Nombre	Redes Seguras: Encriptado, filtrado Mac, contraseñas WPA2
Temática	Seguridad

Descripción y principales características

Si existe una red de ordenadores en la empresa, es imprescindible protegerla. Adicionalmente, a medida de que el uso de Internet se vuelve cada vez más un factor clave en competitividad para las organizaciones, el riesgo de sufrir un problema de seguridad continúa.

Utilizar contraseñas seguras para el acceso a la red (no el típico "1234"), proteger la red Wifi, ocultando por ejemplo el SSID o utilizando cifrado WPA2, o configurar un firewall a nivel de red pueden ser buenas soluciones.

La consecución de una red segura dentro de la empresa se obtiene con medidas preventivas y políticas de seguridad, aplicadas por el "administrador" de la red para monitorizar y evitar el acceso no autorizado, el uso indebido y la modificación de la red y los recursos de ésta, protegiéndose de ataques externos, internos y de accesos remotos desautorizados.

En cualquier caso, medidas principales que se pueden implementar en cualquier organización:

1. **Protección de los recursos de IT internos**. El cortafuegos (firewall), es el elemento que establece un perímetro de seguridad entre la red interna de la empresa y el exterior. Se recomienda instalar un hardware con esta capacidad, mismo que puede estar integrado al router de conexión a internet y la red inalámbrica. Para facilitar la gestión y visibilidad en la red, es recomendable que el firewall sea capaz de reconocer aplicaciones, usuarios y dispositivos que se conectan a través de él.

2. **Proveer navegación segura en Internet**. Cualquier empresa, sin importar su tamaño, está expuesta a diversos tipos de software malicioso (malware), por lo cual debe de contar con medidas de filtrado en web y navegación segura a sus empleados para evitar ser víctima de contagio de virus, gusanos, troyanos o phishing que lleven a la pérdida de información o fraude. Esta función, se logra con un dispositivo anti-malware, puede integrarse al firewall y brinda una capa de seguridad adicional a los antivirus de PCs y servidores comunes.

3. **Mantener sistemas operativos y aplicaciones actualizados**. Es crucial el mantener los diferentes sistemas con los parches y actualizaciones correspondientes. Esto disminuye el riesgo de explotación de debilidades en software que lleven a robo o pérdida de información. Hoy en día diversos sistemas y aplicaciones permiten de ser actualizados de manera automatizada, para ello se debe habilitar esta función cuando sea posible, especialmente en sistemas operativos, navegadores web y aplicaciones críticas para el negocio.

4. **Seguridad en dispositivos móviles**. El uso de contraseñas seguras y de mecanismos seguros de encriptación en redes inalámbricas son otras medidas que deben ser adoptadas en la empresa. También, el proveer acceso a la red interna a través del internet utilizando una red privada virtual VPN es otra funcionalidad integrable a un firewall, que permite al trabajador móvil acceder a recursos de la red interna desde su dispositivo personal o PC en casa manteniendo la confidencialidad de la información.

5. **Cultura de seguridad en el trabajo**. Tal vez este es el punto más importante de la lista, dado que los empleados son los principales actores en salvaguardar la información de la empresa. Una PyME tiene la ventaja de poder adoptar ágilmente una cultura de protección de la información y recursos, elemento que podría resultar completo en empresas de mayor tamaño.

Aspectos a tener en cuenta

Cuando se habla de seguridad en redes, se atienden a los siguientes conceptos:

- **Cifrado**: Cloud Computing, el auge de la movilidad con los dispositivos móviles y las redes inalámbricas, y BYOD (Bring Your Own Device) acrecentan el problema. Estas tendencias, además de ser unas de las principales fuentes de la multiplicación exponencial de los datos, traen una complicación añadida: que esos

datos discurren a través de diferentes tecnologías y redes.

Por ello el cifrado es obligatorio en cualquier tecnología que almacene o por la que transiten datos que deben ser confidenciales. De esta forma si un ciberdelincuente logra interceptarlos en Internet o colarse en las redes corporativas superando los obstáculos de seguridad y hacerse con ellos, no sea capaz de leerlos y por tanto le sean inútiles. Mediante el encriptado de la información se consigue que ésta sólo sea comprensible tanto por el emisor como por el receptor, siendo ilegible para terceros que no poseen los datos necesarios para su interpretación

- **Filtrado MAC ("Media Access Control")**: Cada tarjeta de red posee una dirección MAC única que estableció el fabricante. En cuanto a su forma, una dirección MAC está compuesta por 6 bloques hexadecimales separados por dos puntos, por ejemplo: 00:AB:3F:34:90:CE.
  Mediante esta técnica únicamente autorizamos el acceso a la red a aquellas tarjetas de red que indiquemos en un listado.

- **Contraseñas WPA2**: Una contraseña de este tipo es segura debido al cifrado que lleva y consta de una combinación de letras, números y símbolos. Permiten proteger las redes inalámbricas (WI-FI) mediante contraseñas. Habitualmente, viene una contraseña de este tipo en el router de conexión a internet: conviene cambiarla cuanto antes.
  Anteriormente eran contraseñas de tipo **WEP**. Estas contraseñas no son seguras y cualquier persona puede descifrarlas sin tener siquiera conocimientos de informática.

- **Firewall**: Filtro que controla toda las comunicaciones de una red a otra, en función de los permisos que se fijen

- **Certificados de servidor**: Uno de los componentes más esenciales en cualquier operación o transacción segura en la web es un certificado SSL que es un protocolo de seguridad. Es absolutamente esencial en funciones y páginas web de comercio electrónico, tiendas online, banca online,... También son indispensables en los accesos vía páginas web a redes privadas corporativas o empresariales.

  El protocolo SSL se basa en la utilización de un sistema de cifrado que emplea un algoritmo que sólo conocen la máquina del usuario conectado y el servidor que brinda la conexión. Estas claves permiten la encriptación de los datos para que nadie que no las tenga pueda leer su contenido.

  Es necesario que el sitio web tenga un certificado de seguridad conocido como certificado SSL que son expedidos por una autoridad de certificación (CA). Los CA más reconocidos a nivel mundial son: VeriSign, Thawte, GeoTrust y RapidSSL.

  Si una conexión es segura, el prefijo HTTP de la dirección URL de la página web, cambia a HTTPS (que significa HTTP seguro), lo segundo es que en alguna parte de la ventana del navegador (ello depende de que navegador utilice), se visualiza un icono con forma de candado; el mismo al darle clic abre una ventana con todos los datos del certificado SSL en cuestión, y los datos de la entidad CA que genero este certificado

- **Autenticación** del usuario de la red mediante contraseña

Valor añadido para el negocio

- Permite gestionar con seguridad toda la información confidencial (clientes, ventas, pedidos, proveedores...)
- Aumenta la productividad. Una red segura "filtra" cualquier riesgo que le pueda surgir al empleado y no pierde tiempo con estos problemas
- Genera confianza a sus usuarios y clientes
- Permite agregar nuevos servicios y aplicaciones con seguridad
- Acceso seguro desde cualquier lugar a toda la información de la empresa. Movilidad
- Control interno del uso de aplicaciones informáticas (internet, programas de gestión, correo...)
- Permite asignar diferentes permisos de acceso de usuarios a diferentes niveles de información en la red

- Todos los equipos informáticos y smartphones pueden acceder a la red con seguridad
- Elaboración de un plan de seguridad. Reducción del riesgo de inactividad empresarial por fallo de seguridad
- Disminución del riesgo de sanciones administrativas por incumplimiento legal (LOPD)

Tipo de Inversión	Tiempo de Implantación
MEDIA	MEDIO

Casos de Éxito

Optimiza la seguridad en la comunicación y dispositivos de la red, tanto en la red interna de la propia empresa, como en las comunicaciones exteriores de la empresa a través de redes externas.

Aplicaciones

Nombre	Precio	Ventajas	Inconvenientes	Dificultad
JUNIPER NETWORKS	Pago		Tiene coste	Alta
ZENTYAL	Desde 50€/mes	Firewall y detección de intrusos	Tiene coste	Alta

Juniper Networks	URL: http://www.juniper.net/es/es/
Temática	**Dificultad**
Seguridad	ALTA

Descripción y principales características

Juniper Networks ha desarrollado y producido algunas de las innovaciones pioneras y más radicales del mercado en todos los aspectos de la tecnología de redes. Como empresa dedicada en exclusiva a las redes de alto rendimiento, ofrece una amplia cartera de productos que incorpora enrutamiento, conmutación, seguridad, aceleración de aplicaciones, políticas y control de identidades, y administración.

