

**INSTITUTO TECNOLÓGICO**

**DE OAXACA.**

**Alumno:**

Cruz Gallardo Abraham

Garcia Garcia Sergio Javier

Ramírez Cosmes Laura

Crespo López David Salvador

Jiménez Jiménez Javier

**Grupo:** IS-B **Hora:** 13:00-14:00 hrs

**Catedrático:**

Blanhir Ramírez Mario Alberto



**Materia:**

**REDES**

**Trabajo:**

**Proyecto: Centro de negocios**

# Introducción

La tecnología a ido incrementando de una manera increíblemente rápida, de tal manera que ahora es casi imposible imaginar a una persona que no haya tenido un contacto con ella, esto a influenciado mucho a la sociedad, de tal manera que impacta de forma significativa en el ámbito de la economía, la cultura e incluso el estilo de vida de cada persona que cuenta con algún dispositivo tecnológico.

El uso de las diferentes tecnologías ha llevado a la sociedad a buscar las maneras más optimas de compartir información, como son archivos, documentos, audio, video, e incluso tener una conversación normal con una persona que se encuentra a distancia, simplificando así la comunicación, es ahí donde entra el tema de las redes, ya que es gracias a ésto que todo lo anterior dicho sea posible, teniendo como beneficio la posibilidad de acceder por parte de varios usuarios a una misma información. El uso de la redes también ha tenido un gran impacto en la sociedad y este impacto se ve reflejado fuertemente en las empresas, ya que gracias a la implementación de alguna red, han mejorado sus procesos dentro de la propia empresa de una manera eficiente y eficaz.

En el siguiente documento se presenta un diseño de la instalación de la red de un área de negocios para una empresa que se dedica a la consultaría integral. La empresa desea instalarse en la Huajuapan de León y tener sucursales en Salina Cruz, en Pinotepa Nacional y la Ciudad de Oaxaca de Juárez. Se dará conocer la manera que se pretende construir su área de trabajo desde el punto de vista de redes de computadora, describiendo puntos importantes tales como tipo de sistema, la seguridad, el personal, hardware, etc.

# Sistema distribuido

Debemos tener en cuenta que es un sistema distribuido, y cual será su aplicación con este proyecto.

Definición:

"Sistemas cuyos componentes [hardware](https://www.monografias.com/Computacion/Hardware/) y [software](https://www.monografias.com/Computacion/Software/), que están en ordenadores conectados en [red](https://www.monografias.com/Computacion/Redes/), se comunican y coordinan sus [acciones](https://www.monografias.com/trabajos4/acciones/acciones.shtml) mediante el paso de mensajes, para el logro de un objetivo. Se establece la [comunicación](https://www.monografias.com/trabajos12/fundteo/fundteo.shtml) mediante un [protocolo](https://www.monografias.com/trabajos12/mncerem/mncerem.shtml) prefijado por un esquema [cliente](https://www.monografias.com/trabajos11/sercli/sercli.shtml)-[servidor](https://www.monografias.com/trabajos12/rete/rete.shtml)".

Los sistemas distribuidos presentas características tales como:

Concurrencia. Que permite que los [recursos](https://www.monografias.com/trabajos4/refrec/refrec.shtml) disponibles en la red puedan ser utilizados simultáneamente por los usuarios y/o agentes que interactúan en la red.

Carencia de reloj global. Las coordinaciones para la transferencia de mensajes entre los diferentes componentes para la realización de una tarea, no tienen una temporalización general, esta más bien distribuida a los componentes.

Fallos independientes de los componentes. Cada componente del [sistema](https://www.monografias.com/trabajos11/teosis/teosis.shtml) puede fallar independientemente, con lo cual los demás pueden continuar ejecutando sus acciones. Esto permite el logro de las tareas con mayor efectividad, pues el sistema en su conjunto continua trabajando.

