. Utilizar software de aplicación ya instalado.
IV. Utilizar los servicios de impresión donde se brinden.

b) Académicos, Investigadores y Administrativos

I. Utilizar el equipo de cómputo asignado para realizar sus actividades y funciones.
II. El Departamento de Cómputo contará con un área de investigación de seguridad en cómputo. Dicha área será la única a la que se le permitirá realizar pruebas e investigación de seguridad informática, en ambientes controlados.
III. En caso de que el personal académico o administrativo tenga la necesidad de utilizar equipo de cómputo personal en sus actividades en la FMVZ, deberá registrar ese equipo en el Departamento de Cómputo, previa notificación por escrito, avalada por el jefe del área, describiendo la razón del uso de dicho equipo.

2. Políticas prohibitivas:

a) Ejecutar programas que intenten adivinar las contraseñas alojadas en las tablas de usuarios de equipos de cómputo locales o remotos.
b) Hacer uso de herramientas propias de delincuentes informáticos, tales como programas que rastrean vulnerabilidades en sistemas de cómputo propios o ajenos, ya que dicha conducta puede tipificar en delito al acceder sin autorización a equipos de informática.
c) Hacer uso de programas que explotan alguna vulnerabilidad de un sistema de cómputo para proporcionar privilegios no otorgados explícitamente por el ATI.
d) Instalar programas y software personal; en caso de requerirse deberá solicitarse por escrito al Departamento de Cómputo con visto bueno por el jefe de área.
e) Hacer uso bajo ninguna circunstancia de cualquiera de las computadoras con propósitos de ocio o lucro. Por lo tanto, se prohíbe descargar o proveer música, imágenes, videos, etc., con fines de ocio o lucro.
f) Instalar servidores http, ftp, DHCP, DNS, Proxy, etc., sin la autorización previa por escrito del Departamento de Cómputo.

g) Instalar equipos activos de red, tales como: switches, concentradores, enrutadores, puntos de acceso inalámbrico etc., sin autorización previa por escrito del Departamento de Cómputo.

POLÍTICAS DE RESPALDOS

1. El usuario es responsable de:
   a) Mantener una copia de la información que considere pertinente.
2. El ATI es responsable de:
   a) Realizar respaldos de la información crítica, siempre que tenga los medios físicos para realizarla.
   b) Es el responsable de restaurar la información.
   c) Mantener una versión reciente de los archivos más importantes de los sistemas de cómputo.
   d) Almacenar la información respaldada en un lugar seguro.
   e) Borrar la información respaldada cuando deje de ser útil a la organización, antes de deshacerse del medio.

POLÍTICAS DE CORREO ELECTRÓNICO PROPORCIONADO POR LA INSTITUCIÓN (@correo.unam.mx, @servidor.unam.mx y @correo.fmvz.unam.mx)

1. El usuario es la única persona autorizada para leer su correo, a menos que su cuenta esté involucrada en un incidente de seguridad de cómputo, situación en la cual el administrador del sistema podrá auditar dicha cuenta.
2. Está estrictamente prohibido usar la cuenta de correo electrónico para propósitos ajenos a actividades académicas o laborales según sea el caso.
3. Está prohibido enviar correos conteniendo injurias, falsedades y lenguaje soez.
4. Está prohibido enviar correos sin remitente y sin asuntos.
5. Está prohibido enviar por correo virus, archivos o información que ponga en peligro la seguridad de los sistemas de correo electrónico o el flujo normal de la red de datos de la FMVZ.
6. Está prohibido enviar correos SPAM.
7. Está prohibido enviar correos que contengan publicidad personal o con intereses personales.
8. Está prohibido enviar correos haciéndose pasar por otra persona.
9. Está prohibido reenviar cadenas, chistes y toda clase de información intrascendente, ajena a la actividad académica o laboral del usuario.
10. El ATI podrá deshabilitar cualquier cuenta que incurra en los puntos anteriores.
11. El ATI tiene la facultad de dar de baja temporal el sistema por mantenimiento, previo aviso a los usuarios afectados.