Las soluciones de seguridad de Juniper se centran principalmente en dos puntos:

- Control de **Acceso**: control de acceso a aplicaciones y redes dinámico, basado en estándares y no vinculado a un proveedor concreto. Incluidos el acceso de usuarios invitados, usuarios móviles, el cumplimiento de normas, las amenazas internas y la subcontratación/deslocalización.
- Gestión de **amenazas**: con un entorno de seguridad fiable y con capacidad de respuesta para redes de alto rendimiento.

Aspectos a tener en cuenta

Según el conocimiento técnico que haya dentro de la compañía, puede ser recomendable el contratar un servicio de soporte ya sea con Juniper o con un partner recomendado ya que se trata de productos muy complejos.

En cualquier caso, es necesario que dentro de la organización haya un perfil que conozca el funcionamiento de esta tecnología para que sirva de soporte en primer instancia y como interlocutor del proveedor si el no supiera solucionar la incidencia en un primer momento.

Casos de Éxito

Descarga	Soporte / Ayuda
http://www.juniper.net/support/downloads/	http://www.juniper.net/customers/support/

Coste

Juniper Networks proporciona un presupuesto a medida para la empresa en función del tamaño de la misma y de sus requerimientos. Para ello hay que contactar con ellos en la ruta http://www.juniper.net/es/es/how-to-buy/. También es posible contactar con un partner autorizado por Juniper y gestionarlo directamente con él.

Principales hitos de implantación

Para implementar una arquitectura de red segura, hay que seguir los siguientes pasos a grandes rasgos:

1- Definir la topología de la red a montar
2- Analizar qué elementos serán necesarios (routes, hubs, switches, firewall,...)
3- Implementar las medidas de seguridad

La implementación de estas soluciones tiene un componente físico que es el que definirá el tiempo que se tardará en tener operativa la solución. En cualquier caso, se estima en 3 o 4 semanas el tiempo necesario.

Zentyal	URL: http://www.zentyal.com/es/
Temática	**Dificultad**
Seguridad	ALTA

Descripción y principales características

Zentyal es un software que conforma una plataforma de red unificada para las PYMEs.

Puede actuar gestionando la infraestructura de red, como puerta de enlace a Internet (Gateway), gestionando las amenazas de seguridad (UTM), como servidor de oficina, como servidor de comunicaciones unificadas o una combinación de estas. Además, Zentyal incluye un framework para desarrollar nuevos servicios basados en Unix.

Zentyal proporciona lo siguiente:

- Arquitectura híbrida con la nube
- Servidor completo de correo, web, FTP, proxy HTTP
- Gestión centralizada de usuarios, grupos y privilegios
- Control de acceso de recursos compartidos
- Firewall

Aspectos a tener en cuenta

Según el conocimiento técnico que haya dentro de la compañía, puede ser recomendable el contratar un servicio de soporte con un partner ya que se trata de productos muy complejos.

En cualquier caso, es necesario que dentro de la organización haya un perfil que conozca el funcionamiento de esta tecnología para que sirva de soporte en primer instancia y como interlocutor del proveedor si el no supiera solucionar la incidencia en un primer momento.

Casos de Éxito

Descarga	Soporte / Ayuda
N/A	http://forum.zentyal.org/

Coste

Hay tres ediciones orientadas para las pymes cuyo precio de licencias oscila entre 50 y 120 euros al mes:

- Professional: hasta 25 usuarios
- Business: hasta 75 usuarios
- Premium: hasta 300 usuarios

Hay que contactar a través de la web o directamente con un partner para que hagan al negocio un presupuesto a medida de implantación en función de las características técnicas requeridas.

No incluye:

- Dispositivos físicos de la infraestructura de red

Principales hitos de implantación

Para implementar una arquitectura de red segura, hay que seguir los siguientes pasos:

1- Obtener el software
2- Configuración de los componentes de red y de seguridad

La implementación de estas soluciones tiene un componente físico que es el que definirá el tiempo que se tardará en tener operativa la solución. En cualquier caso, se estima en 3 o 4 semanas el tiempo necesario.

Nombre	Phishing o suplantación de identidad
Temática	Seguridad

Descripción y principales características

El phishing es una técnica de captación ilícita de datos personales (principalmente relacionados con claves para el acceso a servicios bancarios y financieros) a través de correos electrónicos o páginas web que imitan/copian la imagen o apariencia de una entidad bancaria/financiera (o cualquier otro tipo de empresa de reconocido prestigio).

La técnica del phishing más común utiliza el correo electrónico para ponerse en contacto con los usuarios, utilizando mensajes que imitan, casi a la perfección, el formato, lenguaje y la imagen de las entidades bancarias/financieras, y que siempre incluyen una petición final en la solicita a los usuarios la "confirmación" de determinados datos personales alegando distintos motivos: problemas técnicos, cambio de política de seguridad, posible fraude, etc...

Estos mensajes de correo electrónico siempre incluyen enlaces que conducen "aparentemente" a las páginas web oficiales de las citadas entidades pero que, en realidad, remiten a "páginas web piratas" que imitan o copian casi a la perfección la página web de la entidad financiera, siendo su finalidad principal captar datos de los usuarios.

Dada la confianza que los usuarios tienen depositada en las entidades de las que son clientes, y por desconocimiento o simplemente ante la incertidumbre y temor creados, acceden a dichas páginas web piratas, donde el defraudador o delincuente informático, obtiene los datos personales o claves de acceso personales.

Es a partir de este momento donde empieza el fraude:

1. Utilización del número de tarjeta y fecha de caducidad para compras por Internet (comercio electrónico).
2. Realización de transferencias bancarias no consentidas ni autorizadas.
3. Retirada de efectivo en cajeros con duplicados de las tarjetas.
4. ....

Normalmente ninguna entidad se pone en contacto con sus usuarios para pedirle sus claves de acceso a las aplicaciones. Hay que tener en cuenta esto y no darlas. Y en caso de duda contactar telefónicamente con la entidad que sea para aclararlo.

Aspectos a tener en cuenta

El phishing puede producirse de varias formas, desde un simple mensaje al teléfono móvil, una llamada telefónica, una web que simula una entidad, una ventana emergente, y la más usada y conocida por los internautas, la recepción de un correo electrónico.

Otra advertencia es el uso de **troyanos** para el robo de dichos datos. Un troyano es un código malicioso que se instala en el ordenador, y su objetivo a diferencia de los virus comunes no es hacer que los equipos vayan mal en su trabajo, sino pasar inadvertidos para poder ejercer su función de robo de datos.

Valor añadido para el negocio

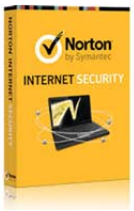
- Mediante la protección contra la suplantación de identidad mantendrá los datos de la empresa seguros
- La mejor protección es no dar información personal o financiera a través de llamada telefónica, email,...

Tipo de Inversión	Tiempo de Implantación
BAJA	CORTO

Casos de Éxito				
Aplicaciones				
Nombre	**Precio**	**Ventajas**	**Inconvenientes**	**Dificultad**
NORTON INTERNET SECURITY 2013	Desde 74,99 €/año			Baja
KASPERSKY SMALL OFFICE SECURITY	Desde 167,20 €/año			Media

Norton Internet Security	URL: http://es.norton.com/
Temática	**Dificultad**
Seguridad	BAJA

Descripción y principales características



El navegar por internet, hacer gestiones online en el banco o realizando compras,... hace necesario el tener programas de seguridad que sirvan de protección contra las amenazas que pueden venir desde internet.

Norton Internet Security proporciona la siguiente funcionalidad:

- Todas las descargas, archivos y aplicaciones se comprueban antes de utilizarse.
- Los mensajes instantáneos y de correo electrónico se escanean siempre.
- Cortafuegos doble que salvaguarda el ordenador de piratas informáticos de forma continua.
- Tecnología contra suplantación de identidad.
- Identifica los sitios web peligrosos en los resultados de la búsqueda directamente en el motor de búsqueda
- Rápido y moderado en cuanto al uso de recursos del sistema

Aspectos a tener en cuenta

No confundir este software con un antivirus. Norton Internet Security se basa en Norton Antivirus, pero incluye características adicionales (firewall, phising,...) que hacen que la navegación por Internet sea más segura.