Existen distintos tipos de modelos dentro de los ordenadores interconectados, como es el procesamiento central o Host, donde todo el procesamiento de la [organización](https://www.monografias.com/trabajos6/napro/napro.shtml) se llevaría a cabo en una sola [computadora](https://www.monografias.com/trabajos15/computadoras/computadoras.shtml), normalmente un Mainframe, y los usuarios empleaban sencillos ordenadores personales. Pero este modelo presenta un gran inconveniente, cuando la carga de procesamiento aumenta se tiene que cambiar el hardware del Mainframe, lo cual es más costoso que añadir más computadores personales [clientes](https://www.monografias.com/trabajos11/sercli/sercli.shtml) o [servidores](https://www.monografias.com/trabajos12/rete/rete.shtml) que aumenten las capacidades.

Otro modelo es el Grupo de servidores. Al igual que el anterior es un tanto centralizado, son un [grupo](https://www.monografias.com/trabajos14/dinamica-grupos/dinamica-grupos.shtml) de ordenadores actuando como servidores, normalmente de [archivos](https://www.monografias.com/trabajos7/arch/arch.shtml) o de impresión, poco inteligentes para un número de Minicomputadores que hacen el procesamiento conectados a [una red](https://www.monografias.com/Computacion/Redes/) de área local. Pero con este modelo podría generarse una saturación de los medios de comunicación entre los servidores poco inteligentes y los minicomputadores, por ejemplo cuando se solicitan archivos grades por varios clientes a la vez, podían disminuir en gran medida la velocidad de transmisión de [información](https://www.monografias.com/trabajos7/sisinf/sisinf.shtml).

El modelo que se usara en nuestro proyecto es el Cliente Servidor ya que predomina en la actualidad, y permite descentralizar el procesamiento y recursos, sobre todo, de cada uno de los [servicios](https://www.monografias.com/trabajos14/verific-servicios/verific-servicios.shtml) y de la visualización de la Interfaz Gráfica de Usuario. Esto hace que ciertos servidores estén dedicados solo a una aplicación determinada y por lo tanto ejecutarla en forma eficiente.

Nuestro cliente servidor podrá hacer las sig. funciones:

• Manejo de la interfaz de usuario.

• Captura y validación de los datos de entrada.

• Generación de consultas e informes sobre las [bases de datos](https://www.ecured.cu/Bases_de_datos" \o "Bases de datos).

• Por su parte los servidores realizan, entre otras, las siguientes funciones:

• Gestión de periféricos compartidos.

• Control de accesos concurrentes a bases de datos compartidas.

• Enlaces de comunicaciones con otras redes de área local o extensa.

¿Por qué elegimos el cliente servidor?

Muchos clientes ven interesante al esquema Cliente-Servidor por razones que están más allá de los méritos técnicos. Esto es ciertamente válido, pero teniendo cuidado con las trampas en las que pueda caer si la solución Cliente-Servidor no fue realizada por una razón técnica primaria. Hay tres razones primordiales a considerar en Cliente-Servidor:

• Tamaño de Datos: Visual FoxPro, al igual que todas las variantes de xBase anteriores a él, tenia la limitación de 2 GB en cualquiera de sus tablas o archivos. Esta limitación tiene que ver con la manera en que los bloqueos son realizados en los registros individuales y, mientras que es ciertamente factible que este límite sea alcanzado, esto es diferente a cómo normalmente lo hace [Microsoft](https://www.ecured.cu/Microsoft" \o "Microsoft). A pesar de que hay muchos workarrounds para estos límites, estos incrementan los retos con Visual FoxPro en cuanto las tablas se agranden – tiempos prolongados para reindexar en caso de corrupción, por ejemplo. En resumen, si el tamaño se vuelve un factor mayor, considere si el uso de Cliente-Servidor es adecuado.