POLÍTICAS DE AUDITORÍA DE LOS SERVICIOS DE CÓMPUTO

1. El ATI deberá contar con herramientas de auditoría de los sistemas de cómputo.
2. Los usuarios en ninguna situación podrán realizar monitoreos de la red de datos de la FMVZ.

3. El ATI o el administrador de la red de datos de la FMVZ tendrán la facultad de realizar auditorías permanentemente a los equipos de cómputo, sistemas de cómputo y a la red de telecomunicaciones.

POLÍTICAS DE USO DE DIRECCIONES IP Y ACCESO A INTERNET

1. El Departamento de Cómputo deberá contar con un registro de direcciones IP utilizadas.
2. Ningún área puede hacer uso de una dirección IP que no le corresponda, sin autorización expresa y escrita del ATI o el administrador de la red de datos de la FMVZ.
3. Ningún usuario podrá hacer modificación en la configuración de la dirección IP asignada a la computadora que está bajo su resguardo.
4. Cada computadora que pretenda ser incorporada la red de datos de la FMVZ deberá ser configurada previamente en el Departamento de Apoyo Técnico en Cómputo.
5. Se permite el uso de rangos de direcciones privadas 192.168.X.X, pero su asignación podrá ser únicamente para los equipos existentes en esa área y estará bajo la supervisión del ATI o el administrador de la red de datos de la FMVZ.
6. Las direcciones IP que podrán otorgarse serán no homologadas o privadas. Las homologadas o públicas sólo serán otorgadas si se justifica ampliamente el uso y estará sujeto a disponibilidad.
7. El ATI o el administrador de la red de datos de la FMVZ podrán realizar reasignaciones de los rangos de las direcciones IP homologadas y privadas para un mejor desempeño de la red.
8. El ATI o el administrador de la red de datos de la FMVZ son los únicos autorizados para solicitar el alta, baja o cambios de nombres canónicos de hosts, alias y mail exchangers ante la Dirección General de Servicios de Cómputo Académico.
9. En cuestión de acceso a la red de datos, se ofrecen dos tipos de acceso a la red, filtrado y parcialmente filtrado. El primero se refiere a la revisión y bloqueo de comunicaciones no deseadas en la red de datos (programas que fomentan la violación de derechos de autor y permiten la descarga de audio, video, software propietario, entre otros), así como algunos sitios web potencialmente peligrosos en cuanto al esparcimiento de virus informáticos; el segundo sólo revisa y bloquea aquellas comunicaciones que se tengan bien identificadas como potencialmente dañinas para el correcto funcionamiento del entorno de red de la Facultad. Cabe señalar que estos perfiles de acceso a la red son genéricos, de tal forma que se pueden crear según lo crea conveniente el responsable del área, esto es, se pueden bloquear los programas de mensajería instantánea, sólo permitir el acceso a sitios de la UNAM, a ciertas páginas web, etc.

POLÍTICAS DE NOMBRES DE PC

1. El Departamento de Cómputo deberá contar con un registro de nombres de PC asignados a direcciones IP.

2. Ningún usuario podrá hacer modificación en la configuración del nombre de la PC.
3. El nombre de la PC estará construido por la siguiente nomenclatura **AAA-bcecdxtr**

AAA	b	cecdxtr
Clave de departamento o área	Primer letra del primer nombre de usuario	letras del primer apellido de usuario hasta completar 8

POLÍTICAS DE CONTRATACIÓN Y FINALIZACIÓN DE RELACIONES LABORALES DE RECURSOS HUMANOS EN SISTEMAS INFORMÁTICOS

1. No podrán ser contratados como administradores de sistemas o en áreas de seguridad informática personas que hayan tenido responsabilidades en incidentes de seguridad.
2. Al finalizar la relación laboral por cualquier motivo, los administradores o encargados de los sistemas de cómputo deberán entregar al jefe inmediato todas las cuentas y contraseñas de los sistemas a su cargo.
3. Los responsables de los sistemas de cómputo deberán cambiar todas las contraseñas críticas cuando un administrador de su área deje de prestar sus servicios para el área de informática.