Casos de Éxito

Descarga	Soporte / Ayuda
http://www.symantec-norton.com/Norton_Internet_Security_p127.aspx?lang=es-ES&par=goo_es_norton_internet_security_2013&par1=es_es_norton_internet_security_promotion&gclid=CIqBuN-1obwCFSn4wgodWSoAcw	https://support.norton.com/sp/es/es/home/current/info?pv=off

Coste

Cada licencia se puede utilizar en 3 ordenadores y además proporciona soporte gratuito 24x7. El precio de cada licencia es de 74,99 euros por año.

No incluye:

- Tiempo de instalación y configuración del software.
- Tiempo de aprendizaje.

Principales hitos de implantación

Para implementar en la organización el Norton Internet Security, hay que hacer lo siguiente:

1- Obtener el software desde la página web del fabricante.
2- Instalarlo y configurarlo en cada ordenador que se desee proteger
3- Registrarse y obtener la licencia para de esta forma activar el producto en cada equipo.

La instalación de estas soluciones son prácticamente inmediata. En cualquier caso, se estima en 1 a 3 días el tiempo necesario en función de los conocimientos técnicos de la persona que acometa la tarea.

Kapersky Small Office Security	URL: http://www.kaspersky.es/
Temática	**Dificultad**
Seguridad	MEDIA

Descripción y principales características

Kaspersky Small Office Security ofrece tecnologías de protección para empresas diseñadas para garantizar facilidad de instalación, configuración y uso.

El programa protege sus equipos de escritorio y servidores de archivos con Windows, así como smartphones y tablets Android; para mantener a buen recaudo las transacciones bancarias online y la información dela empresa.

Tiene las siguientes características principales:

- Protección de los PCs, servidores, teléfonos inteligentes y tabletas Android contra programas maliciosos.
- Protección adicional para garantizar la seguridad de las transacciones financieras y bancarias online
- Modo pago seguro y el teclado virtual para evitar el robo de las contraseñas por parte de malware
- Identifica sitios web de phishing diseñados para engañar y conseguir sus contraseñas y datos personales
- Bloquea descargas y archivos adjuntos sospechosos
- Administración de contraseñas
- Restricción a empleados de funciones de mensajería, sitios web,... durante la jornada laboral

Aspectos a tener en cuenta

En cuanto a seguridad en dispositivos móviles, hay que tener en cuenta que, aparte de las amenazas presentes en cualquier equipo informático, estos dispositivos están expuestos a problemas derivados del robo o pérdida. Esta herramienta cuenta con una funcionalidad que aporta la geolocalización del dispositivo.

Casos de Éxito

Descarga	Soporte / Ayuda
http://www.kaspersky.es/descargar-version-de-prueba#tab=tab-2	http://support.kaspersky.com/sp

Coste

El precio de cada licencia varía en función del número de ordenadores a proteger y del tiempo para la que se obtenga. Así, para proteger 5 equipos, 5 dispositivos móviles y un servidor, el coste sería de 167,20 euros al año. Por ejemplo, si se comprara para dos años, el segundo tendría un descuento de 100 euros.

No incluye:

- Tiempo de instalación y configuración del software.
- Tiempo de aprendizaje.

Principales hitos de implantación

Para implementar en la organización el Kapersky Small Office Security, hay que hacer lo siguiente:

1- Obtener el software desde la página web del fabricante.

2- Instalarlo y configurarlo en cada ordenador que se desee proteger
3- Registrarse y obtener la licencia para de esta forma activar el producto en cada equipo.

La instalación de estas soluciones son prácticamente inmediata. En cualquier caso, se estima en 1 a 3 días el tiempo necesario en función de los conocimientos técnicos de la persona que acometa la tarea.

Nombre	Antivirus, malware y cortafuegos
Temática	Seguridad

Descripción y principales características

Son programas informáticos que ayudan a proteger toda la información presente en aparatos informáticos y en la red de la empresa, ante ataques externos a la empresa

Aspectos a tener en cuenta

- *L*os antivirus son programas cuyo objetivo es detectar y/o eliminar virus informáticos. Los virus informáticos tratan de alterar el buen funcionamiento de las herramientas informáticas, pudiendo causar graves perjuicios al infectado
- El *malware* es un software o programa informático maligno que se infiltra o daña el ordenador y su información, sin el consentimiento previo del usuario
- Los cortafuegos o *firewall* se trata de un dispositivo (*hardware* o *software*) que impide el acceso no autorizado de intrusos a un ordenador o a una red

Valor añadido para el negocio

- Permiten controlar e impedir el acceso a la red de la empresa y a la información que se tenga
- Permiten estar protegidos ante la infección por un virus y tomar las medidas necesarias para tratarlo en caso de infección. Esta infección puede causar leves incidencias (bloquear el ordenador, ralentizarlo,...) y graves incidencias (acceso remoto no autorizado, robo de información, suplantación de identidad...)
- Máxima seguridad para la información que se tenga y en especial, la más sensible (datos personales, bancarios, ventas...)
- Generan confianza en la información que se maneja y los programas instalados
- Generan confianza en los clientes, ya que perciben que sus datos están protegidos
- Evitan posibles sanciones por la pérdida de información confidencial

Tipo de Inversión	Tiempo de Implantación
BAJA	CORTO

Casos de Éxito

Aplicaciones

Nombre	Precio	Ventajas	Inconvenientes	Dificultad
AVAST	Desde 30,09€/mes	Gratis para versión hogar		Baja
BITDEFENDER	Desde 29,97€/año	Posibilidad de *cloud*		Baja
AVG	Desde	Reparación automática		Baja

	78,94€/año			

Avast!	URL: http://www.avast.com/es-ww/index
Temática	**Dificultad**
Seguridad	BAJA

Descripción y principales características

AVAST Software fue creada hace 25 años, período en el que la empresa ha ido evolucionando, al igual que sus soluciones, desde las ofrecidas en sus inicios hasta la innovadora idea de ofrecer avast! Antivirus para hogares de manera gratuita para convertirse en el programa más descargado del mundo, con más de 200 millones de usuarios.

La iniciativa ha sido galardonada con numerosos premios internacionales, tales como estudios de pruebas de software independientes como AV-Comparatives, AV-Test y Virus Bulletin han reconocido la eficacia de avast! Antivirus, así como Softonic ha anunciado que avast! Antivirus es el programa más descargado de Europa.

La versión para pymes de avast! tiene las siguientes características:

- Interfaz de usuario muy sencilla
- Uno de los mejores motores antivirus y antispyware
- Detección de comportamientos no usuales
- Actualización de la base de datos de virus en tiempo real
- Compatible con Windows

Aspectos a tener en cuenta

Es importante definir la periodicidad de actualización del antivirus. Para ello se deberá tener acceso a Internet. De esta manera se consigue que el antivirus esté actualizado con las 'vacunas' para virus de reciente creación.

Casos de Éxito

Descarga	Soporte / Ayuda
http://www.avast.com/es-es/endpoint-protection	http://www.avast.com/es-es/support

Coste

Avast! es un antivirus gratuito para versión de hogar pero con un coste de 39,09€ al año por dispositivo en que se instale para empresas. Se ofrecen descuentos por compras con volumen.

No incluye:

- Tiempo de instalación.
- Tiempo de recursos para formarse en el manejo de la herramienta

Principales hitos de implantación

Es una herramienta de escritorio que hay que instalar individualmente en cada ordenador que se requiera, por ello no

se considera una implantación propiamente dicha con hitos a cumplir. Hay que seguir estos pasos:

- ✓ Bajar la última versión de avast! desde la página oficial.
- ✓ Ejecutar el fichero bajado. Se recomienda hacer la instalación típica.
- ✓ Al terminar la instalación es probable que pida reiniciar el sistema.
- ✓ Hay que registrarse en la web de avast!, que proporcionará un código que hay que introducir en "Acerca de Avast/Código de licencia"

El tiempo de implantación del antivirus es muy reducido. No obstante es necesario invertir cierto tiempo para poder familiarizarse con la herramienta. Este tiempo podrá ser de hasta 2 días en función de la capacitación y el conocimiento técnico de la persona o empresa que las utiliza.

Bitdefender	**URL:** http://www.bitdefender.es/
Temática	**Dificultad**
Seguridad	BAJA

Descripción y principales características

Bitdefender nació en 2001 y ha logrado un amplio conocimiento a nivel mundial, ya que ofrece soluciones antivirus que han sido galardonadas y premiadas en el sector como como El mejor software de seguridad de Internet.