•Seguridad: Fundamentalmente, todos los accesos a las tablas FoxPro van a través de la red del [sistema operativo](https://www.ecured.cu/Sistema_operativo" \o "Sistema operativo), así que los usuarios necesitan tener acceso a los directorios conteniendo las tablas VFP. Cualquiera que pueda tener acceso a las tablas puede, eventualmente, imaginarse como leerlos. También es simple usar un driver ODBC y [Excel](https://www.ecured.cu/Microsoft_Excel" \o "Microsoft Excel), o si ellos necesitan usar un editor hexadecimal para romper su esquema de encriptación. Muchos sistemas Cliente-Servidor pueden eliminar esta amenaza en conjunto con la restricción de acceso de los clientes a la interface del [servidor](https://www.ecured.cu/Servidor" \o "Servidor), y no necesariamente a todos los datos. Si esta tratando con material altamente confidencial, Cliente-Servidor tiene sentido por razones de seguridad.

•Bajo Ancho de Banda: Visual FoxPro es el producto para manejo bases de datos escritorio y basado en [LAN](https://www.ecured.cu/LAN" \o "LAN) mas rápido y con mejor mejor desempeño disponible en el mercado hoy en día. Pero VFP obtiene su desempeño fenomenal tomando ventaja del ambiente LAN, pre-obteniendo información de columna, haciendo localmente algún tipo de caching de encabezados de tablas y contenidos de índices. Mientras que el proceso de adquirir esta información es casi imperceptible en un ambiente de red, haciendo lenta la apertura inicial de tablas en milisegundos, esto puede ser un retardo substancial si se está en un “cable delgado” (por ejemplo conexiones Dial-Up, WAN o [Internet](https://www.ecured.cu/Internet" \o "Internet) saturado) entre el cliente y los datos. En estas situaciones, poner los datos, la responsabilidad de hacer las consultas y procesamiento de los datos en el [servidor](https://www.ecured.cu/Servidor" \o "Servidor) minizará los costos de comunicación y mejorará la velocidad.

# Seguridad

La red es una importante área de exposición a riesgos. Por lo general, define el perímetro real de seguridad mismo. En consecuencia, los atacantes suelen dirigirse a la red como punto de partida para acceder a otros activos de TI. La seguridad de red consiste en defender la red y los recursos relacionados frente a las amenazas. La [seguridad de red](https://www.hpe.com/mx/es/networking/network-security.html) emplea contramedidas físicas y de software para proteger la infraestructura de red contra el acceso no autorizado, el uso inadecuado, la modificación y la destrucción.

La seguridad de red resulta esencial para la ciberseguridad general porque la red es una línea de defensa muy importante contra los ataques externos. Puesto que prácticamente todos los datos y aplicaciones están conectados a la red, una seguridad de red sólida ofrece protección contra las infracciones de datos. No obstante, a medida que la red se expande e incorpora capacidades inalámbricas y diversos tipos de dispositivos, la seguridad de red se vuelve más compleja. La seguridad de red necesita mantenerse al día en este tipo de cambios para garantizar la seguridad de la organización.

En nuestro proyecto realizaremos una serie de pasos para aplicar la mayor La seguridad pertinente para que los clientes puedan acceder al sistema vía Internet y a nivel local.

1. Qué debe incluir su política de Seguridad de la empresa.  
  
Responsables del desarrollo, implantación y gestión de la política  
Director de Política de Seguridad. Personal encargado de realizar, supervisar, inspeccionar, modificar las normas y reglas establecidas en la política de seguridad.  
Director de Seguridad. Personal encargado de, en virtud de la política de seguridad establecida, asignar roles de acceso a la información, proveer de permisos y soportes informáticos, controlar la entrada y salida de información, identificación y resolución de incidencias, etc.  
  