POLÍTICA DE SANCIONES

1. Si llegase a ocurrir un incidente grave, se informará al Departamento de Seguridad en Cómputo de la DGSCA y se seguirán los procedimientos establecidos por éste. Como medida precautoria y teniendo como prioridad el mantener la seguridad de los sistemas de cómputo, las cuentas o direcciones IP involucradas se deshabilitarán en toda la FMVZ hasta que se deslinden las responsabilidades del incidente.
2. Se aplicarán las siguientes sanciones a los usuarios de los **Laboratorios de Cómputo Académico**

Actividad no permitida	Sanción
Consumo de alimentos, bebidas, utilización de los servicios por ocio o lucro	Suspensión del servicio por un día. Si reincide, cancelación de los servicios en todos los Laboratorios de Cómputo Académico de la FMVZ por un mes
Ejecución de programas que intenten adivinar cuentas y contraseñas locales o remotas Ejecución de herramientas para rastrear vulnerabilidades en sistemas de cómputo propios o ajenos	Suspensión de los servicios por un año en todos los Laboratorios de Cómputo Académico de la FMVZ. Si reincide, cese definitivo de los servicios de cómputo durante toda su estancia en la FMVZ, y en su caso, al poder ser considerado como un delito, se turnará a la Unidad Jurídica de la FMVZ para

Uso de programas que explotan alguna vulnerabilidad del sistema Cambio de la configuración de los equipos que afecte su funcionamiento Envíos de falsas alarmas o mensajes que atenten contra la integridad física o moral de las personas Utilización de los servicios con fines de ocio o lucro	los efectos correspondientes
Instalación de software externo al oficial	Suspensión del servicio por una semana. Si reincide, suspensión por un mes de todos los Laboratorios de Cómputo Académico de la FMVZ

Estas sanciones, que pueden imponerse a los alumnos de la FMVZ, son independientes de aquéllas que se mencionan en la Legislación Universitaria

3. Se aplicarán las siguientes sanciones a los usuarios **académicos y administrativos**

Actividad no permitida	Sanción
Consumo de alimentos, bebidas, utilización de los servicios por ocio o lucro Utilización una sesión activa ajena Acceso con una cuenta diferente a la propia Ejecución de programas que intenten adivinar cuentas y contraseñas locales o remotas Ejecución de herramientas para rastrear vulnerabilidades en sistemas de cómputo propios o ajenos Instalación de software externo al oficial Cambio de la configuración de los	Se emitirá una amonestación firmada por el Director de la FMVZ. En caso de reincidencia se harán del conocimiento del Director de la FMVZ los hechos constitutivos de sanción, siendo éste quién podrá proceder respecto a las sanciones conforme a lo establecido en la Legislación Universitaria y el Contrato Colectivo de Trabajo aplicable

Actividad no permitida	Sanción
equipos que afecte su funcionamiento Envíos de falsas alarmas o mensajes que atenten contra la integridad física o moral de las personas Cualquier violación por parte de algún académico, investigador, trabajador administrativo, residente, etc., de la política de uso de direcciones IP Violación de las políticas por parte de un académico, investigador, trabajador, en un incidente no grave Utilización de los servicios con fines no académicos, ocio o lucro	

4. En caso de robo y daño físico de equipo y material de forma intencional, el responsable tendrá que resarcir los daños, turnándose el asunto a la Unidad Jurídica de la FMVZ.

POLÍTICAS DE EJERCICIO PRESUPUESTAL

1. El presupuesto anual de la partida centralizada 514 para compra de equipo de cómputo será asignado por el CCFMVZ.
2. No se considera obligación del CCFMVZ ni del Departamento de Cómputo adquirir equipo de cómputo individual para los académicos; sin embargo, se propiciará que cada departamento adquiera dicho equipo con ingresos extraordinarios o con presupuesto asignado al mismo.

TRANSITORIOS

Único: El presente reglamento entrará en vigor al día siguiente de haber sido aprobado por el H. Consejo Técnico.