Este antivirus incluye una Administración Centralizada que consolida la funcionalidad antivirus corporativa con Herramientas de Red dirigidas por asistentes que simplifican la gestión de configuración remota masiva y la auditoría en toda la red de equipos y servidores basados en Windows. Entre sus principales características destacan las siguientes:

- Protección antivirus frente a amenazas online reconocida sistemáticamente
- La mejor capacidad de respuesta de la industria frente a nuevas amenazas.
- Detiene el secuestro de la identidad comercial
- Seguridad contra espionaje y correo basura con contenido malicioso
- Mantener segura la información financiera y la del cliente
- Hacer cumplir controles en los puntos finales con políticas de seguridad de usuario ampliadas al sistema
- Simplificar la administración de la red con el asistente virtual y reducir el trabajo manual de generación de informes.
- Automatizar la recopilación de datos de auditoría de red para generar informes de inventario y cambios.
- Garantizar la conformidad con las licencias de software e identificar las aplicaciones no autorizadas.

Aspectos a tener en cuenta

Es importante definir la periodicidad de actualización del antivirus. Para ello se deberá tener acceso a Internet. De esta manera se consigue que el antivirus esté actualizado con las 'vacunas' para virus de reciente creación.

Bitdefender ha hecho hincapié en la sencillez de su instalación y manejo de la herramienta.

Casos de Éxito

Descarga	Soporte / Ayuda
http://www.bitdefender.es/business/#Descarga de evaluación	• Formulario de contacto: http://www.bitdefender.es/site/Buy/inquire/

Coste

La empresa ofrece diferentes opciones para comprar sus licencias:

- *Cloud Security* es la mejor solución de seguridad para pymes con infraestructura y recursos de TI escasos o inexistentes, 119 € para 5 puestos y 2 años de duración.
- *Bitdefender Internet Security* asegura las operaciones de banca y compra online, seguridad online para niños, protección de la privacidad en redes sociales, el precio es de 29,97 € para 3PCs durante 1 año.
- *Bitdefender On-Premise Business Solutions 3.6* es ideal para pymes con servidores en sus instalaciones, el precio es de 399,99 € año para 10 licencias.

No incluye:

- Tiempo de instalación.
- Tiempo de recursos para formarse en el manejo de la herramienta

Principales hitos de implantación

Es una herramienta de escritorio que hay que instalar individualmente en cada ordenador que se requiera, por ello no se considera una implantación propiamente dicha con hitos a cumplir. Se deben seguir estos pasos:

- ✓ Bajar la última versión de Bitdefender desde la página oficial.
- ✓ Ejecutar el fichero bajado. Se recomienda hacer la instalación típica.
- ✓ Al terminar la instalación es probable que pida reiniciar el sistema.
- ✓ Hay que introducir el código de activación suministrado en la compra.

El tiempo de implantación dependerá en gran medida del producto adquirido, si bien como norma general suele ser inferior a 3 horas, ya que sólo requiere el registro en el servicio, iniciar la sesión en la consola desde el navegador e implementar remotamente la protección en todos los sistemas.

AVG	URL: http://free.avg.com/es-es/homepage
Temática	**Dificultad**
Seguridad	BAJA

Descripción y principales características

AVG se fundó en 1991 y desde entonces ha desarrollado su actividad dentro del mercado del software de seguridad.

AVG Internet Security 2014 protege a los usuarios mientras navegan por Internet y se comunican con servicios de mensajería instantánea (IM), y de manera simultánea proporciona seguridad a las redes de área local (si existen) frente a ataques al sistema peligrosos. La principal función de la herramienta es inactivar a los virus, el spam, el spyware y los troyanos, a la vez que hace que el robo de identidad, las vulnerabilidades Web, el phishing oculto y los rootkits sean un recuerdo lejano.

En cuanto a las características implementadas en la nueva versión de antivirus destacar las siguientes:

- Interfaz sencilla
- Compatible con Windows
- Detecta y lo alerta de todo riesgo de seguridad que exista, ofreciendo un sencillo botón de reparación automática que con un clic repara automáticamente el problema y restablece el sistema al mejor modo de protección
- Actualizaciones automáticas
- Soporte telefónico de lunes a viernes
- Protección frente hackers
- Protección de la actividad online

Aspectos a tener en cuenta

Es importante definir la periodicidad de actualización del antivirus. Para ello se deberá tener acceso a Internet. De esta manera se consigue que el antivirus esté actualizado con las 'vacunas' para virus de reciente creación.

Casos de Éxito

Descarga	Soporte / Ayuda
http://www.avg.com/es-es/free-antivirus-download	http://www.avg.com/es-es/customer-support

Coste

La versión para negocios del programa tiene un coste de 78,94€ con las siguientes funcionalidades principales:

- Soporte dado por expertos de AVG
- Consola de administrador
- Antivirus para servidores y estaciones de trabajo
- Firewall contra hackers

Asimismo existe una versión superior por 111,96€ al año que incorpora funcionalidades adicionales de protección de correo electrónico.

No incluye:

- Tiempo de instalación.
- Tiempo de recursos para formarse en el manejo de la herramienta

Principales hitos de implantación

Es una herramienta de escritorio que hay que instalar individualmente en cada ordenador que se requiera, por ello no se considera una implantación propiamente dicha con hitos a cumplir. Se deben seguir estos pasos:

- ✓ Bajar la última versión de AVG desde la página oficial.
- ✓ Ejecutar el fichero bajado. Se recomienda hacer la instalación típica.
- ✓ Al terminar la instalación es probable que pida reiniciar el sistema.
- ✓ Hay que introducir el código de activación suministrado en la compra.

El tiempo de implantación del antivirus es muy reducido. No obstante es necesario invertir cierto tiempo para poder familiarizarse con la herramienta. Este tiempo podrá ser de hasta 2 días en función de la capacitación y el conocimiento técnico de la persona o empresa que las utiliza

Nombre	Back-ups, copias de seguridad
Temática	Seguridad

Descripción y principales características

Las copias de seguridad son algo esencial para mantener salvaguardados los datos de la empresa, de los clientes, proveedores, de las facturas, etc,...

Normalmente puede que no se le preste la atención debida a este tema hasta que se produce alguna pérdida de información debida por ejemplo a que alguien elimina un archivo por error o por corrupción de un disco duro de un ordenador u otro tipo de almacenamiento. Es por ello, que para evitar pérdidas de datos, hay que implementar políticas de seguridad para evitar posibles situaciones desastrosas para la empresa.

1. Realizar **backups o copias de seguridad**: esto se realiza con programas informáticos que realizan una copia de los datos originales (clientes, proveedores, facturación...), a otra ubicación distinta de forma periódica.

   Las copias de seguridad de datos se pretende salvaguardar toda la información disponible y original en soporte informático, así se podrían recuperar (restore o restauración de datos) en caso de pérdida. Estas copias se realizan para recuperar información o sistemas informáticos ante catástrofes informáticas, naturales, ataque, etc;

2. Elaborar **planes de contingencia** en caso de que sucediera algo inesperado como por ejemplo si deja de estar operativo algún dispositivo de la compañía. Por ejemplo, si se estropea el router de conexión a internet, contar con una conexión 3G con la cual seguir al menos conectados al email.

Aspectos a tener en cuenta al implementar en la empresa medidas de copias de seguridad:

- **Realizar copias periódicas**. La frecuencia dependerá de la cantidad de información que se vaya generando o de su criticidad: mensual, quincenal, semanal,...
- **Automatizar el proceso**. Lo ideal es que el resguardo de la información se haga de forma automática para evitar despistes, dejadez, etc...
- **Clasificar el contenido**. No toda la información que genera el negocio es relevante, por ello conviene identificar con claridad carpetas y archivos para que luego sea más fácil de encontrar en caso de necesidad y disminuir los costes de almacenamiento de las copias de seguridad.
- **Elegir la mejor ubicación**. Es recomendable tener la copia en una unidad externa situada además en una ubicación física distinta de donde están situados los datos originales.
- **Verificar la copia**. Una vez concluida la operación, comprobar siempre si la copia se realizó correctamente y si contiene la información de referencia (fecha, contenido, etc.).

