Asociación de Universidades e Instituciones
de Educación Superior
Consejo Regional Noroeste

POLÍTICAS INSTITUCIONALES DE SEGURIDAD EN CÓMPUTO

Red de Seguridad en Cómputo
del Consejo Regional Noroeste de la ANUIES

Nuestro reconocimiento: Documento basado en el trabajo desarrollado por la
Red de Seguridad en Cómputo en el año 2003,
del Consejo Regional Sur-Sureste de la ANUIES

Octubre 2004

CAPÍTULO 1 6

DISPOSICIONES GENERALES 6

Artículo 1. Ámbito de aplicación y fines 6

Artículo 2. Definiciones 6

Artículo 3. Frecuencia de evaluación de las políticas. 7

CAPÍTULO 2 8

POLÍTICAS SEGURIDAD FÍSICA 8

Artículo 4. Acceso Físico 8

Artículo 5. Robo de Equipo 8

Artículo 6. Protección Física 8

Artículo 7. Respaldos 9

CAPÍTULO 3 10

POLÍTICAS DE SEGURIDAD LÓGICA 10

DE LA RED DE LA INSTITUCIÓN DE EDUCACIÓN SUPERIOR 10

Artículo 8. De la Red-IES 10

Artículo 9. De las Dependencias de la Institución de Educación Superior 10

Artículo 10. Políticas de uso aceptable de los usuarios 11

Artículo 11. De los servidores de la Red-IES 11

Artículo 12. Del Sistema Institucional de Información 12

CAPÍTULO 4 14

POLÍTICAS DE SEGURIDAD LÓGICA 14

PARA ADMINISTRACIÓN DE LOS RECURSOS DE CÓMPUTO 14

Artículo 13. Área de Seguridad en Cómputo 14

Artículo 14. Administradores de Tecnologías de Información 14

Artículo 15. Renovación de Equipo 15

CAPÍTULO 5 16

POLÍTICAS DE SEGURIDAD LÓGICA 16

PARA EL USO DE SERVICIOS DE RED 16

Artículo 16. Servicios en las dependencias universitarias 16

Artículo 17. Uso de los Servicios de red por los usuarios 16

CAPÍTULO 6 18

POLÍTICAS DE SEGURIDAD LÓGICA 18

PARA EL USO DEL ANTIVIRUS INSTITUCIONAL 18

Artículo 18. Antivirus de la Red-IES 18

Artículo 19 Políticas antivirus de las dependencias universitarias 18

Artículo 20. Uso del Antivirus por los usuarios 18

CAPÍTULO 7 20

POLÍTICAS DE OPERACIÓN DE LOS CENTROS DE CÓMPUTO 20

CAPÍTULO 8 21

SANCIONES 21

Artículo 21. Generales 21

ANEXO 1 22

REGLAMENTO DE LOS CENTROS DE CÓMPUTO 22

Capítulo I. Generales 22

Capítulo II. Derechos 24

Capítulo III. Obligaciones 24

Capítulo IV. Restricciones 25

Capítulo V. Sanciones 25

ANEXO RCC1 del Artículo 13b **26**

Equipo Multimedia **26**
Responsabilidad 26
Uso 26

De las Impresiones **26**
Impresión de trabajos. 26
Procedimiento para solicitar servicio de Impresión. 26
Tipos de impresión que se permiten. 26

De las Instalaciones **26**
Limpieza 26
Escaleras y pasillos. 27
Sanitarios 27

Transitorios **27**
Primero. Imprevistos 27
Segundo Vigencia 27

ANEXO 2 **28**

MODELO DE PROTECCIÓN ELÉCTRICA EN INSTALACIONES DE SISTEMAS DE CÓMPUTO Y COMUNICACIONES **28**

1. Capturar la descarga atmosférica en un punto designado. 28

2. Conducir sin riesgo la descarga a tierra en forma segura. 28

3. Disipar la energía a tierra. 28

4. Crear un plano de tierra equipotencial. 28

5. Proteger contra transitorios entrantes por los circuitos de potencia. 31

6. Proteger contra transitorios entrantes por los circuitos de comunicación/datos. 31

REQUISITOS DE TELECOMUNICACIONES **32**

CAPÍTULO 1
DISPOSICIONES GENERALES

Artículo 1 Ámbito de aplicación y fines

1.1 Las políticas de seguridad en cómputo tienen por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes de telemática) y personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios de cómputo de las Instituciones de Educación Superior del consejo regional Noroeste de la ANUIES.

1.2 Cada Institución de Educación Superior es la responsable de dar a conocer y hacer cumplir estas políticas de seguridad internamente.

1.3 Las Instituciones de Educación Superior pueden agregar guías particulares complementarias de acuerdo a su naturaleza y funciones.

Artículo 2. Definiciones

ABD: Administrador de las bases de datos del Sistema Institucional de Información de la IES.

ASC-IES: Área de Seguridad en Cómputo de la Institución de Educación Superior. Se encarga de definir esquemas y políticas de seguridad en materia de cómputo para la Institución.

ATI: Administrador de Tecnologías de Información. Responsable de la administración de los equipos de cómputo, sistemas de información y redes de telemática de una dependencia de la Institución de Educación Superior.

Base de datos: Colección de archivos interrelacionados.

CAV: Central Antivirus.

Centro de cómputo: Salas de cómputo y/o salas de procesamiento de información que cuenten con equipamiento de cómputo.

Centro de Operaciones: Es la dependencia que se encarga del funcionamiento y operación de las Tecnologías de Información y comunicaciones de la IES.

Centro de telecomunicaciones: Espacio designado en la dependencia a los equipos de telecomunicaciones y servidores. 7

Contraseña: Conjunto de caracteres que permite el acceso de un usuario a un recurso informático.

Dependencia: Es toda Facultad, Escuela, Dirección, Subdirección, Departamento y Centro de Investigaciones de la IES.

IES: Institución de Educación Superior

NOC: Network Operation Center.

Recurso informático: Cualquier componente físico o lógico de un sistema de información.

Red-IES: Equipos de cómputo, sistemas de información y redes de telemática de una Institución de Educación Superior.

RSC-ANUIESNW: Red de Seguridad en Cómputo del consejo Regional Noroeste de la ANUIES.

SII-IES: Sistema Institucional de Información de la Institución de Educación Superior.

Solución Antivirus: Recurso informático empleado en la IES para solucionar problemas con virus.

TIC: Tecnologías de Información y Comunicaciones

Usuario: Cualquier persona que haga uso de los servicios proporcionados por la Institución de Educación Superior, responsables de los equipos de cómputo, sistemas de información y redes de telemática.

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.

Artículo 3. Frecuencia de evaluación de las políticas.

3.1 Se evaluarán las políticas del presente documento, con una frecuencia anual por la Red de Seguridad en Cómputo del consejo regional Noroeste

3.2 Las políticas de cada Institución de Educación Superior serán evaluadas por el Área de seguridad en cómputo de la IES con una frecuencia semestral.

CAPÍTULO 2
POLÍTICAS SEGURIDAD FÍSICA

Artículo 4. Acceso Físico

4.1 Todos los sistemas de comunicaciones estarán debidamente protegidos con infraestructura apropiada de manera que el usuario no tenga acceso físico directo. Entendiendo por sistema de comunicaciones: el equipo activo y los medios de comunicación.