Cree una directiva de uso aceptable  
  
Una directiva de uso aceptable es un documento en el que se informa a los empleados de lo que pueden y no pueden hacer en los equipos de la empresa. Ponga por escrito las normas que espera que se cumplan. Puede describir su política sobre la creación de contraseñas, indicar la frecuencia de cambio de contraseñas o mencionar el riesgo que supone abrir archivos adjuntos de correo electrónico de remitentes desconocidos. También puede incluir la prohibición de Instalar software no autorizado en los equipos. En este documento, que debe ser firmado por todos los empleados, tienen que constar las sanciones (en casos extremos, incluso el despido) por contravenir esas normas. En su calidad de propietario o director del negocio, también deberá firmar una copia de la directiva. Si la directiva es larga y detallada, ayude a los empleados a recordar los puntos principales con un resumen de una página que puede distribuir y colocar cerca de sus estaciones de trabajo.  
  
Plan de Actuación en caso de alarma de Seguridad  
  
2. Conciencie a sus empleados  
  
Distribuya proactivamente a través de comunicaciones periódicas las actualizaciones en las políticas.  
  
PASO 2 PROTEJA SUS EQUIPOS DE ESCRITORIO Y PORTATILES  
  
1. Proteger de los virus y el software espía  
  
Los virus, así como los gusanos y los troyanos, son programas maliciosos que se ejecutan en su equipo. Entre las acciones que pueden provocar este tipo de código malicioso se encuentran: borrado o alteración de archivos, consumo de recursos del equipo, acceso no autorizado a archivos, infección de los equipos de los clientes con los que se comunique mediante correo electrónico… El virus se puede extender por los equipos de su empresa y producir momentos de inactividad y pérdidas de datos muy graves. Existen herramientas de eliminación de software malintencionado que comprueban infecciones por software malintencionado específico y ayuda a eliminarlas.  
  
Instalaremos software antivirus. Dispondremos de protección antivirus en todos sus equipos de escritorio y portátiles. El software antivirus examina el contenido de los archivos en las pc en busca de indicios de virus. Cada mes aparecen cientos de virus nuevos, por lo que habrá que actualizar periódicamente los antivirus con las últimas definiciones para que el software pueda detectar los nuevos virus.  
  
Nos aseguraremos que el antivirus esta actualizado.  
  
2. Actualizaciones Software.  
  
A los piratas informáticos les gusta encontrar y aprovechar cualquier error de seguridad en los productos de software más populares. Cuando Microsoft u otra compañía descubren una vulnerabilidad en su software, suelen crear una actualización que se puede descargar de Internet (tanto para el Sistema Operativo como cualquier aplicación que se tenga instalada). Será necesario instalar las actualizaciones tan pronto se pongan a la disposición del público. Windows Update permite recibir actualizaciones periódicamente.  
  
3. Configure un firewall.  
  
Un firewall es un programa encargado de analizar tanto el tráfico entrante como saliente de un equipo, con el fin de bloquear determinados puertos y protocolos que potencialmente podrían ser utilizados por las aplicaciones.  
  
4. Evitaremos el correo electrónico no deseado. (Spam)  
  
El spam son mensajes de correo electrónico comercial no solicitado. Si recibimos un correo electrónico de un remitente desconocido lo eliminaremos sin abrirlo, puede contener virus, y tampoco responderemos al mismo, ya que estaríamos confirmando que la dirección es correcta y esta activa. No realizaremos envío de publicidad a aquellas personas que no hayan autorizado previamente el consentimiento de recibir publicidad. Adoptaremos medidas de protección frente al correo electrónico no deseado. Como filtros de correo electrónico actualizados.  
  
5. Utilizar solamente software legal.  
  
El uso de software ilegal además de generar riesgos de carácter penal, también puede generar problemas en la seguridad de la información, lo que lo que conlleva a pérdidas en la rentabilidad y productividad de la organización. El software legal ofrece garantía y soporte del fabricante.  
  
6. Navegación Segura.  
  
Acceder únicamente a sitios de confianza. Analizar con un antivirus todo lo que descarga antes de ejecutarlo en su equipo. No explorar nunca sitios Web desde un servidor. Utilizar siempre un equipo o portátil cliente. Mantener actualizado el navegador a la última versión.  
Configurar el nivel de seguridad de su navegador según nuestras preferencias. Descargar los programas desde los sitios oficiales para evitar suplantaciones maliciosas (Phishing). Configurar su navegador para evitar pop-ups emergentes. Utilice un usuario sin permisos de Administrador para navegar por Internet, así impedimos la instalación de programas y cambios en los valores del sistema.  
  