Aspectos a tener en cuenta

Hay que tener en cuenta que actualmente con la modalidad de **Cloud Computing**, todos los datos por ejemplo de facturación de la empresa pueden estar en la aplicación del proveedor online que suministra el servicio. Estos proveedores aseguran una disponibilidad del 99% pero no obstante, es recomendable copiar los datos en algún dispositivo físico local como medida de precaución. Y viceversa, si siempre se trabaja con servidores y aplicaciones locales, se puede contratar un servicio de almacenamiento online para guardar en él las copias de seguridad.

Valor añadido para el negocio

- Mantener segura toda la información, principalmente la más críticos para la empresa
- Acceso a la información en cualquier lugar y en cualquier momento

Tipo de Inversión	Tiempo de Implantación
BAJA	CORTO

Casos de Éxito

Aplicaciones

Nombre	Precio	Ventajas	Inconvenientes	Dificultad
URANIUM	Desde 80€/año	Tiene versión gratuita		Media
BACK IN TIME	Gratis			Media
FBACKUP 4.8	Gratis			Media

Uranium Backup	**URL:** http://www.uranium-backup.com/es/
Temática	**Dificultad**
Seguridad	MEDIA

Descripción y principales características

Uranium Backup Free es un software fiable que incluye una herramienta de planificación completa, un sistema de informes completo con notificación por correo electrónico y un cliente de correo electrónico (no se admiten copias de seguridad en línea).

Se trata de una herramienta de copias de seguridad clásica, con copias programadas, aviso por correo electrónico, posibilidad de guardar los archivos en dos o más espacios a la vez, compresión en un único ZIP para que ocupe menos espacio y protegido con contraseña. Asimismo se caracteriza por su facilidad a la hora de su configuración.

Las principales características de esta solución sectorial hotelera son las siguientes:

- **Transferencia de datos y duplicación de archivos**: Uranium Backup puede copiar archivos y car prácticamente cualquier dispositivo de almacenamiento masivo: discos duros USB/Firewire/SATA externos, RDX/REV, dispositivos NAS, etc.
- **Orígenes y destinos ilimitados**: La gran flexibilidad de Uranium Backup permite configurar tareas de seguridad con un número ilimitado de elementos de origen y copiar los datos en un número ilimitado de ubi también con ejecuciones en paralelo y un alto rendimiento.
- **Exclusión de la copia de seguridad carpetas y archivos específicos**: Ahorra espacio de almacenamien dispositivos de copia de seguridad y consigue un mejor rendimiento de la copia de seguridad excluyendo a carpetas específicos de la copia de seguridad. Uranium permite configurar fácilmente filtros avanzados ba extensiones de archivos (inclusión y exclusión), rutas de acceso específicas e incluso rutas de acceso pa dinámicas.
- **Compresión ZIP y cifrado AES 256 bits**: Uranium puede comprimir archivos y carpetas utilizando la altamente compatible compresión Zip64 con el fin de ahorrar espacio de almacenamiento. También puedes datos con el algoritmo más seguro que existe hoy en día: AES 256 bits.
- **Copia de permisos NTFS (ACL)**: Uranium Backup puede copiar y sincronizar también atributos de segu NTFS (ACL) y, por tanto, es posible mantener los permisos existentes que se han aplicado específicamente a los o a las carpetas.
- **Planificación de copias de seguridad automáticas**: Uranium Backup incluye una herramienta de plan automática y flexible, para poder configurar las copias de seguridad del ordenador en cualquier momento sin qu que recordártelo.
- **Eficaz sistema de notificaciones por correo electrónico**: después de cada copia de seguridad, Uraniun puede enviar una notificación por correo electrónico que indica por ejemplo si la copia de seguridad se ha correctamente.

Aspectos a tener en cuenta

Como medida de precaución, las copias periódicas deben ser resguardadas en otros dispositivos, periféricos como CD o discos externos de memoria, u otro sistema informático, para garantizar la disponibilidad de dichos datos si el equipo actual se corrompiese y no permitiese el acceso a los datos almacenados en él.

Además, esas copias tienen que estar perfectamente identificadas o etiquetadas de tal forma que se sepa de qué es la copia, de que fecha es,...

Una limitación que tiene Uranium Backup es que no tiene una funcionalidad de recuperación de la copia de seguridad. Hay ir al sitio en donde se almacenó y copiar los archivos manualmente en donde se requieran.

Casos de Éxito

Descarga	Soporte / Ayuda
http://www.uranium-backup.com/es/descargar-uranium-backup/	http://www.uranium-backup.com/es/soporte-tecnico/

Coste

La versión gratuita del programa ofrece las funcionalidades básicas de planificación, registros. Esta versión no tiene realmente mucha funcionalidad y cuenta con tantas restricciones que realmente no merece la pena.

En cuanto a las licencias de pago, se tienen las siguientes posibilidades por instalación:

- *Uranium Backup Base*, 80€ (IVA no incluido), permite planificación, registros, sincronización, servicio de grabación en CD/DVD/BD, imágenes de disco.
- *Uranium Backup Pro Tape*, 150€ (IVA no incluido), permite planificación, registros, sincronización, servicio de grabación en CD/DVD/BD, imágenes de disco, backup en cinta.
- *Uranium Backup Pro DB*, 150€ (IVA no incluido), permite planificación, registros, sincronización, servicio de grabación en CD/DVD/BD, imágenes de disco, Backup de Exchange/SQL.
- *Uranium Backup Pro Shadow*, 150€ (IVA no incluido), permite planificación, registros, sincronización, servicio de grabación en CD/DVD/BD, imágenes de disco, instantánea (VSS).
- *Uranium Backup Pro Virtual*, 229€ (IVA no incluido), permite planificación, registros, sincronización, servicio de grabación en CD/DVD/BD, imágenes de disco, instantánea (VSS), Backup de MVs ESX/ESXi.
- *Uranium Backup Gold*, 290€ (IVA no incluido), permite planificación, registros, sincronización, servicio de grabación en CD/DVD/BD, imágenes de disco, Backup en cinta, Backup de Exchange/SQL, instantánea (VSS), Backup de MVs ESX/ESXi.

Existen descuentos aplicados en función del número de licencias que se vayan a adquirir.

No incluye:

- Tiempo de instalación.
- Tiempo de recursos para formarse en el manejo de la herramienta

Principales hitos de implantación

Es una herramienta que hay que descargar e instalar. Además, es necesario el realizar su configuración:

- Orígenes de datos a copiar
- Destino de la copia
- Planificación de las copias para automatizarlas
- Configurar alertas de email

Se estima necesario hasta 2 días para la implantación del software con su configuración correspondiente, si bien otro factor que influirá en el tiempo de implantación es la capacitación y el conocimiento técnico de la persona o empresa que lo realiza.

Back In Time	URL: http://backintime.le-web.org/
Temática	**Dificultad**
Seguridad	MEDIA

Descripción y principales características

Back In Time es una aplicación de copias de seguridad que, al estilo de Time Machine de Apple, toma "instantáneas" del equipo en momentos determinados para posteriormente restaurar esos archivos o directorios.

El funcionamiento de esta aplicación es el siguiente: toma "fotos/instantáneas" del equipo en un momento dado y hace una copia de los ficheros. La aplicación gestiona las diferentes instantáneas de forma incremental (solo añade los cambios), permitiendo la restauración del subconjunto de archivos deseado en el momento que se desee.

Back In Time permite al usuario:

- Mantener su disco duro a salvo con una copia de seguridad.
- Recuperar documentos o directorios sin problemas.
- Realizar copias manualmente o programarlas por días, semanas o meses.
- Limitar el tamaño máximo de las copias y la antigüedad de las mismas.

Esta herramienta es sólo utilizable para GNU Linux y Unix.

Aspectos a tener en cuenta

Como medida de precaución, las copias periódicas deben ser resguardadas en otros dispositivos, periféricos como CD o discos externos de memoria, u otro sistema informático, para garantizar la disponibilidad de dichos datos si el equipo actual se corrompiese y no permitiese el acceso a los datos almacenados en él.

Además, esas copias tienen que estar perfectamente identificadas o etiquetadas de tal forma que se sepa de qué es la copia, de que fecha es,...

La herramienta es gratis y esto es un diferencial respecto a otras de la familia pero una clara limitación es que está hecha para funcionar sólo en ambientes Linux, lo que la hace inaccesible para la mayoría de usuarios.

Casos de Éxito

Descarga	Soporte / Ayuda
http://backintime.le-web.org/download_page/	https://answers.launchpad.net/backintime

Coste

Programa gratuito.

