**B. Identificación de las políticas de uso de equipos de cómputo en una organización.**

 Asignación de bienes informáticos.

 Garantías de los bienes informáticos.

 Seguridad Física del site.

 Mantenimiento preventivo y correctivo.

 Instalación Eléctrica.

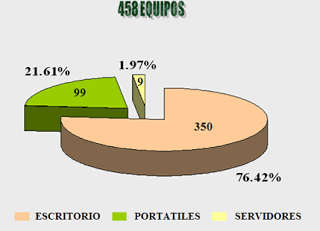
**IDENTIFICACION DE LAS POLITICAS DE USO DE EQUIPOS DE CÓMPUTO EN UNA ORGANIZACION**

**ASIGNACIÓN DE BIENES INFORMÁTICOS DE CÓMPUTO**

**Bienes informáticos**: Son todos aquellos elementos que forman el sistema (ordenador) en cuanto al hardware, ya sea la unidad central de proceso o sus periféricos, así como todos los equipos que tienen una relación directa de uso con respecto a ellos y que, en conjunto, conforman el soporte físico del elemento informático. Asimismo, se consideran bienes informáticos los bienes inmateriales que proporcionan las ordenes, datos, procedimientos e instrucciones, en el tratamiento automático de la información y que, en su conjunto, conforman el soporte lógico del elemento informático.

Cada empresa cuenta con un área o personal encargado que realizará la asignación o movimiento de bienes informáticos de cómputo personal y periféricos, asignándolos a las diferentes áreas de a empresa o exclusivamente al área de computo centro de cómputo o laboratorio de computo.

Existe un documento denominado “Listado de revisión (Check List)” el cual contiene los datos generales del usuario y de los bienes informáticos entregados, así mismo, contendrá los datos de software instalado y configuración del equipo, contando con la firma de conformidad del usuario correspondiente.

[](http://4.bp.blogspot.com/-pEdAttBiVIw/UXv6jROpE4I/AAAAAAAAAAQ/MQ1yTuUK7qE/s1600/GraficaEquipos.gif)

**GARANTÍA DE BIENES INFORMÁTICOS**

[](http://1.bp.blogspot.com/-9i-SFsVtnCY/UXv8Jlfm2CI/AAAAAAAAABA/uGmzDVsVyPE/s1600/images.jpg)

El **equipo de cómputo** cuenta con 1 o 3 años de garantía dependiendo el tipo de bien informático, dicha garantía es a partir de la fecha que se emite la factura de compra por parte del proveedor; esta gestión se realizará a través del Departamento de Informática.

Los **bienes muebles y electrónicos** cuentan con 1 año de garantía a partir de la fecha que se emite la factura de compra por parte del proveedor; esta gestión se realizará a través del área de adquisiciones.

La garantía de los bienes antes citados aplicará únicamente por defectos de fabricante o vicios ocultos.

[](http://4.bp.blogspot.com/-3S7sFeXNkyI/UXv7XxrcqLI/AAAAAAAAAA4/inJh_-9mVOw/s1600/seguridad-informatica-computadoras.png)**SEGURIDAD FISICA DEL SITE**

Es muy importante ser consciente que por más que una empresa sea la más segura desde el punto de vista de ataques externos, Hackers, virus, etc.; la seguridad de esta será nula si no se ha previsto como combatir un incendio.

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa que intenta a acceder físicamente a una sala de operaciones de esta.

Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma.

Así, **la Seguridad Física** consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

**TIPOS DE DESASTRES**

concepto vale, también, para el edificio en el que nos encontramos y/o la empresa. Es por ello que siempre se recomendarán pautas de aplicación general y no procedimientos específicos.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

Las principales amenazas que se prevén en la seguridad física son:

1. Desastres naturales, incendios accidentales tormentas e inundaciones.
2. Amenazas ocasionadas por el hombre.
3. Disturbios, sabotajes internos y externos deliberados.

No hace falta recurrir a películas de espionaje para sacar ideas de cómo obtener la máxima seguridad en un sistema informático, además de que la solución sería extremadamente cara.

A veces basta recurrir al sentido común para darse cuenta de que cerrar una puerta con llave o cortar la electricidad en ciertas áreas siguen siendo técnicas válidas en cualquier entorno.