4.2 Las visitas deben portar una identificación con un código de colores de acuerdo al área de visita, que les será asignado por el centro de cómputo.

4.3 Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un responsable del área con permiso de la autoridad correspondiente.

4.4 Se deberán establecer horarios de acceso a instalaciones físicas, especificando los procedimientos y en qué casos se deberá hacer excepciones.

4.5 Se debe definir qué personal está autorizado para mover, cambiar o extraer equipo de la IES a través de identificaciones y formatos de E/S; y se debe informar de estas disposiciones a personal de seguridad.

Artículo 5. Robo de Equipo

5.1 La IES deberá definir procedimientos para inventario físico, firmas de resguardo para préstamos y usos dedicados de equipos de tecnología de información.

5.2 El resguardo de los equipos de comunicaciones deberá quedar bajo el área o persona que los usa, permitiendo conocer siempre la ubicación física de los equipos.

5.3 El centro de operaciones, así como las áreas que cuenten con equipos de misión crítica deberán contar con vigilancia y/o algún tipo de sistema que ayude a recabar evidencia de accesos físicos a las instalaciones.

Artículo 6. Protección Física

6.1 Las puertas de acceso a las salas de cómputo deben ser preferentemente de vidrio transparente, para favorecer el control del uso de los recursos de cómputo.

6.2 El centro de telecomunicaciones de la IES debe:

- Recibir limpieza al menos una vez por semana, que permita mantenerse libre de polvo.
- Ser un área restringida.
- Estar libre de contactos e instalaciones eléctricas en mal estado
- Contar por lo menos con un extinguidor de incendio adecuado y cercano al centro de telecomunicaciones.

6.3 El centro de telecomunicaciones deberá seguir los estándares vigentes para una protección adecuada de los equipos de telecomunicaciones y servidores (Anexo 2).

6.4 Los sistemas de tierra física, sistemas de protección e instalaciones eléctricas del centro de telecomunicaciones deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.

6.5 Cada vez que se requiera conectar equipo de cómputo, se deberá comprobar la carga de las tomas de corriente.

6.6 Contar con algún esquema que asegure la continuidad del servicio.

6.7 Se deberá tener fácil acceso a los procedimientos de contingencias.

6.8 Se deberá contar con un botiquín de primeros auxilios.

6.9 Se deberán contar con rutas de evacuación y sus señalamientos correspondientes.

6.10 Se programarán simulacros de evacuación en casos de contingencia

Artículo 7. Respaldos

7.1 La Base de Datos del SII-IES será respaldada diariamente en forma automática y manual, según los procedimientos generados para tal efecto.

7.2 Los respaldos del SII-IES deberán ser almacenados en un lugar seguro y distante del sitio de trabajo.

CAPÍTULO 3

POLÍTICAS DE SEGURIDAD LÓGICA DE LA RED DE LA INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Artículo 8. De la Red-IES

8.1 La Red-IES tienen como propósito principal servir en la transformación e intercambio de información entre organizaciones académicas y de investigación, entre éstas y otros servicios locales, nacionales e internacionales, a través de conexiones con otras redes.

8.2 Si una aplicación en la red es coherente con los propósitos de las Red-IES, entonces las actividades necesarias para esa aplicación serán consistentes con los propósitos de la TIC-IES.

8.3 La Red-IES no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.

8.4 Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos de las IES sin el consentimiento explícito responsable del equipo.

8.5 No se permite interferir o interrumpir las actividades de los demás usuarios por cualquier medio o evento salvo que las circunstancias así lo requieran, como casos de contingencia, los cuales deberán ser reportados en su momento a sus autoridades correspondientes.

8.6 No se permite el uso de los servicios de la red cuando no cumplan con los quehaceres establecidos.

8.7 Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de la IES y se usarán exclusivamente para actividades relacionadas con la institución.

8.8 Todas las cuentas de acceso a los sistemas y recursos de cómputo de la RED-IES son personales e intransferibles, se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.

8.9 El uso de analizadores de red es permitido única y exclusivamente por el personal del Centro de operaciones de la red y por los ATI que ellos autoricen para monitorear la funcionalidad de la Red-IES, contribuyendo a la consolidación del sistema de seguridad en la IES bajo las políticas y normatividades de la IES.

8.10 No se permitirá el uso de analizadores para monitorear o censar redes ajenas a las IES y no se deberán realizar análisis de la Red-IES desde equipos externos a la IES.

8.11 Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectará temporal o permanentemente al usuario o red involucrados dependiendo de la normatividad de la IES. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

Artículo 9. De las Dependencias de la Institución de Educación Superior

9.1 Las Dependencias deben llevar un control total escrito y/o sistematizado de sus recursos de cómputo.

9.2 Las Dependencias son las responsables de calendarizar y organizar al personal encargado del mantenimiento preventivo y correctivo de los equipos de cómputo.

9.3 Las Dependencias deberán reportar al ATI y/o al Centro de Operaciones de la RED-IES cuando un usuario deje de laborar o de tener una relación con la institución.

9.4 Si una dependencia viola las políticas vigentes de uso aceptable de la Red-IES, el Centro de Operaciones de la Red-IES aislará la red de esa dependencia.

9.5 Para reforzar la seguridad de la información de la cuenta bajo su criterio deberá hacer respaldos de su información dependiendo de la importancia y frecuencia del cambio de la misma.

9.6 Los administradores no podrán remover del sistema ninguna información de cuentas individuales, a menos que la información sea de carácter ilegal, o ponga en peligro el buen funcionamiento de los sistemas, o se sospeche de algún intruso utilizando una cuenta ajena.

Artículo 10. Políticas de uso aceptable de los usuarios

10.1 Los recursos de cómputo empleados por el usuario:

- Deberán ser afines al trabajo desarrollado.
- No deberán ser proporcionados a personas ajenas.
- No deberán ser utilizados para fines personales.

10.2 Todo usuario debe respetar la intimidad, confidencialidad y derechos individuales de los demás usuarios.

10.3 El correo electrónico no se usará para envío masivo, materiales de uso no académico o innecesarios (entiéndase por correo masivo todo aquel que sea ajeno a la institución, tales como cadenas, publicidad y propaganda comercial, política o social, etcétera).

10.4 Para reforzar la seguridad de la información de su cuenta, el usuario –conforme su criterio- deberá hacer respaldos de su información, dependiendo de la importancia y frecuencia de modificación de la misma.

10.5 Queda estrictamente prohibido inspeccionar, copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de derechos de autor.

10.6 Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de cómputo y red de la IES, de acuerdo con las políticas que en este documento se mencionan.

10.7 Los usuarios deberán solicitar apoyo al ATI de su dependencia ante cualquier duda en el manejo de los recursos de cómputo de la institución.

Artículo 11. De los servidores de la Red-IES

11.1 El Centro de Operaciones de la Red-IES tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red-IES.

11.2 La instalación y/o configuración de todo servidor conectado a la Res-IES deberá ser notificada al Centro de Operaciones de la Red-IES.

11.3 Durante la configuración del servidor los ATI deben normar el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios.