No incluye:

- Tiempo de instalación
- Tiempo de recursos para formarse en el manejo de la herramienta

Principales hitos de implantación

Es una herramienta que hay que descargar e instalar. Además, es necesario el realizar su configuración:

- Orígenes de datos a copiar
- Destino de la copia
- Planificación de las copias para automatizarlas

Se estima necesario de 3 a 4 días para la implantación del software con su configuración correspondiente, si bien otro factor que influirá en el tiempo de implantación es la capacitación y el conocimiento técnico de la persona o empresa que lo realiza.

FBackup	URL: http://www.fbackup.com/
Temática	**Dificultad**
Seguridad	MEDIA

Descripción y principales características

FBackup tiene una interfaz sencilla que va guiando al usuario en el proceso de definición de la tarea de respaldo mediante un asistente.

Las principals características de Back In Time son:

- **Es gratuito para uso personal y comercial**. FBackup es un software de copia de seguridad gratuita, tanto para uso comercial y personal.
- **Copias de seguridad automáticas**. Se define una tarea de respaldo, y se pone a funcionar de forma automática, ya que la herramienta FBackup ejecutará automáticamente la copia de seguridad en la fecha programada.
- **Copia de seguridad con compresión ZIP estándar**. Cuando se utilice "copia de seguridad completa" , las fuentes se archivarán utilizando compresión zip estándar. FBackup utiliza la compresión ZIP64 , lo que significa que puede crear archivos zip con un tamaño superior a 2 GB. Asimismo, la herramienta ofrece la posibilidad de proteger los archivos zip de copia de seguridad con contraseña.
- **Copias exactas de los archivos**. Si el usuario no quiere tener los archivos almacenados en un archivo zip, FBackup puede hacer copias exactas de las fuentes de copia de seguridad con "backup espejo". Desde FBackup también se pueden realizar copias de seguridad de las carpetas vacías, puede utilizar este tipo de copia de seguridad para crear en el destino de un "espejo" copia de los archivos originales.
- **Ejecutar acciones antes / después de la copia de seguridad**. Para cada trabajo de copia de seguridad, se puede definir una acción para ejecutar antes o después de la copia de seguridad. Por ejemplo, puede seleccionar "Borrar copia de seguridad" antes de ejecutar la copia de seguridad o "cerrar sesión" el ordenador una vez que la copia de seguridad ha terminado con éxito.
- **Actualizaciones automáticas**. FBackup comprueba automáticamente si hay actualizaciones semanales, de modo que el usuario sabrá cuando se libera una nueva versión.
- **Destinos de copia de seguridad múltiples**. Por defecto, las copias de seguridad se almacenan en la partición local de Windows pero se puede indicar otro destino.
- **Copia de seguridad de archivos abiertos**. Si un archivo está en uso por otro programa en el momento de la copia de seguridad, FBackup todavía será capaz de realizar una copia de seguridad de ese archivo, ya que utiliza el Servicio de instantáneas de volumen que Windows proporciona. Por lo tanto, siempre y cuando el usuario esté utilizando Windows 8, 7 , Vista, XP , 2008 / Server 2003 (32/64-bit) , FBackup respaldará los archivos abiertos.
- **Multi-idioma**

Aspectos a tener en cuenta

Como medida de precaución, las copias periódicas deben ser resguardadas en otros dispositivos, periféricos como CD o discos externos de memoria, u otro sistema informático, para garantizar la disponibilidad de dichos datos si el equipo actual se corrompiese y no permitiese el acceso a los datos almacenados en él.

Además, esas copias tienen que estar perfectamente identificadas o etiquetadas de tal forma que se sepa de qué es la copia, de que fecha es,...

Cabe destacar la gran sencillez de esta herramienta.

Casos de Éxito

Descarga	Soporte / Ayuda
http://www.fbackup.com/quick-download.php	• Foro de la herramienta: http://www.fbackup.com/forum/

Coste

Programa gratuito.

No incluye:

- Tiempo de instalación
- Tiempo de recursos para formarse en el manejo de la herramienta

Principales hitos de implantación

Es una herramienta que hay que descargar e instalar. Además, es necesario el realizar su configuración:

- Orígenes de datos a copiar
- Destino de la copia
- Planificación de las copias para automatizarlas

Se estima necesario de 1 a 2 días para la implantación del software con su configuración correspondiente, si bien otro factor que influirá en el tiempo de implantación es la capacitación y el conocimiento técnico de la persona o empresa que lo realiza.

Nombre	Gestión de usuarios y contraseñas
Temática	Seguridad

Descripción y principales características

Actualmente el método más extendido para obtener acceso a información personal que hemos almacenado en nuestro equipo y/o servicios en línea es mediante contraseñas que solo debe conocer el propietario de la herramienta o de la cuenta.

Esta contraseña es habitualmente la única barrera entre nuestro datos confidenciales y potenciales atacantes merece la pena invertir un poco de tiempo y esfuerzo en generar y utilizar una contraseña segura. Para generar contraseñas seguras hay que tener en cuenta:

- La longitud de las contraseñas no debe ser inferior a ocho caracteres. A mayor longitud más difícil será de reproducir y mayor seguridad ofrecerá.
- Las contraseñas deben estar formadas por una mezcla de caracteres alfabéticos (donde se combinen las mayúsculas y las minúsculas), dígitos e incluso caracteres especiales (@, ¡, +, &,...).
- Cambia las contraseñas regularmente. (Por ejemplo cada x meses).
- Evitar lo siguiente:
    - La contraseña no debe contener el identificador o nombre de usuario de la cuenta, o cualquier otra información personal que sea fácil de averiguar (cumpleaños, nombres de hijos, conyuges, ...).
    - Usar la misma contraseña para todo. Si alguna de ellas queda expuesta, todas las demás cuentas protegidas por esa misma contraseña también deberán considerarse en peligro.
    - Guardar las contraseñas en un lugar público y al alcance de los demás.
    - Compartir las contraseñas en Internet, por correo electrónico ni por teléfono

Aspectos a tener en cuenta

El problema que existe actualmente, es que cada aplicación o sitio web en el que se esté registrado exige que se cree un usuario con su contraseña correspondiente. Y para recordarlas todas habitualmente se pone siempre la misma lo cual supone un riesgo de seguridad. Por ello existen programas de gestión de contraseñas que las almacenan para evitar tener que ser recordadas todas. Y para acceder al listado de claves hay una clave o “palabra maestra” que es la que sí ha de ser recordada.

Valor añadido para el negocio

- Mejora la seguridad de equipos individuales y de la red
- Permite gestionar los accesos a estos sistemas informáticos
- Se gestiona la información disponible
- Se delimita qué información es accesible y a quién
- Permite verificar quién accede al sistema informático
- Permite cifrar la información de cada usuario

Tipo de Inversión	Tiempo de Implantación
BAJA	CORTO

Casos de Éxito

Aplicaciones

Nombre	Precio	Ventajas	Inconvenientes	Dificultad
CLAVES .EXE DE ASOCIACION DE INTERNAUTAS	Gratis	Generación de claves		Baja
KEEPASS	Gratis	Almacenamiento de claves		Baja

KeePass	URL: http://keepass.info/
Temática	**Dificultad**
Seguridad	BAJA

Descripción y principales características

KeePass es un programa de gestión de parejas usuario/contraseñas para PCs:

- Software de código abierto que permite disponer del código para realizar cualquier modificación sobre él si la empresa lo requiriera.
- Gratuito, sin coste de licencias.

Su principal característica es:

- Almacena todas las claves en una única base de datos con una fuerte encriptación.
- Se puede acceder a la base de datos mediante una única clave o palabra de paso que es la que hay que recordar.
- La base de datos sólo se puede almacenar en local no da la opción de almacenamiento en la nube.

La aplicación KeePass es una solución Open Source que se caracteriza por:

- Funciona sobre Windows
- Es portable y no requiere instalación; se puede transportar en un USB y ejecutar en cualquier ordenador.
- La lista de claves se puede exportar a múltiples formatos como TXT, HTML, XML and CSV.
- Se pueden gestionar las claves por grupos.
- Se pueden asignar teclas o combinaciones de ellas a las claves. Si la aplicación está en ejecución en fondo, puede auto-completar la clave en un formulario al pulsar la combinación correspondiente.
- Soporta multilenguaje, entre ellos el castellano

Aspectos a tener en cuenta

Los riesgos más comunes en una implantación de un software de gestión de claves es la palabra de paso para acceder a la base de datos de claves, no debe ser olvidada.