A continuación, se analizan los peligros más importantes que se corren en un centro de procesamiento; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes **tipos de riesgos.**

* **Incendios**
* **Inundaciones**: Se las define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial.  
  Esta es una de las causas de mayores desastres en centros de cómputos.  
  Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior.  
  Para evitar este inconveniente se pueden tomar las siguientes medidas: construir un techo impermeable para evitar el paso de agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras.
* **Condiciones Climatológicas**
* **La influencia de las señales o rayos de radar** sobre el funcionamiento de una computadora ha sido exhaustivamente estudiada desde hace varios años.  
  Los resultados de las investigaciones más recientes son que las señales muy fuertes de radar pueden inferir en el procesamiento electrónico de la información, pero únicamente si la señal que alcanza el equipo es de 5 Volts/Metro, o mayor. Ello podría ocurrir sólo si la antena respectiva fuera visible desde una ventana del centro de procesamiento respectivo y, en algún momento, estuviera apuntando directamente hacia dicha ventana.
* Instalaciones Eléctricas

**Acciones Hostiles**

1. **Robo**: Las computadoras son posesiones valiosas de las empresas y están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero.

Es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera, robar tiempo de máquina.

La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección que la que otorgan a una máquina de escribir o una calculadora.

El software, es una propiedad muy fácilmente sustraíble y las cintas y discos son fácilmente copiados sin dejar ningún rastro

1. **Fraude**: Cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines.

Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones.

1. **Sabotaje:** El peligro más temido en los centros de procesamiento de datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.

Físicamente, los imanes son las herramientas a las que se recurre, ya que con una ligera pasada la información desaparece, aunque las cintas estén almacenadas en el interior de su funda de protección. Una habitación llena de cintas puede ser destruida en pocos minutos y los centros de procesamiento de datos pueden ser destruidos sin entrar en ellos.

Además, suciedad, partículas de metal o gasolina pueden ser introducidos por los conductos de aire acondicionado. Las líneas de comunicaciones y *eléctricas pueden ser cortadas, etc.*

***[](http://1.bp.blogspot.com/-ZFdEso7aEF8/UXv7T1Y_mHI/AAAAAAAAAAw/YlKRBnVbEV8/s1600/seguridad.jpg)*CONTROL DE ACCESOS**

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución:

1. **Utilización de Guardias**
2. **Utilización de Detectores de Metales:** El detector de metales es un elemento sumamente práctico para la revisión de personas, ofreciendo grandes ventajas sobre el sistema de palpación manual.

La sensibilidad del detector es regulable, permitiendo de esta manera establecer un volumen metálico mínimo, a partir del cual se activará la alarma.  
La utilización de este tipo de detectores debe hacerse conocer a todo el personal. De este modo, actuará como elemento disuasivo. Utilización de Sistemas Biométricos

1. **Verificación Automática de Firmas (VAF)**: En este caso lo que se considera es lo que el usuario es capaz de hacer, aunque también podría encuadrarse dentro de las verificaciones biométricas.

Mientras es posible para un falsificador producir una buena copia visual o facsímil, es extremadamente difícil reproducir las dinámicas de una persona: por ejemplo, la firma genuina con exactitud.

La VAF, usando emisiones acústicas toma datos del proceso dinámico de firmar o de escribir.

La secuencia sonora de emisión acústica generada por el proceso de escribir constituye un patrón que es único en cada individuo. El patrón contiene información extensa sobre la manera en que la escritura es ejecutada.  
El equipamiento de colección de firmas es inherentemente de bajo costo y robusto.  
Esencialmente, consta de un bloque de metal (o algún otro material con propiedades acústicas similares) y una computadora barata.

1. **Seguridad con Animales:** Sirven para grandes extensiones de terreno, y además tienen órganos sensitivos mucho más sensibles que los de cualquier dispositivo y, generalmente, el costo de cuidado y mantenimiento se disminuye considerablemente utilizando este tipo de sistema.

Este sistema posee la desventaja de que los animales pueden ser engañados para lograr el acceso deseado.

1. Protección Electrónica

#### **INSTALACIÓN ELÉCTRICA Y SUMINISTRO DE ENERGÍA.**

#### Imagen1

#### **SUMINISTRO DE ENERGÍA**

Todas las computadoras  dependen vitalmente del suministro de energía eléctrica. Si este suministro falla, el sistema queda totalmente fuera de juego inmediatamente y durante el tiempo que el fallo dure, pudiendo también verse afectados los sistemas de aire acondicionado y de protección de incendios.

#### **AIRE ACONDICIONADO**

Se debe proveer un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de computadoras y equipos de proceso de datos en forma exclusiva.