GLOSARIO

Administrador. El responsable de mantener en operación continua los recursos de cómputo con los que cuenta un sitio.
Alias de host. Designación adicional que puede recibir un host (por ejemplo, un alias para el host web de la FMVZ es www.fmvz.unam.mx)
Ataque. Un incidente cuyo objetivo es causar daño a un sistema, robar información del mismo, o utilizar sus recursos de forma no autorizada.
Centro de cómputo. Salas de cómputo y/o salas de procesamiento de información que cuenten con equipamiento de cómputo.
Centro de operaciones. Es el área que se encarga del funcionamiento y operación de las tecnologías de información y comunicaciones de la FMVZ.
Centro de telecomunicaciones. Espacio designado en la dependencia a los equipos de telecomunicaciones y servidores.
Departamento de Seguridad en Cómputo. Es un punto de encuentro al cual puede acudir la comunidad de cómputo para obtener información, asesorías y servicios de seguridad; así como para intercambiar experiencias y puntos de vista, logrando con ello, establecer políticas de seguridad adecuadas, disminuir la cantidad y gravedad de los problemas de seguridad y difundir la cultura de la seguridad en cómputo**.**
DGSCA. Dirección General de Servicios de Cómputo Académico de la UNAM es la entidad universitaria encargada de la operación de los sistemas centrales de cómputo académico y de las telecomunicaciones de la institución.
DHCP. Protocolo de Configuración Dinámica de Host. Asigna automáticamente direcciones IP a las computadoras conectadas a la red de datos.
Dirección IP. Identificador lógico único para cada equipo conectado en una red de computadoras.
DNS. Es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar distintos tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.
Firewall. Un dispositivo de hardware y software que actúa como una barrera protectora entre una red privada y el mundo exterior; se usa para proteger el acceso a los recursos internos desde el exterior, así como para controlar los recursos externos que son accedidos desde la red privada.
FTP. Protocolo de Transferencia de Archivos, permite el intercambio de archivos cliente/servidor.
Herramientas de seguridad. Programas que permiten incrementar la confiabilidad de un sistema de cómputo. Existe una gran variedad de ellos, casi todos de libre distribución. Algunos ejemplos de herramientas de seguridad a considerar para implementar un esquema de seguridad son:
http. Protocolo de Transferencia de Hiper Texto, permite el intercambio de hipertexto. Es el protocolo sobre el que funcionan los sitios Web.
Incidente de seguridad. Un evento que pone en riesgo la seguridad de un sistema de cómputo.

Mail exchanger. Designación de función de intercambiador de correo electrónico que puede recibir un host (por ejemplo, un host mail exchanger es servidor.unam.mx)

Nombre canónico de host. Nombre formal que recibe un host dentro de un dominio registrado en el DNS (por ejemplo, el nombre canónico del host web de la FMVZ es cuauhtli.fmvz.unam.mx)

- Para auditoría interna: COPS, Tiger, Tripwire
- Para control de acceso: TCP-Wrapper, PortSentry
- Para el manejo de autenticación: Kerberos, SecureRPC
- Para el manejo de contraseñas: anipasswd, passwd+, crack, John The Ripper, S/Key
- Para el monitoreo de redes: Satan, ISS

Sistema de detección de intrusos (SDI). SDI es la abreviatura de Sistema de Detección de Intrusos. Es el arte de detectar actividad inapropiada, incorrecta o anónima. Los sistemas de Detección de Intrusos que operan en un host para detectar actividad maliciosa se conocen como Sistemas de Detección de Intrusos para host y los sistemas DI que operan en el flujo de datos de una red se conocen como sistemas de Detección de Intrusos para red.

Sitio. Cualquier organización (militar, gubernamental, comercial, académica, etc.) que posea recursos relativos a redes y computadoras.

SPAM. Mensaje de correo electrónico no solicitado por el receptor, usualmente distribuido a una lista de direcciones y cuyo contenido generalmente es publicidad de productos o servicios.

Usuario. Cualquier persona que hace uso de alguno de los recursos de cómputo con los que cuenta una organización.

Virus informático. Pieza de código ejecutable con habilidad de reproducirse, regularmente escondido en documentos electrónicos, que causan problemas al ocupar espacio de almacenamiento, así como destrucción de datos y reducción del desempeño de un equipo de cómputo.