Borrar las cookies, los ficheros temporales y el historial cuando utilice equipos ajenos para no dejar rastro de su navegación.  
  
Comercio Electrónico  
  
Observar en la barra de navegación del navegador, que la dirección Web comienza por https: indicar que se trata de una conexión segura y el contenido que transfiera será cifrado por la Red.  
Observaremos que aparece un candado () en la parte inferior derecha de su navegador. Esto significa que la entidad posee un certificado emitido por una autoridad certificadora, el cual garantiza que realmente se ha conectado con la entidad destino y que los datos transmitidos son cifrados.  
  
PASO 3 PROTEJA SU RED  
  
1. Utilizaremos contraseñas seguras.  
  
Informar a los empleados de la importancia de las contraseñas es el primer paso para convertir las contraseñas en una valiosa herramienta de seguridad de la red, ya que dificultan la suplantación de su usuario. Es decir, no se debe dejar en cualquier parte ni se debe compartir. Características de una contraseña "segura":  
Una longitud de ocho caracteres como mínimo; cuanto más larga, mejor. Una combinación de letras mayúsculas y minúsculas, números y símbolos. Se debe cambiar cada 90 días como mínimo y, al cambiarla, debe ser muy distinta de las contraseñas anteriores. No utilice datos personales.  
  
2. Protegeremos una Red WIFI.  
  
Para maximizar seguridad en la red Wifi es necesario usar la siguiente lista de consejos en conjunto.  
  
Ocultar el SSID  
  
Ocultar el SSID (identificador de redes inalámbricas) al exterior es una buena medida para evitar las intrusiones, aun que este dato puede descubrirse fácilmente aunque este se presente oculto.  
  
Cambiar el nombre SSID  
  
Cifrado WEP  
  
Se basa en claves de 64 ó 128 bits. La encriptación WEP no es la opción más segura.  
Encriptación WPA o WPA2 (Wi-Fi Protected Access)  
Surgió como alternativa segura y eficaz al WEP, se basa en el cifrado de la información mediante claves dinámicas, que se calculan a partir de una contraseña.  
Cambiar clave de acceso del punto de acceso  
Es necesario modificar las claves de acceso periódicamente.  
  
3. Configure un firewall a nivel de Red.  
  
Un firewall es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Un firewall puede ser un dispositivo software o hardware  
  
PASO 4 PROTEGEREMOS NUESTROS SERVIDORES  
  
En el momento en que los servidores están en peligro, también lo está toda la red.  
  
1. Certificados de servidor.  
  
Identifican a los sitios Web. Requiere de la existencia de una autoridad certificadora (CA) que afirme, mediante los correspondientes certificados de servidor, que éstos son quienes dicen ser antes del establecimiento del canal seguro. Le permitirá establecer comunicaciones seguras con sus clientes, cifrando la conexión usando la tecnología SSL para que no pueda ser leída por terceros.  
  
2. Mantenga sus servidores en un lugar seguro.  
  
Las empresas deben asegurarse de que sus servidores no son vulnerables a las catástrofes físicas. Coloque estos equipos en una sala segura y con buena ventilación. Haga una relación de los empleados que tienen las llaves de la sala de servidores.  
  
3. Práctica de menos privilegios.  
  
Asigne distintos niveles de permisos a los usuarios. En vez de conceder a todos los usuarios el acceso "Administrador, debe utilizar los servidores para administrar los equipos cliente. Los servidores de Windows se pueden configurar para conceder a cada usuario acceso únicamente a programas específicos y para definir los privilegios de usuario que se permiten en el servidor. De este modo se garantiza que los usuarios no pueden efectuar cambios que son fundamentales en el funcionamiento del servidor o equipo cliente.  
  