11.4 Los servidores que proporcionen servicios a través de la RED-IES e Internet deberán:

1. Funcionar 24 horas del día los 365 días del año.
2. Recibir mantenimiento preventivo semanal.

3.Recibir mantenimiento mensual que incluya depuración de bitácoras.
4.Recibir mantenimiento semestral que incluya la revisión de su configuración.
5.Ser monitoreados por el ATI de la Dependencia y por el Centro de Operaciones de la RED-IES.

11.5 La información de los servidores deberá ser respaldada de acuerdo con los siguientes criterios:
Diariamente, los correos e información crítica.
Semanalmente, los documentos web.
Mensualmente, configuración del servidor y bitácoras.

11.6 Los servicios institucionales hacia Internet sólo podrán proveerse a través de los servidores autorizados por el Centro de Operaciones de la Red-IES.

11.7 El Centro de Operaciones de la IES es el encargado de asignar las cuentas a los usuarios para el uso de correo electrónico en los servidores que administra.

11.8 Para efecto de asignarle su cuenta de correo al usuario, éste deberá llenar el formato de solicitud de cuenta con que cuenta la IES y entregarlo al responsable administrativo de la Red-IES, con su firma, como usuario, y la del director de su dependencia.

11.9 Una cuenta deberá estar conformada por un nombre de usuario y su contraseña asignada. El nombre de usuario deberá contar como máximo de 8 caracteres y no deberá contener alias.

11.10 La cuenta será activada en el momento en que el usuario se presente en el Centro de Operaciones de la RED-IES con una identificación personal, siendo el Centro de Operaciones de la RED-IES el responsable de verificar la asignación de la contraseña.

11.11 Los servidores deberán ubicarse en un área física que cumpla las recomendaciones para un centro de telecomunicaciones:

- Acceso restringido.
- Temperatura adecuada.
- Protección contra descargas eléctricas (ver anexo 2).
- Mobiliario adecuado que garantice la seguridad de los equipos.

11.12 En caso de olvido de la contraseña por parte del usuario, el Centro de Operaciones de la RED-IES podrá apoyarse con el ATI de la dependencia para el cambio de contraseña.

Artículo 12. Del Sistema Institucional de Información

12.1. El ABD tendrá acceso a la información de la Base de Datos del SII-IES únicamente para:

- La realización de los respaldos de la BD.
- Solucionar problemas que el usuario no pueda resolver.
- Diagnóstico o monitoreo del SII-IES.

12.2 El Administrador de la Base de Datos del SII-IES no deberá eliminar ninguna información del sistema, a menos que la información esté dañada o ponga en peligro el buen funcionamiento del sistema.

12.3 El Administrador de la Base de Datos del SII-IES es el encargado de asignar las cuentas a los usuarios para el uso del SII-IES. Para tal efecto será necesario seguir el procedimiento determinado por la IES.

12.4 Las contraseñas serán asignadas por el Administrador de la Base de Datos del SII-IES en el momento en que el usuario desee activar su cuenta, previa solicitud al responsable del SII-IES, de acuerdo con el procedimiento generado.

12.5 En caso de olvido de contraseña de un usuario, será necesario que se presente con el Administrador de la Base de Datos del SII-IES para reasignarle su contraseña.

CAPÍTULO 4
POLÍTICAS DE SEGURIDAD LÓGICA
PARA ADMINISTRACIÓN DE LOS RECURSOS DE CÓMPUTO

Artículo 13. Área de Seguridad en Cómputo

13.1 El ASC-IES es el encargado de suministrar medidas de seguridad adecuadas contra la intrusión o daños a la información almacenada en los sistemas así como la instalación de cualquier herramienta, dispositivo o software que refuerce la seguridad en cómputo. Sin embargo, debido a la amplitud y constante innovación de los mecanismos de ataque no es posible garantizar una seguridad completa.

13.2 El ASC-IES debe mantener informados a los usuarios y poner a disposición de los mismos el software que refuerce la seguridad de los sistemas de cómputo de la IES.

13.3 El ASC-IES es el único autorizado para monitorear constantemente el tráfico de paquetes sobre la red, con el fin de detectar y solucionar anomalías, registrar usos indebidos o cualquier falla que provoque problemas en los servicios de la Red-IES.

Artículo 14. Administradores de Tecnologías de Información

14.1 El ATI debe cancelar o suspender las cuentas de los usuarios previa notificación, cuando se le solicite mediante un documento explícito por las autoridades de una Dependencia en los siguientes casos:

- Si la cuenta no se está utilizando con fines institucionales.
- Si pone en peligro el buen funcionamiento de los sistemas.
- Si se sospecha de algún intruso utilizando una cuenta ajena.

14.2 El ATI deberá ingresar de forma remota a computadoras única y exclusivamente para la solución de problemas y bajo solicitud explícita del propietario de la computadora.

14.3 El ATI deberá utilizar los analizadores previa autorización del ASC-IES y bajo la supervisión de éste, informando de los propósitos y los resultados obtenidos.

14.4 El ATI deberá realizar respaldos periódicos de la información de los recursos de cómputo que tenga a su cargo, siempre y cuando se cuente con dispositivos de respaldo.

14.5 El ATI debe actualizar la información de los recursos de cómputo de la Dependencia a su cargo, cada vez que adquiera e instale equipo o software.

14.6 El ATI debe registrar cada máquina en el padrón único de control de equipo de cómputo y red de la Dependencia a su cargo.

14.7 El ATI debe auditar periódicamente los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados, configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.

14.8 EL ATI debe realizar la instalación o adaptación de sus sistemas de cómputo de acuerdo con las solicitudes del ASC-IES en materia de seguridad.

14.9 Es responsabilidad del ATI revisar diariamente las bitácoras de los sistemas a su cargo.

14.10 EL ATI reportará al ASC-IES los incidentes de seguridad, de acuerdo con el formato de control de incidentes de la IES, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.

Artículo 15. Renovación de Equipo

14.1 Se deberán definir los tiempos estimados de vida útil de los equipos de cómputo y telecomunicaciones para programar con anticipación su renovación.

CAPÍTULO 5

POLÍTICAS DE SEGURIDAD LÓGICA PARA EL USO DE SERVICIOS DE RED

Artículo 16. Servicios en las dependencias universitarias

16.1 Cada dependencia definirá los servicios de red a ofrecer en los servidores e informará al Centro de operaciones de la red para su autorización.

16.2 Las dependencias pueden utilizar la infraestructura de la RED-IES para proveer servicios a los usuarios de la misma dependencia y/o pertenecientes a la IES.

16.3 El ATI es el responsable de la administración de contraseñas y deberá guardar su confidencialidad, siguiendo el procedimiento para manejo de contraseñas de la IES.

16.4 La Dependencia deberá notificar al ATI cuando un usuario deje de laborar o de tener relación con la IES.

16.5 La Dependencia deberá notificar al Centro de operaciones cuando el ATI deje de tener alguna relación oficial con la Dependencia o con la IES.

16.6 El ATI realizará las siguientes actividades en los servidores de su dependencia:

- Respaldo de información conforme a los procedimientos indicados por el centro de operaciones.
- Revisión de bitácoras y reporte cualquier eventualidad al Centro de Operaciones de la RED-IES.
- Implementar de forma inmediata las recomendaciones de seguridad proporcionados por el ASC-IES y reportar el Centro de operaciones posibles faltas a las políticas de seguridad en cómputo.
- Monitoreo de los servicios de red proporcionados por los servidores a su cargo.
- Calendarizar y organizar y supervisar al personal encargado del mantenimiento preventivo y correctivo de los servidores.