#### [Imagen4](https://aplicaciondelanormatividadinformatica6104.files.wordpress.com/2015/06/imagen4.jpg)**TEMPERATURA Y HUMEDAD**

La temperatura no debe sobrepasar los 18 °C y el límite de humedad no debe superar el 65% para evitar el deterioro.

**MANTENIMIENTO CORRECTIVO Y PREVENTIVO**

**[](http://2.bp.blogspot.com/-D9MHsooIX6w/UXv96Y1YcBI/AAAAAAAAABU/sNwrpenpy6Y/s1600/problemas-pc-2.jpg)**

**MANTENIMIENTO PREVENTIVO:**

El mantenimiento preventivo permite detectar fallos repetitivos, disminuir los puntos muertos por paradas, aumentar la vida útil de equipos, disminuir costos de reparaciones, detectar puntos débiles en la instalación entre una larga lista de ventajas. 

Relativo a la informática, el mantenimiento preventivo consiste en la revisión periódica de ciertos aspectos, tanto de hardware como de software en un pc. Estos influyen en el desempeño fiable del sistema, en la integridad de los datos almacenados y en un intercambio de información correcta, a la máxima velocidad posible dentro de la configuración optima del sistema.

Dentro del mantenimiento preventivo existe software que permite al usuario vigilar constantemente el estado de su equipo, así como también realizar pequeños ajustes de una manera fácil.

El mantenimiento preventivo en general se ocupa en la determinación de condiciones operativas, de durabilidad y de confiabilidad de un equipo en mención este tipo de mantenimiento nos ayuda en reducir los tiempos que pueden generarse por mantenimiento correctivo.

En lo referente al mantenimiento preventivo de un producto software, se diferencia del resto de tipos de mantenimiento (especialmente del mantenimiento perfectivo) en que, mientras que el resto (correctivo, evolutivo, perfectivo, adaptativo...) se produce generalmente tras una petición de cambio por parte del cliente o del usuario final, el preventivo se produce tras un estudio de posibilidades de mejora en los diferentes módulos del sistema.

Aunque el mantenimiento preventivo es considerado valioso para las organizaciones, existen una serie de fallas en la maquinaria o errores humanos a la hora de realizar estos procesos de mantenimiento. El mantenimiento preventivo planificado y la sustitución planificada son dos de las tres políticas disponibles para los ingenieros de mantenimiento.

Algunos de los métodos más habituales para determinar que procesos de mantenimiento preventivo deben llevarse a cabo son las recomendaciones de los fabricantes, la legislación vigente, las recomendaciones de expertos y las acciones llevadas a cabo sobre activos similares.

El primer objetivo del mantenimiento es evitar las consecuencias de los fallos del equipo, logrando prevenir las incidencias antes de que estas ocurran. Las tareas de mantenimiento preventivo incluyen acciones como cambio de piezas desgastadas, cambios de aceites y lubricantes, etc. El mantenimiento preventivo debe evitar los fallos en el equipo antes de que estos ocurran. 

Es importante limpiar el equipo ya que la mezcla del polvo con el ambiente húmedo en caso extremos ocasiona que este sea un magnifico conductor eléctrico provocando pequeños fallos en los componentes electrónicos de una computadora, además el polvo reduce la eficiencia de los ventiladores de enfriamiento provocando que disminuya su rendimiento.

Para evitar esto hay que darle un Mantenimiento preventivo, el cual consiste en una limpieza total de todos los componentes del equipo, por ejemplo: CPU, ratón, teclado, etc.; así como mantenerlo libre de agentes contaminantes tales como líquido, polvo, etc. el cual se realiza de una manera periódica. 

**Características del área de trabajo para el mantenimiento preventivo.**

Mesa: De superficie lisa, sin perforaciones y amplia para evitar que se extravíen o caigan piezas pequeñas.

Iluminación: Buena y suficiente para poder tener una buena visibilidad.   
Energía eléctrica: Se debe contar con conexiones eléctricas a la mano por si hay que utilizar algún dispositivo de limpieza eléctrico.

Consta de la revisión de tu computadora, haciendo un análisis minucioso de las necesidades de tu computadora tanto de la parte física (hardware), como de la parte lógica (software).

Necesidad de aumento de memoria, tarjetas de video, de sonido, modem, red, puertos firewire, usb y más.

Actualización del software, dependiendo del sistema operativo que requieras, actualización de antivirus, antispam, firewalls, así como programas a la medida en el caso de que quieras mejorar tu equipo.