En cuanto a los aspectos a tener en cuenta son:

- Al ser una aplicación para recordar contraseñas, estas no han de ser recordadas por el usuario con lo que puede generar claves fuertes y complejas.
- Asimismo, es de vital importancia, por tanto, que esta palabra de paso sea muy robusta para que el resto no se vean en peligro. También es sumamente importante que no sea apuntada ni divulgada en forma alguna.

Casos de Éxito

Descarga	Soporte / Ayuda
http://keepass.info/download.html	http://keepass.info/help/base/index.html

Coste

Programa gratuito.

No incluye:

- Mantenimiento (actualización de versiones por ejemplo)
- Tiempo de recursos para formarse en el manejo de la herramienta

Principales hitos de implantación

Esta herramienta no requiere de instalación, únicamente se ha de descargar.

El tiempo de implantación es inmediato, una vez descargado. No obstante es necesario invertir cierto tiempo para poder familiarizarse con la herramienta. Este tiempo podrá ser de hasta 1 día en función de la capacitación y el conocimiento técnico de la persona o empresa que la utiliza.

Claves.exe	URL: http://www.seguridadenlared.org/73.html
Temática	**Dificultad**
Seguridad	BAJA

Descripción y principales características

Claves.exe es un programa generador de contraseñas seguras creado por la Asociación de Internautas que lo pone a disposición de los usuarios de forma gratuita.

- Aplicación muy sencilla.
- Gratuito, sin coste de licencias.

Su principal característica es:

- Tiene varias opciones para formar una clave segura, desde simples combinaciones de letras (mayúsculas o minúsculas) hasta combinaciones con números, caracteres especiales o todo ello junto.
- Permite obtener contraseñas desde 8 a 14 caracteres.
- Funciona sobre Windows
- Ocupa sobre 700 Kb y no requiere instalación
- Se puede copiar la clave generada y pegarla en otro documento (por ejemplo una aplicación de gestión de usuarios/contraseñas)

Aspectos a tener en cuenta

Aspectos a tener en cuenta en la generación de claves son los siguientes:

- Las combinaciones de letras, números y caracteres especiales proporcionan contraseñas más seguras.
- Cuanta más cantidad de caracteres tenga una contraseña, más segura es.

Casos de Éxito

Descarga	Soporte / Ayuda
http://www.seguridadenlared.org/archivos/claves.zip	• Formulario de contacto: http://www.seguridadenlared.org/contactar.php

Coste

Programa gratuito.

No incluye:

- Tiempo de recursos para formarse en el manejo de la herramienta

Principales hitos de implantación

Esta herramienta no requiere de instalación, únicamente se ha de descargar. Por tanto, su tiempo de implantación es inmediato, una vez descargado e instalado.

Nombre	Sistemas y herramientas criptográficas
Temática	Seguridad

Descripción y principales características

Son herramientas destinadas a proteger la confidencialidad de la información tanto en tránsito como almacenada. Permiten el cifrado y descifrado de la información mediante técnicas criptográficas, lo que impide un uso indebido de la misma por personas no autorizadas y permite el intercambio de la información de forma segura a través de medios o sistemas de comunicación inseguros, por ejemplo a través de correo electrónico o transferencia de ficheros.

Así mismo, no solo protege la confidencialidad de la información, sino que además incorpora mecanismos para detectar modificaciones, cambios o manipulaciones durante su envío o almacenamiento. Por tanto, son herramientas que también protegen la integridad de la información.

Estas herramientas se pueden utilizar:

- Para la protección de las comunicaciones, cuando intervenga información sensible o se estén llevando a cabo transacciones electrónicas. Así mismo, es muy recomendable su uso en el envío de todo tipo de información a través de correo electrónico.
- Para el cifrado de información confidencial almacenada en soportes de almacenamiento tanto fijos como extraíbles, como son los discos duros, memorias USB (pen-drives), así como ordenadores portátiles y todo tipo de dispositivos con los que habitualmente se viaje.

Por ello existen dos tipos de sistemas:

- **Herramientas de cifrado de las comunicaciones**. Son herramientas que protegen la información en tránsito en aplicaciones de: mensajería instantánea, correo electrónico, navegación web, etc. Permiten ocultar la información en mensajes y ficheros adjuntos para que se puedan enviar de forma segura a través de una red insegura, como es internet.
- **Herramientas de cifrado de discos duros y soportes de almacenamiento**. Son herramientas destinadas a la encriptación de todo tipo de soportes de almacenamiento: discos duros (de servidores ordenadores personales y estaciones de trabajo), discos duros externos y memorias USB.

Aspectos a tener en cuenta

Estas herramientas además, permiten detectar modificaciones, cambios o manipulaciones durante su envío o almacenamiento.

El uso de estas herramientas debe ir acompañado de seguridad en acceso a redes sobre todo inalámbricas, uso de VPNS etc..

Valor añadido para el negocio

- Protege la información confidencial
- Confianza de los usuarios
- Evita posibles sanciones administrativas por violación de la legislación. Imperativo legal
- Almacenamiento seguro
- Autenticación de la información
- Comunicación segura

Tipo de Inversión	Tiempo de Implantación
BAJA	MEDIO

Casos de Éxito				
Aplicaciones				
Nombre	**Precio**	**Ventajas**	**Inconvenientes**	**Dificultad**
GNU PRIVACY	Gratis			Media

GNU Privacy Guard	URL: http://www.gnupg.org/
Temática	**Dificultad**
Seguridad	MEDIA

Descripción y principales características

GNU Privacy Guard es una herramienta de software libre de cifrado y firmas digitales.

El programa vio la luz en 1991, y desde entonces se ha convertido en una herramienta imprescindible para el cifrado de toda clase de archivos, ya que a pesar de sus más de 20 años de vida, sigue siendo una tecnología de cifrado muy segura.

GPG cifra los mensajes usando pares de claves individuales asimétricas generadas por los usuarios. Las claves públicas pueden ser compartidas con otros usuarios pero siempre cuidadosamente para prevenir falsas identidades.

Aspectos a tener en cuenta

El cifrado se puede aplicar a cualquier elemento virtual, como mensajes, comunicaciones, archivos y documentos. PGP tiene muchas utilidades, como por ejemplo, adjuntar una firma digital a un documento o archivo, lo que le da veracidad y permite al receptor cerciorarse de que ese fichero ha sido enviado por quien dice ser y no por un impostor. Por otro lado, PGP también sirve para crear certificados seguros para, por ejemplo, servicios online.

Casos de Éxito

Descarga	Soporte / Ayuda
http://www.gpg4win.org/	http://www.gnupg.org/documentation/index.html

Coste

Herramienta gratuita.

No incluye:

- Tiempo de instalación y configuración del software.
- Tiempo de aprendizaje.

Principales hitos de implantación

Para empezar a usar el GNU Privacy Guard, hay que hacer lo siguiente:

1- Descargarse el programa.
2- Instalarlo en cada ordenador en que se desee usar

La instalación de estas soluciones es prácticamente inmediata. En cualquier caso, se estima en 1 a 3 días el tiempo en familiarizarse con la herramienta en función de los conocimientos técnicos de la persona que acometa la tarea.

Nombre	Redes privadas: VPNs
Temática	Seguridad

Descripción y principales características

VPN (Virtual Private Network) o “red privada virtual” permite extender una red privada a través de una red pública (internet) de manera segura.

Una VPN permite utilizar una red pública, ampliamente extendida y de bajo costo cómo Internet para aumentar la movilidad, mejorar la productividad de los empleados. Estos trabajadores remotos que desarrollan sus actividades en la calle, en el hogar o en otras oficinas, disponen así de un acceso a una única red privada de la compañía desde cualquier parte del mundo utilizando su ordenador e Internet.

Las VPN se implementan usando protocolos especiales que permiten a los usuarios comunicarse de manera segura y comprobar que la transmisión se hace desde una fuente confiable navegando en la red como si estuvieran en su propia oficina.

Los aspectos esenciales que debe garantizar una red privada virtual son:

- **Autenticación y autorización**: garantiza que los datos están siendo trasmitidos o recibidos desde dispositivos remotos autorizados y no desde un equipo cualquiera haciéndose pasar por él.
- **Integridad**: Asegura que los datos no han sido modificados o alterados durante la transmisión.
- **Confidencialidad de los datos**: en el caso que fuesen interceptados durante la transmisión, no pueden ser decodificados. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma.

Aspectos a tener en cuenta

Con una inversión relativamente pequeña, se la posibilidad de una conexión global desde cualquier parte del mundo con la oficina. Cada usuario remoto de la red empresarial puede comunicarse de manera segura y confiable utilizando Internet para conectarse a su red privada local.

Una VPN puede crecer para adaptarse a más usuarios y diferentes lugares mucho más fácil que las líneas dedicadas. De hecho, la escalabilidad es otra de las grandes ventajas de una VPN sobre las líneas rentadas.

Valor añadido para el negocio

- Facilidad de comunicación
- Integridad, confidencialidad y seguridad de datos
- Reducción de costes en comunicación
- Fácil de usar.
- Mejora la productividad al extender la red empresarial y sus aplicaciones.
- Aumento de flexibilidad

Tipo de Inversión	Tiempo de Implantación
MEDIA	MEDIO

Casos de Éxito				
Aplicaciones				
Nombre	**Precio**	**Ventajas**	**Inconvenientes**	**Dificultad**
OPENVPN	Desde 7,5$/año	Gratuita en modo prueba Libre y configurable		Alta
JUNOS PULSE	2000$/año aprox	Reduce coste y tiempo de implementación		Alta

Open VPN	URL: http://openvpn.net/
Temática	**Dificultad**
Seguridad	ALTA

Descripción y principales características

Una VPN utiliza las redes públicas de telecomunicaciones para llevar a cabo comunicaciones de datos privados. La mayoría de las implementaciones VPN utilizan Internet como la infraestructura pública y una variedad de protocolos especializados para soportar comunicaciones privadas a través de Internet.

OpenVPN Access Server es una solución de software con todas las funciones de Capa de Internet Segura (SSL) VPN que integra capacidades de servidor OpenVPN, las capacidades de gestión empresarial, simplificada OpenVPN conectan la interfaz del usuario, y los paquetes de software de cliente.

Las principales características de esta herramienta son las siguientes:

- **Compatible** con todos los sistemas operativos.
- Basado en software de **código abierto**. Esto significa que puede crearse para cualquier plataforma o dispo restricciones, desarrollar una interfaz de usuario mediante la interfaz de gestión, mientras que al mismo tiem interoperar con las características más avanzadas de OpenVPN tal y como la autenticación multi- factor.
- **Autenticación de desafío / respuesta**. Esta funcionalidad permite a los usuarios del servidor de acceso a d su propia módulos de autenticación que pueden iniciar una autenticación secuencia de pregunta/respues significa que el módulo de autenticación puede pedir al usuario un número de preguntas, y obtener sus respues atrás, con el fin de decidir si se permite o no el acceso.
- **Capacidad de inicio de sesión único**. Mediante el uso de módulos de autenticación personalizados con l posible implementar un inicio de sesión único, donde la firma en la VPN de forma automática pre - auten aplicaciones web que los usuarios finales necesitan acceder a través de la VPN .
- **Ejecución de scripts de forma segura en los clientes**. En este caso el servidor de acceso tiene un model más flexible para la secuencia de comandos, incluyendo muchas salvaguardas (tales como la firma de la escrit prevenir el abuso de esta capacidad.

Aspectos a tener en cuenta

Antes de desplegar la herramienta es conveniente probar adecuadamente que la conexión funciona así como las aplicaciones corporativas a través de dicha conexión. Por ello es conveniente al menos al principio, habilitarla a un grupo reducido de usuarios para probar y solucionar posibles problemas que surjan.

Casos de Éxito

Descarga	Soporte / Ayuda

https://openvpn.net/index.php/access-server/overview.html	• Tutoriales y ayuda: https://openvpn.net/index.php/access-server/section-faq-openvpn-as.html

Coste

Aplicación gratuita para los dos primeros accesos a la aplicación para modo de prueba. Luego hay que comprar licencia cuyo coste varía en función del período de vigencia:

- Licencia anual, con un precio de 7,5$ por conexión de cliente, con una compra mínima de 10 clientes.
- Licencia bianual, con un precio de 14,5$ por conexión de cliente con una compra mínima de 10 clientes.
- Licencia trianual, con un precio de 20,25$ por conexión de cliente con una compra mínima de 10 clientes.
- Licencia para cuatro años, con un precio de 25,50 $ por conexión de cliente con una compra mínima de 10 clientes.
- Licencia para cinco años, con un precio de 30$ por conexión de cliente con una compra mínima de 10 clientes.

En todos los casos, el precio incluye las actualizaciones y el soporte..

No incluye:

- Tiempo de instalación y configuración.
- Tiempo de recursos para formarse en el manejo de la herramienta

Principales hitos de implantación

OpenVPN Access Server consta de tres componentes principales: Servidor OpenVPN, interfaz de usuario Interfaz Web admin / admin y Connect Client.

- Instalar el paquete OpenVPN-AS.
- Posteriormente se procede a la configuración de la Interfaz Web admin.
- Configuración de la red de ajuste de los servidores.
- Definición de los ajustes del VPN, tales como la dirección de red IP dinámica.
- Configuración de los permisos del usuario.

Se estima necesario hasta 5 o 6 días para la implantación del software con sus pruebas de conexión, si bien otro factor que influirá en el tiempo de implantación es la capacitación y el conocimiento técnico de la persona o empresa que lo realiza.

Junos Pulse	URL: http://www.juniper.net/
Temática	**Dificultad**
Seguridad	ALTA

Descripción y principales características

Junos Pulse permite la conectividad dinámica VPN SSL, control de acceso a red (NAC), seguridad móvil, y la colaboración, a través de una interfaz de usuario final simple. Simplifica y optimiza la conectividad a los usuarios finales, al mismo tiempo, comprobar su tipo de dispositivo y el estado de seguridad, la ubicación, identidad, y la adhesión a las políticas de control de acceso de las empresas.

Junos Pulse entrega de manera inteligente servicios a través de una interfaz de usuario integrada para dispositivos móviles y no móviles donde los administradores pueden simplificar y asegurar la rápida y móvil sin problemas, a distancia, y la red local, la nube, y el acceso a las aplicaciones a los usuarios finales mediante la configuración de políticas que permite automáticamente el apropiado red o nube conexión - sin interacción del usuario.

Las principales características de esta herramienta son:

- Permite segura la identidad y acceso a la red móvil y remota basada en roles, y aumenta la visibilidad y capa gestión.
- Reduce el costo y el tiempo de implementación.
- Utiliza estándares de la industria y abiertos, como la red de confianza Connect (TNC) especificaciones.
- Sirve como una plataforma de integración de un conjunto cada vez mayor de las mejores en su clase de dis móviles y administración de aplicaciones, seguridad móvil , el acceso y soluciones de conectividad.
- Proporciona una plataforma de servicios de valor añadido para los proveedores de servicios.
- AppConnect pulso por aplicación VPN SDK contiene transparencia y seguridad a las comunicaciones de apl móviles para iOS y dispositivos Android.
- Junos Pulse es la única solución integrada de acceso, la seguridad y la colaboración que las empresas neces apoyar tanto Bring Your Our Device (BYOD) permitiendo "trabajar en cualquier parte" aplicable a cualquier disp

Aspectos a tener en cuenta

Antes de desplegar la herramienta es conveniente probar adecuadamente que la conexión funciona así como las aplicaciones corporativas a través de dicha conexión. Por ello es conveniente al menos al principio, habilitarla a un grupo reducido de usuarios para probar y solucionar posibles problemas que surjan.

Casos de Éxito

Descarga	Soporte / Ayuda

http://www.juniper.net/support/downloads/	http://www.juniper.net/customers/support/

Coste

El precio de la licencia está en torno a los 2.000 dólares al año. No obstante, hay que ponerse en contacto con Juniper directamente o bien con un partner certificado, y harán una oferta personalizada para la empresa.

https://www.juniper.net/es/es/how-to-buy/

Principales hitos de implantación

Hay que descargar e instalar el software y activarlo. Para activarlo, hay que generar el código de activación desde la página web de Juniper. Acto seguido hay que configurar la conexión remota con la red interna de la empresa, habilitando

Se estima necesario hasta 5 o 6 días para la implantación del software con sus pruebas de conexión, si bien otro factor que influirá en el tiempo de implantación es la capacitación y el conocimiento técnico de la persona o empresa que lo realiza.