16.7 El ATI es el único autorizado para asignar las cuentas a los usuarios de su dependencia con previa anuencia de las autoridades de la misma.

16.8 El Centro de Operaciones de la RED-IES aislará cualquier servidor de red, notificando a los ATI y autoridades de la Dependencia, en las condiciones siguientes:

- Si los servicios proporcionados por el servidor implican un tráfico adicional en la RED-IES.
- Si se detecta la utilización de vulnerabilidades que puedan comprometer la seguridad en la RED-IES.
- Si se detecta la utilización de programas que alteren la legalidad y/o consistencia de los servidores.
- Si se detectan accesos no autorizados que comprometan la integridad de la información.
- Si se viola las políticas de uso de los servidores.
- Si se reporta un tráfico adicional que comprometa a la red de la IES.

Artículo 17. Uso de los Servicios de red por los usuarios

17.1. El usuario deberá definir su contraseña de acuerdo al procedimiento establecido para tal efecto.

17.2 El usuario deberá renovar su contraseña y colaborar en lo que sea necesario, a solicitud del ATI, con el fin de contribuir a la seguridad de los servidores en los siguientes casos:

- Cuando ésta sea una contraseña débil o de fácil acceso.
- Cuando crea que ha sido violada la contraseña de alguna manera.

17.3 El usuario deberá notificar al ATI en los siguientes casos:

- Si observa cualquier comportamiento anormal (mensajes extraños, lentitud en el servicio o alguna situación inusual) en el servidor.
- Si tiene problemas en el acceso a los servicios proporcionados por el servidor.

17.4 Si un usuario viola las políticas de uso de los servidores, el ATI podrá cancelar totalmente su cuenta de acceso a los servidores, notificando a las autoridades de la dependencia correspondiente.

CAPÍTULO 6
POLÍTICAS DE SEGURIDAD LÓGICA
PARA EL USO DEL ANTIVIRUS INSTITUCIONAL

Artículo 18. Antivirus de la Red-IES

18.1 Deberán ser utilizadas en la implementación y administración de la Solución Antivirus.

18.2 Todos los equipos de cómputo de la IES deberán tener instalada la Solución Antivirus.

18.3 Periódicamente se hará el rastreo en los equipos de cómputo de la IES, y se realizarán las siguientes acciones:

- Actualización automática de las firmas antivirus proporcionadas por el fabricante de la Solución Antivirus en los equipos conectados a la RED-IES.
- Actualización manual de las firmas antivirus por el ATI en los equipos no conectados a la RED-IES.

Artículo 19 Políticas antivirus de las dependencias universitarias

19.1 El ATI será el responsable de:

- Implementar la Solución Antivirus en las computadoras de la dependencia.
- Solucionar contingencias presentadas ante el surgimiento de virus que la solución no haya detectado automáticamente.
- Configurar el analizador de red de su dependencia para la detección de virus.
- Notificar a la CAV en caso de contingencia con virus.

19.2 El Centro de Operaciones de la RED-IES aislará la red de una dependencia notificando a las autoridades competentes, en las condiciones siguientes:

- Cuando la contingencia con virus no es controlada, con el fin de evitar la propagación del virus a otras redes de la RED-IES.
- Si la dependencia viola las políticas antivirus.
- Cada vez que los usuarios requieran hacer uso de discos flexibles, éstos serán rastreados por la Solución Antivirus en la computadora del usuario o en un equipo designado para tal efecto en las áreas de cómputo de las dependencias.

19.3 En caso de contingencia con virus el ATI deberá seguir el procedimiento establecido por la IES.

Artículo 20. Uso del Antivirus por los usuarios

20.1 El usuario no deberá desinstalar la solución antivirus de su computadora pues ocasiona un riesgo de seguridad ante el peligro de virus.

20.2 Si el usuario hace uso de medios de almacenamiento personales, éstos serán rastreados por la Solución Antivirus en la computadora del usuario o por el equipo designado para tal efecto.

20.3 El usuario que cuente con una computadora con recursos limitados, contará con la versión ligera de la Solución Antivirus Institucional.

20.4 El usuario deberá comunicarse con el ATI de su dependencia en caso de problemas de virus para buscar la solución.

20.5 El usuario será notificado por el ATI en los siguientes casos:

- Cuando sea desconectado de la red con el fin evitar la propagación del virus a otros usuarios de la dependencia.

- Cuando sus archivos resulten con daños irreparables por causa de virus.
- Si viola las políticas antivirus.

CAPÍTULO 7
POLÍTICAS DE OPERACIÓN DE LOS CENTROS DE CÓMPUTO

Los centros de cómputo podrán ofrecer servicios de cómputo, soporte técnico y servicios audiovisuales.

Cada Dependencia de la IES deberá contar con un reglamento de uso de los centros de cómputo de acuerdo al reglamento de los centros de cómputo presentado en el Anexo 1.

Cada dependencia dará a conocer dicho reglamento mediante diversos mecanismos como pláticas introductorias y la publicación vía web y la entrega del documento.

La administración de los servicios de los centros de cómputo deberá llevarse a través de métodos automatizados.

Los ATI de los Centros de cómputo deberán verificar el grado de seguridad del software adquirido e instalado en los equipos del centro de cómputo.

Para optimizar tiempo y recursos de los Centros de cómputo, las Dependencias deberán contar con los siguientes elementos mínimos: un cañón, conexión a la Red-IES y equipo de cómputo en cada sala. Los equipos deberán ser fijados para evitar alteración o robo de los mismos.

El Centro de cómputo debe contar con: una sala de consulta general, una sala para enseñanza práctica (con computadoras para los alumnos y cañón de vídeo) y una sala de proyección (con cañón de vídeo).

Se podrá dar asesoría siempre y cuando no entorpezca las acciones de mayor relevancia.

El centro de cómputo dará soporte técnico únicamente al equipo de la institución.

Las Dependencias de la IES deberá contar con personal para actividades administrativas, para soporte técnico, para administrar los recursos de cómputo, desarrollo de aplicaciones.

La dependencia deberá contar con servicios automatizados que incluya: Mantenimiento preventivo y correctivo, publicación de documentos de normatividad, inventario,

El centro de cómputo de la IES deberá contar con la siguiente documentación: Información técnica: red, edificios, eléctricas, manuales y procedimientos, normatividad, inventarios de hardware y software, que puedan servir en caso de contingencia.

Se deberá definir el software mínimo que cada computadora deberá contar para su operación.

En caso de daño leve, el personal de soporte técnico deberá reparar o reemplazar en un tiempo definido.

La instalación de Software específico deberá ser realizado en conjunto y común acuerdo del profesor que lo solicite y el ATI. Se requerirá autorización de las autoridades de la dependencia.

CAPÍTULO 8

SANCIONES

Artículo 21. Generales

Cualquier acción que vaya en contra de las políticas de seguridad en cómputo de la IES será sancionada con la suspensión de los servicios de cómputo y red, por un período de tres meses en una primera ocasión y de manera indefinida en caso de reincidencia.