4. Conocer las opciones de seguridad.  
  
Los servidores actuales son más seguros que nunca, pero las sólidas configuraciones de seguridad que se encuentran en los productos de servidor de Windows sólo son eficaces si se utilizan del modo adecuado y se supervisan estrechamente.  
  
PASO 5 MANTENDREMOS SUS DATOS A SALVO  
  
La combinación de estas tres prácticas debe proporcionar el nivel de protección que necesita la mayoría de las empresas para mantener sus datos a salvo.  
  
1. Copias de seguridad de los datos importantes para el negocio.  
  
La realización de copias de seguridad de los datos significa crear una copia de ellos en otro medio. Por ejemplo, puede grabar todos los archivos importantes en un CD-ROM o en otro disco duro. Es recomendable probar las copias de seguridad con frecuencia mediante la restauración real de los datos en una ubicación de prueba.  
  
2. Establecer permisos.  
  
Se pueden asignar distintos niveles de permisos a los usuarios según su función y responsabilidades en la organización. En vez de conceder a todos los usuarios el acceso "Administrador" (instituya una política de "práctica de menos privilegios”).  
  
3. Cifre los datos confidenciales.  
  
Cifrar los datos significa convertirlos en un formato que los oculta. El cifrado se utiliza para garantizar la confidencialidad y la integridad de los datos cuando se almacenan o se transmiten por una red. Utilice el Sistema de archivos cifrados (EFS) para cifrar carpetas y archivos confidenciales.  
  
4. Utilizaremos sistemas de alimentación ininterrumpida (SAI).  
  
Para evitar que los equipos informáticos no se interrumpan bruscamente en caso de corte del suministro eléctrico y para filtrar los “microcortes” y picos de intensidad, que resultan imperceptibles, es recomendable el uso de SAI.  
  
PASO 6 PROTEJER SUS APLICACIONES Y RECURSOS  
  
1. Valorar la instalación del Directorio Activo.  
  
La implementación del directorio activo facilita las tareas tanto de seguridad como de funcionalidad. Ventajas:  
  
La propagación de permisos está centralizada desde el Controlador de Dominio. Posibilidad de escalabilidad según las necesidades particulares de la empresa. La integración con un servicio DNS. Sencillez en la estructuración de ficheros y recursos compartidos. Robustez en la seguridad del sistema. Establecimiento de Políticas.  
  
2. Gestione las Aplicaciones a través del Directorio Activo.  
  
Políticas Permisos Usuario Impresoras Correo Electrónico  
  
3. Preste atención a la base de datos.  
  
Instale los últimos Service Packs de la base de datos. Asegúrese de instalar los Service Packs y las actualizaciones más recientes para mejorar la seguridad. Evalúe la seguridad de su servidor con MBSA (Microsoft Baseline Security Analyzer). Utilice el modo de autenticación de Windows. Aísle el servidor y realice copias de seguridad periódicas del mismo.  
  
4. Cortafuegos de Aplicaciones Web.  
  
Protegiendo de ataques específicamente las comunicaciones en las que intervienen tanto las aplicaciones Web como todos los recursos a ellas asociados.  
  
5. Auditorias Técnicas.  
  
Una auditoría técnica de seguridad puede identificar las vulnerabilidades de una aplicación web.  
  
PASO 7 GESTIÓN DE LAS ACTUALIZACIONES  
  
1. Actualizaciones oportunas.  
  
Las revisiones y las actualizaciones de errores, junto con nuevas versiones de software, se pueden implementar desde el servidor en los equipos y portátiles de los usuarios. Así sabe que se han realizado correctamente de forma oportuna y no tiene que depender de que los usuarios no se olviden.  
  
2. Configuraciones especiales.  
  
Puede impedir que los usuarios instalen programas no autorizados si limita su capacidad para ejecutar programas desde CD-ROM y otras unidades extraíbles o para descargar programas de Internet.  
  