***[](http://4.bp.blogspot.com/-jiCB8gQJEPE/UXv9t1pNPCI/AAAAAAAAABM/9Vo--FGPaI0/s1600/1359564940_220212349_1-Fotos-de--Mantenimiento-preventivo-y-correctivo.jpg)*MANTENIMIENTO CORRECTIVO:**

Incluye todo el soporte asignado para el mantenimiento preventivo más la reparación o instalación de hardware nuevo.

Incluye también el respaldo de datos en disco compacto o en DVD o cualquier otro medio de almacenamiento amplio.

El mantenimiento correctivo se lo realiza cuando es necesario corregir o reparar algún problema que se esté suscitando en nuestra PC el cual puede corresponder a hardware o software respectivamente.

Cuando necesitemos reemplazar un mouse, teclado, fuente de poder, parlantes, tarjeta de memoria o expansión o en el último de los casos se deba realizar una pequeña soldadura estamos hablando de mantenimiento correctivo de hardware.

**En el mantenimiento de hardware podemos encontrar lo siguiente:**

1.- Cambio de Memoria RAM, muchas de las veces es por aumentar la capacidad de las mismas o en raras ocasiones porque se han quemado.

2.- Instalación de tarjetas de expansión, esto es común puesto que muchas de las veces se desean ampliar o mejorar las funciones de un computador y para esto existen las tarjetas de expansión que pueden ser de video, sonido, red, etc. Puede ser considerado mantenimiento correctivo porque es necesario insertar la respectiva tarjeta directamente en la placa base y si no se tiene cuidado esta puede quedar averiada.

3.- Cuando un dispositivo de E/S se encuentre averiado lo más recomendable es reemplazarlo por uno nuevo, pero si el daño no es mayor se podría proceder a la respectiva reparación de este.

En cambio, cuando nos encontremos con errores de Windows o algunos programas que han dejado de funcionar o no funcionan correctamente estamos hablando de mantenimiento correctivo correspondiente a software.

**En el mantenimiento de software podemos encontrar lo siguiente:**

1.- Posible Formateo del disco duro, cuando no exista ninguna otra solución se recomienda previamente respaldar la información del disco duro que va a ser formateado.

2.- Posible Problema con virus, se deberá desinfectar con un antivirus que tenga las bases de datos actualizadas (Para evitar esto se debe actualizar constantemente el antivirus en el mantenimiento preventivo)

3.- Restauración del sistema, esto se puede llegar a suscitar debido a que existen ciertos programas que al ser instalados pueden generar conflictos con otros programas debido en mucha de las ocasiones a la sustitución de ciertas librerías que son requeridas para su normal funcionamiento.

**C. DESCRIPCIÓN DE LA NORMATIVIDAD Y POLÍTICAS DE USO DE LAS REDES LAN EN UNA ORGANIZACIÓN.**

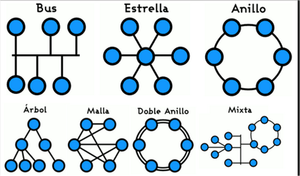
• Sistema de cableado estructurado.

• Manejo de equipos de comunicación.

• Uso de servicio ininterrumpido de corriente.

• Memoria técnica de la red local de voz y datos.

**SISTEMA DE CABLEADO ESTRUCTURADO**

[](https://aplicaciondelanormatividadinformatica6104.files.wordpress.com/2015/06/imagen210.png)Es la infraestructura de cable destinada a transportar, a lo largo y ancho de un edificio, las señales que emite un emisor de algún tipo de señal hasta el correspondiente receptor. Un sistema de cableado estructurado es físicamente una red de cable única y completa, con combinaciones de alambre de cobre (pares trenzados sin blindar UTP), cables de fibra óptica, bloques de conexión, cables terminados en diferentes tipos de conectores y adaptadores.

**Topologías**: Es la representación geométrica de la relación entre todos los enlaces y los dispositivos que los enlazan entre sí (habitualmente denominados nodos).

#### [Imagen3](https://aplicaciondelanormatividadinformatica6104.files.wordpress.com/2015/06/imagen32.png)**TIPOS DE REDES DE ACUERDO A SU EXTENSIÓN**

#### **Red LAN**: Es un grupo de equipos que pertenecen a la misma organización y están conectados dentro de un área geográfica pequeña a través de una red, generalmente con la misma tecnología (la más utilizada es Ethernet).

#### [Imagen4](https://aplicaciondelanormatividadinformatica6104.files.wordpress.com/2015/06/imagen41.png)**Red MAN (Red de Área Metropolitana**: Conecta diversas LAN cercanas geográficamente (en un área de alrededor de cincuenta kilómetros) entre sí a alta velocidad. Por lo tanto, una MAN permite que dos nodos remotos se comuniquen como si fueran parte de la misma red de área local.

#### [Imagen5](https://aplicaciondelanormatividadinformatica6104.files.wordpress.com/2015/06/imagen51.jpg)**Red WAN (Red de área extensa):**

Conecta entre sí varias LAN atravesando importantes distancias geográficas, del orden del tamaño de un país o de un continente.

#### **Red PAN(Red de Área Personal):** Una PAN se suele utilizar para conectar dispositivos personales, como teléfonos celulares, auriculares y asistentes digitales personales entre sí, a otros dispositivos autónomos y redes más grandes, sin necesidad de cables.

[](https://aplicaciondelanormatividadinformatica6104.files.wordpress.com/2015/06/imagen6.jpg)

**MANEJO DE EQUIPOS DE COMUNICACIÓN.**

Una telecomunicación es toda transmisión y recepción de señales de cualquier naturaleza típicamente electromagnética quetengan signos, sonidos, imágenes o, en definitiva, cualquier tipo de información que se desee comunicar a cierta distancia.

[](https://aplicaciondelanormatividadinformatica6104.files.wordpress.com/2015/06/imagen1.png) [](https://aplicaciondelanormatividadinformatica6104.files.wordpress.com/2015/06/imagen2.png) [](https://aplicaciondelanormatividadinformatica6104.files.wordpress.com/2015/06/imagen4.png)[Imagen3](https://aplicaciondelanormatividadinformatica6104.files.wordpress.com/2015/06/imagen3.png)[](https://aplicaciondelanormatividadinformatica6104.files.wordpress.com/2015/06/imagen5.png)

[](https://aplicaciondelanormatividadinformatica6104.files.wordpress.com/2015/06/imagen6.png)**RED**

Es un conjunto de equipos y dispositivos periféricos conectados entre sí. Se debe tener en cuenta que la red más pequeña posible está conformada por dos equipos conectados.

**USO DE SERVICIO ININTERRUMPIDO DE CORRIENTE.**

La Protección contra sobretensión y regulación de voltaje que se vale de un dispositivo que nos ayuda a almacenar energía eléctrica de un tiempo limitado y también todos los elementos disponibles durante un apagón estarán funcionando.

**NO BREAK:** Dispositivo que se conecta al enchufe de pared, integra una circuitería especial que permite alimentar un juego de baterías recargables internas mientras suministra energía eléctrica a la computadora.

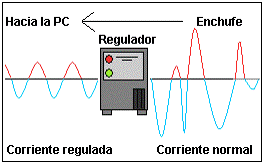


**NOTA:** Se utilizan para que, al ocurrir un apagón, proporciona de inmediato la energía que permite operar la computadora durante el tiempo suficiente para salvar archivos, cerrar programas y apagar el equipo de manera apropiada.

#### [Imagen24](https://aplicaciondelanormatividadinformatica6104.files.wordpress.com/2015/06/imagen24.jpg)

#### **REGULADOR DE VOLTAJE**

Es un dispositivo que tiene varios enchufes, se encarga de mantener el voltaje estabilizado y libre de variaciones.

[](https://aplicaciondelanormatividadinformatica6104.files.wordpress.com/2015/06/imagen25.gif)

#### **SUPRESOR DE PICOS**

Es un dispositivo  que se encarga de suministrar y repartir la corriente a diversos dispositivos conectados a él y que al detectar un voltaje crítico lo canaliza a tierra.

Los supresores protegen sólo contra breves pulsos de alto voltaje

[](https://aplicaciondelanormatividadinformatica6104.files.wordpress.com/2015/06/imagen28.png) 

**MEMORIA TÉCNICA LA RED LOCAL DE VOZ Y DATOS**

La memoria técnica de una red da a conocer toda la información de importancia sobre un centro de cómputo, oficina, etc. Muestra la distribución del cableado en el edificio, así señalando el tipo de conexión.

Se utilizan planos que representen:

La ubicación del techo falso, el teflón y el piso falso,

las lámparas.

el plano de cable, rj45 con medidas.

el de las paredes, ventanas y puerta.

Se realizan tablas de cotización, indicando el precio, la cantidad y el costo total del material, que puede ser desde un RJ45 hasta un switch o una computadora.