ANEXO 1
REGLAMENTO DE LOS CENTROS DE CÓMPUTO

INTRODUCCIÓN

Con el objeto de proporcionar un buen servicio y adecuado manejo de los equipos existentes en los Centros de Cómputo, la ANUIES ha elaborado el presente reglamento para las IES.

OBJETIVO: Proporcionar servicios de cómputo integral y eficiente para los alumnos y maestros, coadyuvando con la calidad académica de la institución.

CAPÍTULO I

GENERALES

Artículo 1.
Únicamente pueden ser usuarios del Centro de Cómputo:

a) Los empleados de la Institución.
b) Los alumnos inscritos de la Institución.
c) El personal o alumnos de Instituciones previa firma de convenio o autorización.

Artículo 2.
El Horario de servicios del Centro de Cómputo será el estipulado por las dependencias de las IES.

Artículo 3.
Para tener derecho a los servicios:

La Coordinación atenderá las peticiones de los usuarios asignándole el equipo que cubra las expectativas para desarrollar sus actividades, las cuales podrán ser de manera individual o por grupo. En caso de:

a) Reservación individual: El usuario deberá proporcionar su número de matrícula vigente correspondiente.
b) Reservación por grupo: Las realizará en forma personal el catedrático del grupo señalando la cantidad de equipos requeridos:
    i. Con un mínimo de n horas previas a la clase o
    ii. Reservando m horas a la semana durante el periodo escolar, autorizadas por el encargado del Centro de Cómputo.

Articulo 4.
Vigencia de las reservaciones:

a) Las reservaciones individuales se respetarán hasta n minutos, pasado este tiempo se procederá a la cancelación de la reservación.
b) Las reservaciones por grupo serán vigentes durante el periodo escolar.

Articulo 5.
Cancelación de reservaciones:

El usuario podrá cancelar su reservación hasta previo inicio de la misma. La anticipación de la cancelación permite al usuario no hacerse acreedor a sanciones

Artículo 6.
Servicios:

a) Los usuarios deberán respetar las especificaciones que los equipos tengan con respecto al software instalado en general.
b) La mesa de trabajo y el equipo de cómputo asignado, son de uso exclusivo para un usuario
c) Los usuarios solo podrán utilizar el equipo de cómputo que les sea asignado. En caso que éste tenga alguna anomalía, deberán reportarlo al área de control, para que se les proporcione otro equipo.
d) El catedrático que solicite alguna reservación por grupo, deberá permanecer con el grupo durante todo el tiempo asignado a la sala, y será responsable del buen uso de los equipos tanto desde el punto de vista técnico como de la información que en ellas se revise acceda o disponga.
e) Los grupos de alumnos no podrán hacer uso de los equipos en las salas sin la presencia del maestro.
f) El usuario que requiera el uso de software especial que no se encuentre instalado o provisto de manera institucional, deberá solicitarlo a la coordinación de servicios, previa justificación que la sustente.
g) Los usuarios deberán contar con sus discos de trabajo para efectuar los respaldos de su información.

Articulo 7.
La instalación de programas es facultad exclusiva del Centro de Cómputo.

Articulo 8.
Derechos de autor.

Queda estrictamente prohibido inspeccionar, copiar y almacenar software que viole la ley de derechos de autor.

Artículo 9.
El Centro de Cómputo no se hace responsable de la información de los usuarios almacenada en los discos duros locales de los equipos de cómputo.

Artículo 10.
El Centro de Cómputo se reserva el derecho de cancelar el uso de las salas de capacitación, laboratorios y/o servicios

Articulo 11.
Equipo ajeno a la institución.
El usuario que requiera conectar equipos personales a la red o periféricos a las computadoras, deberán contar con la autorización correspondiente de la Coordinación de Servicios.

CAPITULO II

DERECHOS

Articulo12.
Son derechos de los usuarios del Centro de Cómputo:

a) Hacer uso de los servicios de cómputo proporcionados por el Centro de Cómputo
b) Reservar el equipo de cómputo para su uso.
c) Cancelar las reservaciones.
d) Solicitar una cuenta personalizada a la Coordinación de Servicios
e) Respaldar información en su cuenta personalizada y/o unidades magnéticas extraíbles.
f) Disponer del equipo de cómputo durante el tiempo establecido por la dependencia. En caso de requerir un tiempo mayor, deberá solicitarlo al área de control a efecto que se le proporcione, siempre que existan equipos disponibles.
g) Introducir únicamente al área de servicios sus discos y material de trabajo.
h) Recibir el reglamento del Centro de Cómputo y una capacitación del mismo en la fecha y horario que estipule la Coordinación de Servicios.

Artículo 13.
Son derechos de los usuarios maestros:

a) Reservar y utilizar las salas de capacitación y/o el laboratorios de cómputo de sus horas frente a grupo, previo llenado de la solicitud correspondiente con el horario autorizado por el Centro de Cómputo
b) Reservar y utilizar equipo multimedia, proyector de cañón, proyector de acetatos y otros disponibles (apegándose a las recomendaciones del anexo RCC1)
c) Cancelar la reservación de las salas y laboratorio de cómputo

CAPITULO III

OBLIGACIONES

Artículo 14.
Son obligaciones del usuario del Centro de Cómputo:

a) Presentar su credencial de la IES en buen estado, con matrícula y sello vigente.
b) Guardar respeto y debido comportamiento.
c) Vacunar sus discos
d) Cerrar su sesión como usuario de la red
e) Apagar el equipo de cómputo, limpiar y acomodar su área de trabajo al término de su sesión.

CAPITULO IV

RESTRICCIONES

Artículo 15.
Queda estrictamente prohibido al usuario:

a) Introducir alimentos, bebidas, fumar y tirar basura.
b) Introducir cualquier tipo de arma o estupefaciente.
c) Introducir cualquier equipos ajenos a la institución.
d) Transferir su cuenta asignada por el Centro de Cómputo.
e) Modificar los parámetros de configuración de hardware y software instalado.
f) Mover el equipo de Cómputo, mobiliario y cambiar los cables de conexión a la red
g) Conectarse a equipos no autorizados.
h) Realizar trabajos con fines de lucro
i) Utilizar cualquier tipo de juego
j) Utilizar programas de plática en línea (chat's).
k) Utilizar la infraestructura de la institución para lanzar virus
l) Utilizar la infraestructura de la institución para realizar ataques internos o externos
m) Accesar a información que pueda dañar la imagen del instituto: faltas a la moral y a las buenas costumbres
n) Realizar trabajos o funciones de Biblioteca.
o) Ingresar a las áreas exclusivas del personal del Centro de Cómputo.
p) Pasar al área de servicios con bultos, mochilas, gorras y portafolios.

CAPITULO V

SANCIONES

Articulo 16.
Las sanciones a que están sujetos los usuarios por incumplimiento de sus obligaciones e incurrir en las restricciones señaladas, son las siguientes:

a) Llamada de atención de manera verbal o escrita.
b) Suspensión desde 15 días hábiles, hasta el fin del periodo escolar de los servicios del Centro de Cómputo.
c) Suspensión definitiva de los servicios del Centro de Cómputo.
d) Reposición o pago de los bienes extraviados, destruidos o deteriorados.

Aplicación del Reglamento de conducta de alumnos de la IES.

Anexo RCC1 del Articulo 13b

Recomendaciones de uso para el Equipo Multimedia

- Usarse en áreas con aire acondicionado
- Conectarse a tomas de corriente de cómputo, si están disponibles.
- Mantenerse alejados de alimentos y bebidas.
- No forzar las conexiones de los dispositivos de los equipos (éstos solo pueden conectarse de una forma)
- Ubicar los equipos de tal forma que el calor generado por éstos no incida sobre equipos de cómputo.
- No mover ni golpear los equipos cuando están encendidos.
- Poner los equipos en modo de reposo (stand-by) durante al menos 5 minutos antes de apagarlos de manera definitiva.
- Al terminar, enrollar los cables y acomodarlos para un transporte seguro. Sin embargo, los cables no deben enrollarse con radios de curvatura muy pequeños, ya que pueden fracturarse.
- No colocar los proyectores o cañones sobre notebooks ya que la pantalla líquida puede dañarse.
- Evitar dejar sin vigilancia los equipos.

De las Impresiones

Impresión de trabajos.

El servicio de impresión se ofrece en el horario estipulado por la coordinación de servicios (mencionar cuál). Cuando y dónde aplique, el usuario deberá pagar por el servicio. El trabajo deberá encontrarse en su versión final, para evitar retrasos con respecto a otros trabajos. No se permitirá la edición de los mismos durante la impresión. El trabajo impreso, cual fuere su resultado, deberá ser pagado por el alumno (en caso que aplique el pago).

Procedimiento para solicitar servicio de Impresión.

El usuario entregará su disco a las personas encargadas de impresiones e indicará en qué aplicación están hechos los trabajos (de ser diferente, explicar el procedimiento vigente).

Tipos de impresión que se permiten.

No se imprimirán trabajos con fines de lucro ni aquellos que no tengan relación con la Institución.

De las Instalaciones

Limpieza

Es obligación de los usuarios mantener limpias todas las instalaciones, tirando la basura en los botes destinados para este fin.

Escaleras y pasillos.

Está prohibido sentarse en las escaleras y pasillos, ya que se obstaculiza el libre tránsito de personas.

Sanitarios

Es obligación de los usuarios mantener limpios los sanitarios.

Transitorios

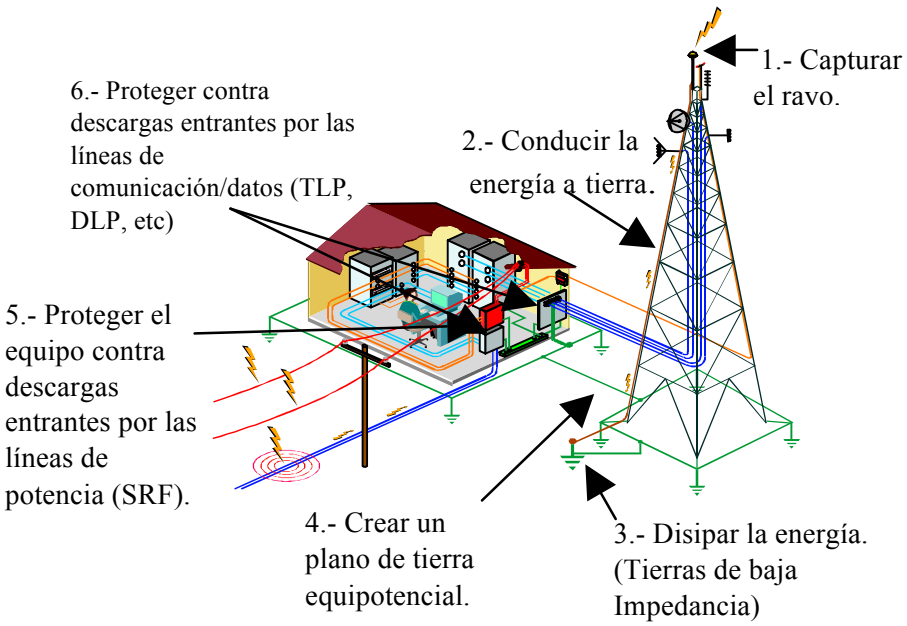
Primero. Imprevistos

Los casos no previstos en este reglamento serán resueltos por la Coordinación de Servicios, entidad administrativa o legal correspondiente.

Segundo Vigencia

Este reglamento entra en vigor cuando la IES así lo determine.

ANEXO 2
MODELO DE PROTECCIÓN ELÉCTRICA EN INSTALACIONES DE SISTEMAS DE CÓMPUTO Y COMUNICACIONES



1.Capturar la descarga atmosférica en un punto designado.

Se requiere contar con una terminal aérea, para una adecuada protección ante descargas eléctricas, el cual deberá aterrizarse a un sistema de tierra física tipo de delta.

2.Conducir sin riesgo la descarga a tierra en forma segura.

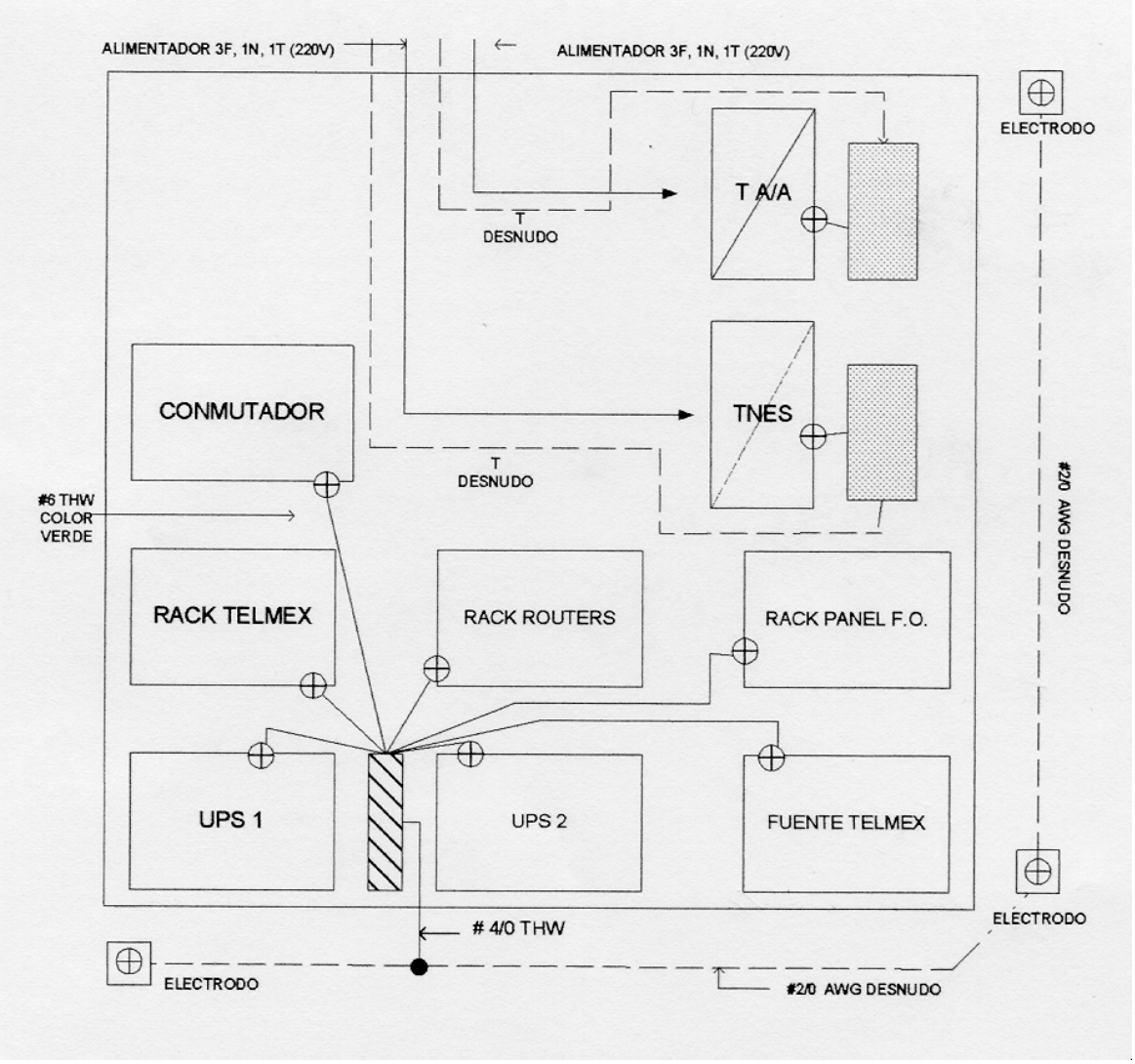
Conductor de cobre, acero o aluminio

3.Disipar la energía a tierra.

Los componentes del sistema de tierra deberan ser: Conector soldadura exotérmica Caldwell, Electrodo, Electrodo a tierra fabricados con una barra de acero recubierta por una gruesa película de cobre (0.254 mm) de acuerdo a las Normas ANSI/UL 467-1984 y ANSI C 33-8, 1972 y Tierra La resistividad del terreno deberá ser considerada con cuidado, incluyendo el contenido de humedad y la temperatura.

4.Crear un plano de tierra equipotencial.

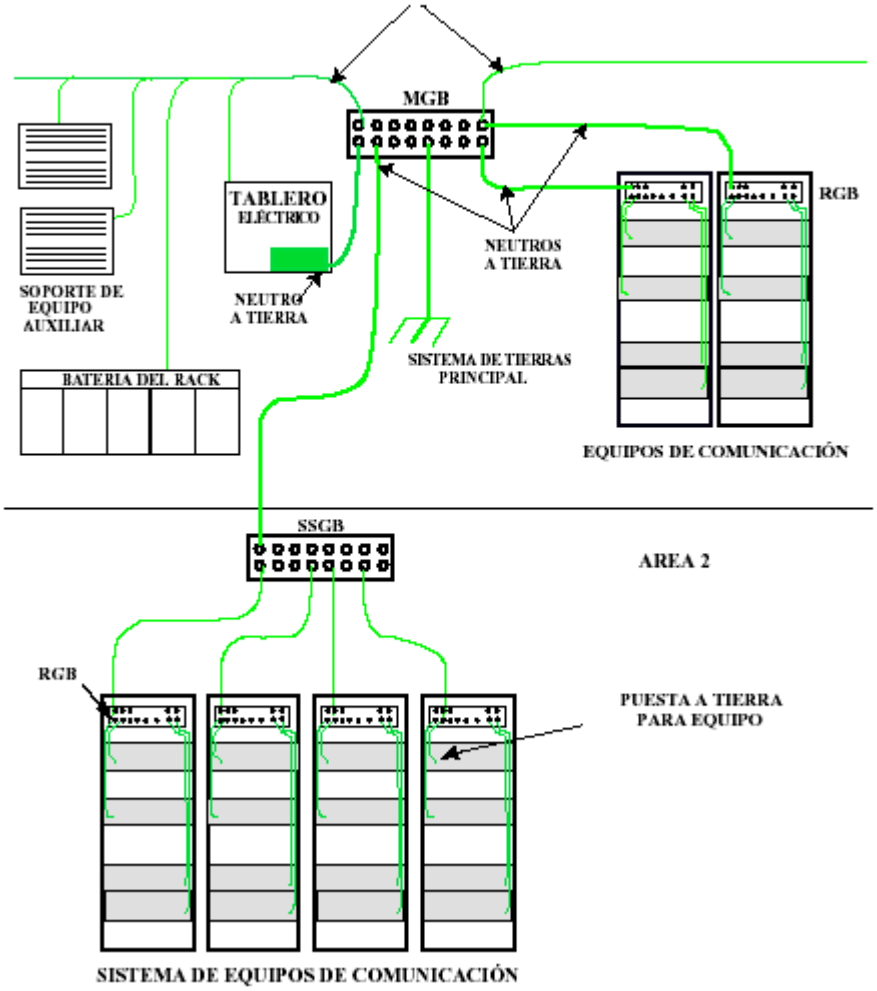
Interconectar todos los Sistemas de Electrodos de Tierra.
Sistema general de Tierra.
Sistemas de Tierra de Pararrayos.
Sistemas de Tierra de Telecomunicaciones.
Cable para Sistemas de Tierra.
Conectar todos los objetos conductivos internos y externos de las instalaciones a Tierra.
Proveer una diferencia de potencial lo más cercana a cero durante transitorios que eleven el potencial.

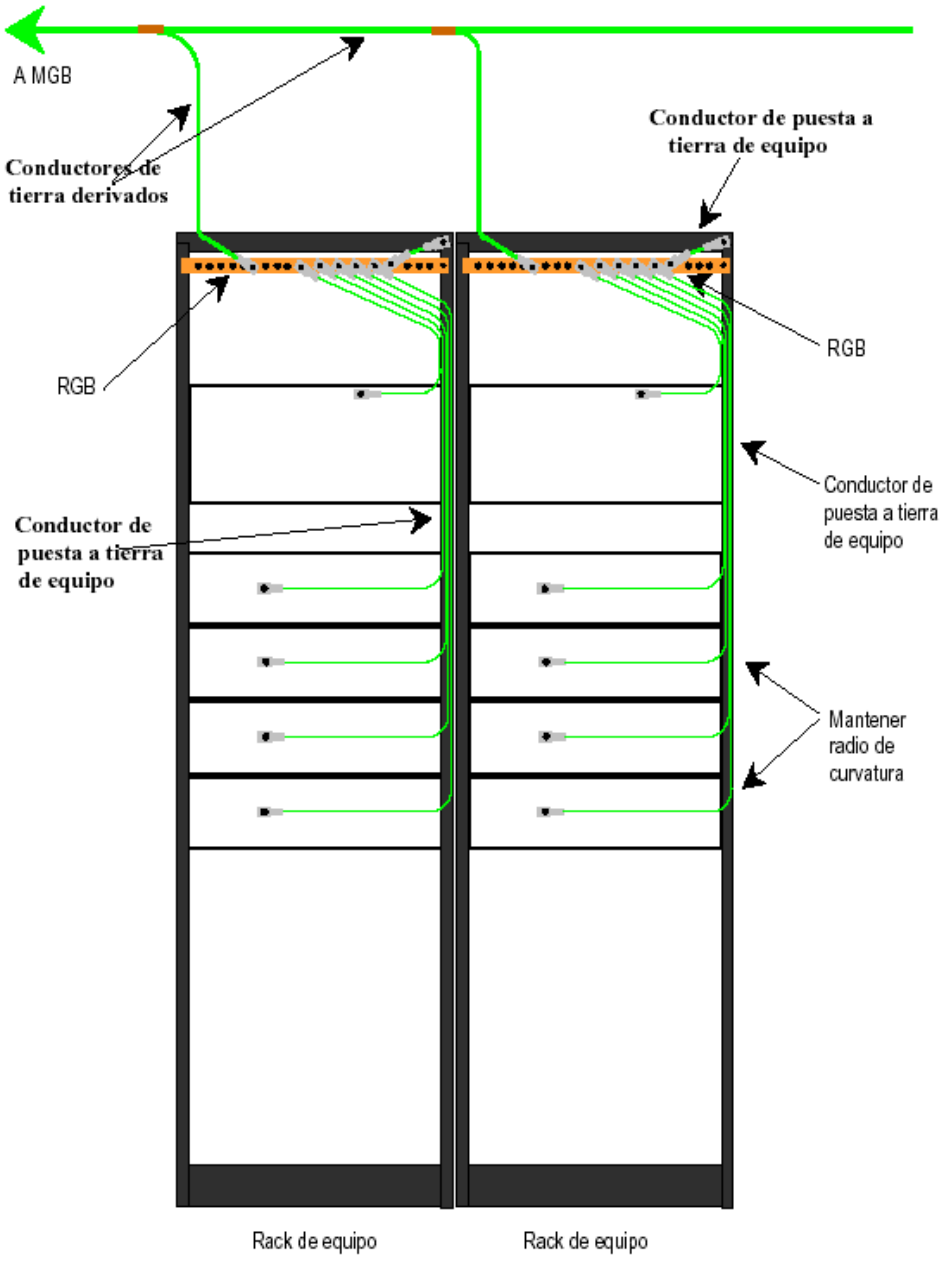

ALIMENTADOR 3F, 1N, 1T (220V)
ALIMENTADOR 3F, 1N, 1T (220V)
ELECTRODO
T A/A
T
DESNUDO
CONMUTADOR
TNES
T
DESNUDO
#6 THW
COLOR
VERDE
#2/0 AWG DESNUDO
RACK TELMEX
RACK ROUTERS
RACK PANEL F.O.
UPS 1
UPS 2
FUENTE TELMEX
4/0 THW
ELECTRODO
ELECTRODO
#2/0 AWG DESNUDO

EQUIPO DENTRO DE EDIFICIO O SHELTER

CABLE INTERNO PERIMETRAL DE TIERRA MONTADO EN LA PARED

AREA 1





NOTA: El rack debe estar totalmente aislado del piso. Y el Sistema de Tierra solo vendrá por arriba.

5. Proteger contra transitorios entrantes por los circuitos de potencia.

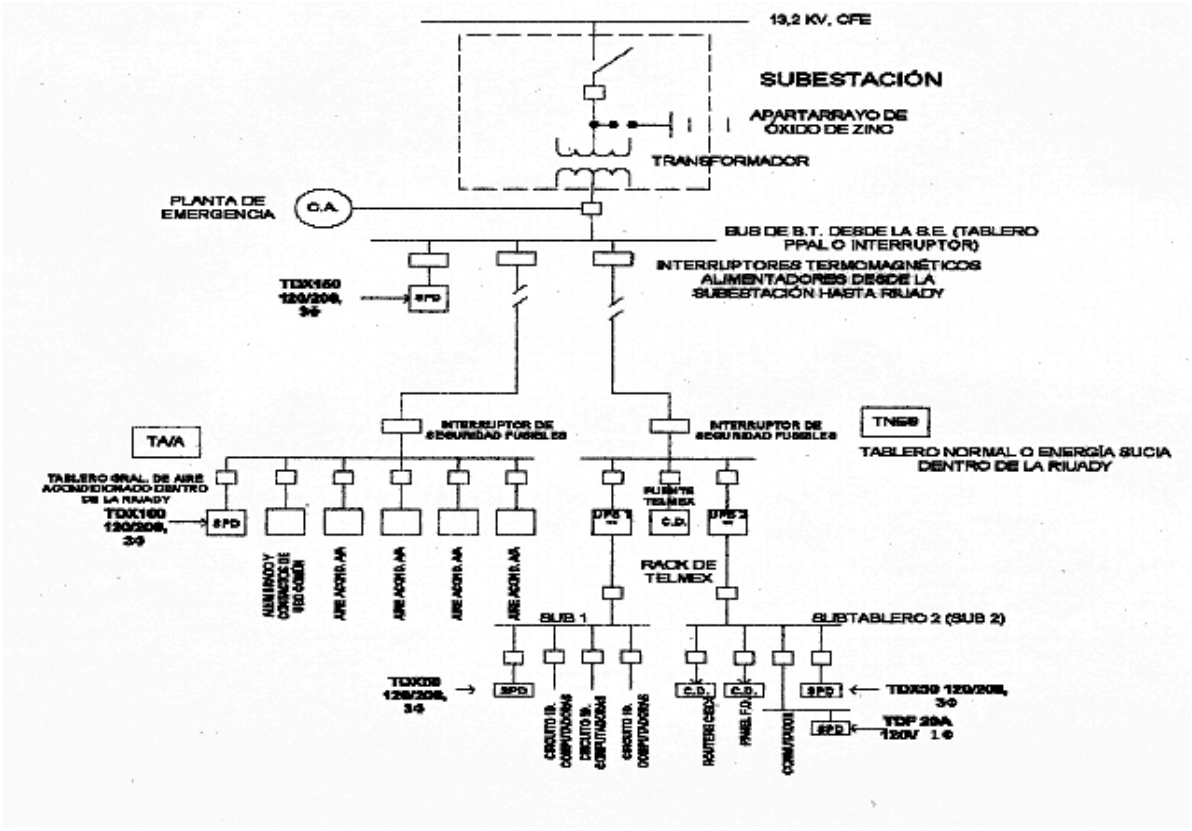
Contar con supresores de picos.

6. Proteger contra transitorios entrantes por los circuitos de comunicación/datos.

REQUISITOS DE TELECOMUNICACIONES

Se recomienda seguir las normas de cableado estructurado, según la norma vigente, que garantizan una mejor administración de los servidores de red, equipos de telecomunicaciones y cableado de los mismos, de acuerdo con los siguientes lineamientos (ver diagrama III):

- •Instalación de un rack de piso de 19" de ancho y 7 pies de alto.
- •Instalación de un kit de protección para la infraestructura metálica: barra de conexión a tierra, aisladores y alfombra de aislamiento.
- •Usar cableado par trenzado categoría 5e+ o 6.
- •Todas las conexiones de red deberán conectarse a un panel de parcheo según sea el medio físico: par trenzado o fibra óptica.



- •Al menos las conexiones de inalámbricos y/o backbones deberán contar con protector de líneas. Se recomienda la instalación de un panel de protección de líneas, el cual deberá estar aterrizado a tierra.
- •Instalar protectores de línea para las conexiones de los enlaces alternos: DS0 e ISDN.