3. Supervisión.  
  
Si se produce un acceso no autorizado en un equipo o si hay un error del sistema de algún tipo en algún equipo, se puede detectar inmediatamente mediante las capacidades de supervisión que están disponibles en un entorno de equipos/portátiles administrado.  
  
PASO 8 PROTEJER SUS DISPOSITIVOS MOVILES  
  
Es muy importante que los trabajadores sean conscientes de la importancia de la seguridad en los aparatos móviles y los peligros que puede llevar consigo un mal uso.  
• Emplear las opciones de bloqueo del dispositivo terminal. No acepte conexiones de dispositivos que no conozca para evitar transferencias de contenidos no deseados. Ignore / borre SMS o MMS de origen desconocido que inducen a descargas o accesos a sitios potencialmente peligrosos. Active mediante PIN el acceso al bluetooth. Bloquee la tarjeta SIM en caso de pérdida para evitar que terceros carguen gastos a su cuenta. Instale un antivirus y manténgalo actualizado para protegerse frente al código malicioso. No descargue software de sitios poco fiables para impedir la entrada por esta vía de códigos potencialmente maliciosos. Configure el dispositivo en modo oculto, para que no pueda ser descubierto por atacantes.  
Desactive los infrarrojos mientras no los vaya a utilizar.  
  
PASO 9 PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL  
  
1. Registrar los ficheros.  
  
Una de las obligaciones básicas establecidas por la LOPD es la inscripción de los Ficheros de datos de carácter personal en la Agencia Española de Protección de Datos, pero para realizar correctamente esta inscripción es necesario realizar previamente la Localización de los Ficheros preexistentes, así como la determinación de los nuevos ficheros a inscribir.  
  
2. Cesión de datos a un tercero.  
  
En muchas ocasiones las empresas contratan y subcontratan a otras empresas la prestación de servicios profesionales especializados, servicios que suponen un acceso a los datos de carácter personal almacenados en nuestros ficheros para que sean tratados, almacenados y/o conocidos por estos profesionales. Aunque debiera proponerse por el Responsable del Fichero, cualquiera de las partes podrá proponer la firma de un contrato de acceso a datos, que deberá formalizarse preferiblemente por escrito, de manera que acredite fehacientemente su celebración y contenido.  
LISTA DE AMENAZAS DE SEGURIDAD ( Más importantes)  
  
- Vulnerabilidades en el Software: Debilidad en el software que podría ser explotada. - Ataques Directos El 70 % del malware procede de ataques directos producidos por empleados de la compañía. o Trabajadores Descontentos o Clientes Insatisfechos o Competidores  
- Malware  
O Virus: Malware cuyo cometido es alterar el funcionamiento normal de un ordenador. o Gusanos: Programa parecido a un virus, cuya principal característica es la capacidad de poder replicarse a si mismos. o Troyanos: Programas que se introducen en el ordenador, para realizar acciones con el objetivo de tomar el control del sistema afectado.  
- Ataques de Denegación de Servicio (DOS ) : Ataque que evita al usuario la utilización de determinados servicios. - Spam: Correo basura o no deseado. - Spyware: Programas espía que recopilan información. - Contenido inapropiado o ilegal - Phishing: Suplantación de identidad de una página Web. - Vishing: es una práctica fraudulenta en donde se hace uso del Protocolo VoIP y la ingeniería social para engañar a personas. - Snifadores de Paquetes: Programas que capturan información en los paquetes que cruzan los nodos de conmutación de las redes. - Acceso a Wifi’s inseguras - Web Sites con código malicioso  
O Instalando Troyanos o Redirección a un site indeseado o Robo passwords o Instalación de keyloggers o Adware/ spyware/ lectura cookies  
- Ataques a las Contraseñas  
O Ataque de Fuerza Bruta o Snifadores de Paquetes o Suplantación de IP: Consiste en la sustitución de una dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar.