SOLUCIONES DE SEGURIDAD INFORMÁTICA PARA EMPRESAS – OCTUBRE 2022

INTRODUCCIÓN

En este dossier se indican las nuevas soluciones que han puesto en marcha los técnicos de Apunts Informática con el objetivo de mejorar la Seguridad Informática de las empresas.

Debido al gran numero de intrusiones y estafas que se producen a través de internet, nos hemos visto obligados a redoblar nuestros esfuerzos y actualizar las soluciones informáticas que ofrecemos a las empresas, para evitar todos estos problemas. A fecha de hoy las principales causas de perdida de datos por parte de las empresas, con el consiguiente coste económico que esto conlleva, vienen derivados por los siguientes motivos:

- La suplantación de identidad
- El hackeo de cuentas de correo
- La encriptación y secuestro de datos
- El acceso a datos bancarios y otros datos sensibles de las empresas y usuarios

SOLUCIONES DE SEGURIDAD INFORMÁTICA PARA EMPRESAS

A continuación les indicamos las soluciones profesionales a nivel de seguridad informática que hemos incorporado a nuestros servicios profesionales y que recomendamos encarecidamente a cualquier empresa actual.

1. Antivirus Profesionales
2. Firewall y complementos
3. Copias de seguridad avanzadas
4. Auditoria de seguridad informática
5. Recomendaciones y buenas prácticas

OBJETIVOS DE ESTE DOSSIER DE SEGURIDAD

El objetivo fundamental de este dossier es el de fortalecer los mecanismos de seguridad de las empresas para evitar intrusiones y pérdidas de información.

Los técnicos de Apunts Informática se comprometen a realizar una auditoria externa totalmente objetiva, para encontrar las deficiencias en los sistemas de seguridad y protección a nivel informático en las empresas.
A partir de esta auditoria se establecerán unas recomendaciones que la empresa puede seguir para mejorar la seguridad de su sistema.

1 ANTIVIRUS PROFESIONALES – OCTUBRE 2022

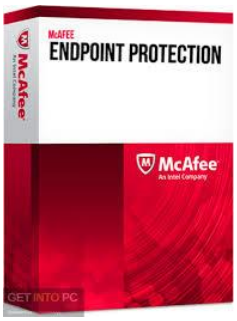
Endpoint Antivirus es un tipo de software diseñado para ayudar a detectar, prevenir y eliminar el malware en los dispositivos, tales como virus, gusanos, bots, troyanos y más.

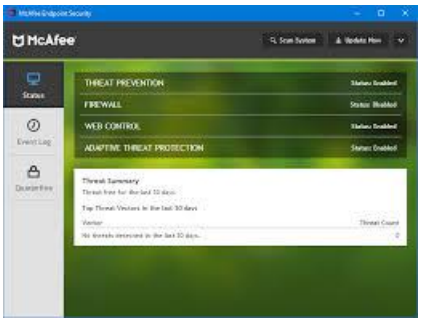
La mejores soluciones de antivirus Endpoints incluyen las siguientes características:

- La capacidad de ejecutar escaneos tanto a intervalos programados como manualmente
- Funciones de seguridad en Internet, incluida la advertencia cuando está a punto de visitar un sitio que parece malicioso y bloquea las descargas automáticas y maliciosas.
- Se actualiza automáticamente para garantizar que la protección contra las amenazas más recientes.
- La capacidad de identificar el tipo de malware que ataca el Endpoint.

OPCIÓN 1:

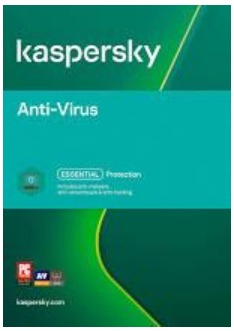
- Endpoint McAfee Antivirus
- Precio Especial: 33,00€ año/usuario





OPCIÓN 2:

- Endpoint Kaspersky Antivirus
- Precio Especial: 46,00€ año/usuario



2 FIREWALL Y COMPLEMENTOS – OCTUBRE 2022

FIREWALL DE SONICWALL

Ya sea una empresa pequeña o grande, esté en casa o en la nube, los firewalls de próxima generación (NGFW) de SonicWall le brindan la seguridad, el control y la visibilidad que necesita para una postura de seguridad cibernética efectiva. El galardonado hardware y la tecnología avanzada de SonicWall están integrados en cada firewall para darle una ventaja frente a las amenazas en evolución. Con soluciones diseñadas para redes de todos los tamaños, los firewalls SonicWall están diseñados para satisfacer sus necesidades específicas de seguridad y facilidad de uso, a un coste que protegerá su presupuesto y asegurará su red.

SONICWALL®
• SecureFirst •

AMPLIACIONES PARA EL FIREWALL DE SONICWALL

Agregue capacidades adicionales a su firewall SonicWall. Seleccione Advanced Gateway Security Suite (AGSS) para proteger su organización con la gama completa de servicios de seguridad o personalice su estrategia con opciones y capacidades individuales para satisfacer sus necesidades de seguridad.

- Advanced Gateway Security Suite (AGSS): proteja su organización con una suite completa de servicios de seguridad para firewalls SonicWall.
- Servicios de Seguridad de la Puerta de Enlace: obtenga protección en tiempo real con el antivirus de gateway, anti-spyware, prevención de intrusiones (IPS) y las funciones de application intelligence y control.
- Capture Advanced Threat Protection (ATP): defiéndase de los ataques desconocidos y de zero-day en la gateway con reparación automatizada utilizando el sandbox de múltiples motores basado en nube.
- Servicio de Filtrado de Contenido: administre el acceso a contenido web inapropiado, improductivo e incluso ilegal y malicioso.
- Servicio Integral Anti-Spam: elimine el correo electrónico no deseado en la gateway con la activación de un clic.

2 FIREWALL Y COMPLEMENTOS – OCTUBRE 2022

OPCIÓN 1: FIREWALL SONICWALL TZ270

CARACTERISTICAS PRINCIPALES SONICWALL TZ270

- Firewall Inspection: 2.00 Gbps
- Application Inspection: 1.00 Gbps
- Threat Prevention: 750 Mbps
- VPN: 750 Mbps (1 VPN de serie, soporta hasta 50)
- Maximum Connections: 750,000
- New Connections/Sec: 6,000
- Ethernet Ports: 8x1GbE

PRECIOS SONICWALL TZ270

	SONICWALL TZ270 8x1GbE	
02-SSC-6841	**SONICWALL TZ270 TOTAL SECURE - ESSENTIAL EDITION 2 AÑOS**	**1057,74**
02-SSC-6843	**SONICWALL TZ270 TOTALSECURE - ADVANCED EDITION 2 AÑOS**	**1.169,81**
02-SSC-8051	STATEFUL HA UPGRADE FOR TZ270 SERIES	127,36
	SONICWALL TZ270 WIRELESS-AC 8x1GbE	
02-SSC-6852	**SONICWALL TZ270 WIRELESS-AC INTL TOTALSECURE - ESSENTIAL EDITION 2 AÑOS**	**1.159,62**
02-SSC-6854	**SONICWALL TZ270 WIRELESS-AC INTL TOTALSECURE - ADVANCED EDITION 2 AÑOS**	**1.332,83**

02-SSC-6846	SONICWALL TZ270 SECURE UPGRADE PLUS - ESSENTIAL EDITION 2YR	957,74
02-SSC-6847	SONICWALL TZ270 SECURE UPGRADE PLUS - ESSENTIAL EDITION 3YR	1.339,81
02-SSC-6844	**SONICWALL TZ270 SECURE UPGRADE PLUS - ADVANCED EDITION 2YR**	**1.069,81**
02-SSC-6845	**SONICWALL TZ270 SECURE UPGRADE PLUS - ADVANCED EDITION 3YR**	**1.563,96**
02-SSC-6860	SONICWALL TZ270 WIRELESS-AC INTL SECURE UPGRADE PLUS - ESSENTIAL EDITION 2YR	1.125,85
02-SSC-6861	SONICWALL TZ270 WIRELESS-AC INTL SECURE UPGRADE PLUS - ESSENTIAL EDITION 3YR	1.451,89
02-SSC-6862	SONICWALL TZ270 WIRELESS-AC INTL SECURE UPGRADE PLUS - ADVANCED EDITION 2YR	1.329,62
02-SSC-6863	SONICWALL TZ270 WIRELESS-AC INTL SECURE UPGRADE PLUS - ADVANCED EDITION 3YR	1.798,30

2 FIREWALL Y COMPLEMENTOS – OCTUBRE 2022

OPCIÓN 2: FIREWALL SONICWALL TZ370

CARACTERISTICAS PRINCIPALES SONICWALL TZ370

- Firewall Inspection: 3.00 Gbps
- Application Inspection: 1.50 Gbps
- Threat Prevention: 1.00 Gbps
- VPN: 1.30 Gbps (2 VPNs de serie, soporta hasta 100)
- Maximum Connections: 900,000
- New Connections/Sec: 9,000
- Ethernet Ports: 8x1GbE

PRECIOS SONICWALL TZ370

	SONICWALL TZ370 8x1GbE	
02-SSC-6817	**SONICWALL TZ370 TOTAL SECURE - ESSENTIAL EDITION 2 AÑOS**	**1.393,96**
02-SSC-6819	**SONICWALL TZ370 TOTALSECURE - ADVANCED EDITION 2 AÑOS**	**1.541,70**
02-SSC-8052	STATEFUL HA UPGRADE FOR TZ370 SERIES	178,30
	SONICWALL TZ370 WIRELESS-AC 8x1GbE	
02-SSC-6828	**SONICWALL TZ370 WIRELESS-AC INTL TOTALSECURE - ESSENTIAL EDITION 2 AÑOS**	**1.597,74**
02-SSC-6830	**SONICWALL TZ370 WIRELESS-AC INTL TOTALSECURE - ADVANCED EDITION 2 AÑOS**	**1.770,94**

02-SSC-6822	SONICWALL TZ370 SECURE UPGRADE PLUS - ESSENTIAL EDITION 2YR	1.492,64
02-SSC-6823	SONICWALL TZ370 SECURE UPGRADE PLUS - ESSENTIAL EDITION 3YR	1.925,66
02-SSC-6820	**SONICWALL TZ370 SECURE UPGRADE PLUS - ADVANCED EDITION 2YR**	**1.701,51**
02-SSC-6821	**SONICWALL TZ370 SECURE UPGRADE PLUS - ADVANCED EDITION 3YR**	**2.272,08**
02-SSC-6836	SONICWALL TZ370 WIRELESS-AC INTL SECURE UPGRADE PLUS - ESSENTIAL EDITION 2YR	1.589,43
02-SSC-6837	SONICWALL TZ370 WIRELESS-AC INTL SECURE UPGRADE PLUS - ESSENTIAL EDITION 3YR	2.129,43
02-SSC-6838	SONICWALL TZ370 WIRELESS-AC INTL SECURE UPGRADE PLUS - ADVANCED EDITION 2YR	1.788,11
02-SSC-6839	SONICWALL TZ370 WIRELESS-AC INTL SECURE UPGRADE PLUS - ADVANCED EDITION 3YR	2.501,32

3 COPIAS DE SEGURIDAD – OCTUBRE 2022

OPCIÓN 1: GESTIÓN DE COPIAS DE SEGURIDAD CON ACRONIS CLOUD

ACRONIS BACKUP CLOUD

- Precio Especial de pago por uso (solo pagamos el espacio que usamos en la nube)
- Desde 0,20€ + IVA por cada 1GB de datos
- Acronis Backup Cloud es una solución segura, escalable e híbrida en la nube que protege todos sus sistemas y dispositivos, en todo momento y en cualquier lugar. Altamente personalizable y económica, Acronis proporciona copias de seguridad, recuperación en caso de situaciones delicadas y acceso seguro a los datos para PYMES y clientes empresariales. Las soluciones de Acronis incluyen software de copia de seguridad de servidores físicos, virtuales y en la nube, gestión de almacenamiento, intercambio seguro de archivos e implementación de sistemas
- En el precio del sistema Acronis ya incluye tanto el almacenamiento como el programa de Acronis que se instala en el equipo y que se encarga de realizar la copia de seguridad.

PRECIO Y PAQUETES DE DATOS RECOMENDADOS DE ACRONIS BACKUP CLOUD

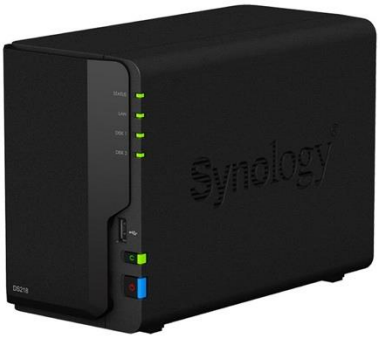
- Opción 1:
  - 100GB DE DATOS - Precio Especial: 20,00€ + IVA (mensual)
  - Sale a 0,20€ + IVA por cada 1GB de datos
- Opción 2:
  - 400GB DE DATOS - Precio Especial: 72,00€ + IVA (mensual)
  - Sale a 0,18€ + IVA por cada 1GB de datos
- Opción 3:
  - 1000GB DE DATOS (1TB)- Precio Especial: 150,00€ + IVA (mensual)
  - Sale a 0,15€ + IVA por cada 1GB de datos

3 COPIAS DE SEGURIDAD – OCTUBRE 2022

OPCIÓN 2: GESTIÓN DE COPIAS DE SEGURIDAD EN DISCOS NAS

DISCO DE RED (NAS) DE 2 BAHIAS - SYNOLOGY

- **SYNOLOGY DS218 NAS 2Bay Disk Station**
  - CPU Realtek RTD1296 Núcleo cuádruple 1.4 GHz
  - RAM 2GB DDR4 – 2 BAHIAS para disco duro
  - Capacidad interna máx. 20 TB (10TB X 2)
  - RAID compatible: Synology Hybrid RAID, Basic,
  - JBOD, RAID 0, RAID 1
  - 1 x Puerto RJ45 1GbE LAN
  - 1 x Puerto eSATA
  - 2 x Puerto USB 3.0
  - 1 x Puerto USBCopy



- Precio Especial NAS DS218 de 4TB con 2 discos de 4TB Western Digital Red (EN RAID 1): 489,00€ + IVA
- Precio Especial NAS DS218 de 6TB con 2 discos de 6TB Western Digital Red (EN RAID 1): 599,00€ + IVA
- Precio Especial NAS DS218 de 8TB con 2 discos de 8TB Western Digital Red (EN RAID 1): 749,00€ + IVA

DISCO DE RED (NAS) DE 4 BAHIAS - SYNOLOGY

- **SYNOLOGY DS418j NAS 2Bay Disk Station**
  - CPU Realtek RTD1296 Núcleo cuádruple 1.4 GHz
  - RAM 1GB DDR4 – 4 BAHIAS para disco duro
  - Capacidad interna máx. 64 TB (16TB X 4)
  - RAID compatible: Synology Hybrid RAID, Basic,
  - JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
  - 1 x Puerto RJ45 1GbE LAN
  - 2 x Puerto USB 3.0
  - 1 x Puerto USBCopy

- Precio Especial NAS DS418j de 12TB: con 4 discos de 4TB Western Digital Red (EN RAID 5): 799,00€ + IVA
- Precio Especial NAS DS418j de 18TB con 4 discos de 6TB Western Digital Red (EN RAID 5): 1089,00€ + IVA
- Precio Especial NAS DS418j de 24TB con 4 discos de 8TB Western Digital Red (EN RAID 5): 1319,00€ + IVA

3 COPIAS DE SEGURIDAD – OCTUBRE 2022

OPCIÓN 3: SISTEMA PROFESIONAL DE COPIAS DE SEGURIDAD USANDO DOS DISPOSITIVOS NAS DE SYNOLOGY

Nuestros especialistas han considerado que sistema de copias de seguridad más fiable que existe actualmente, y por lo tanto el que recomendamos es el que se basa en la utilización de dos discos NAS Synology. Un NAS situado en la propia empresa y otro de igual o menor capacidad situado en un lugar seguro fuera de la propia empresa.

- Configuración
  - 2 discos NAS Synology (pueden ser iguales o de diferentes modelos y capacidades)
  - Se instala el NAS1 en la sede principal de la empresa: en este NAS se realizará una copia de seguridad cada día de la semana de todos los archivos y programas de la empresa. Se instala el NAS2 en otra sede de la empresa, en un lugar seguro o incluso en el domicilio de uno de los responsables de la empresa, con la única condición que tengamos acceso a Internet.
- Funcionamiento
  - Todos los días de la semana se realiza una copia de seguridad de todos los datos de la empresa al NAS1. Todos los días el disco NAS1 copia los datos al NAS2. Una vez a la semana (o al mes), se realiza una copia extra con todos los datos del NAS1 al NAS2. Todos estos procesos se hacen de forma incremental, por lo que consumen poco tiempo y recursos
- Programas necesarios
  - Los programas necesarios de Synology vienen preconfigurados en los propios NAS de Synology. Usamos un programa adicional, como el Acronis o el Goodsync, para copiar los datos al NAS1 de forma automática (visto en otras secciones de este dossier)
  - Cada vez que se realiza la copia de seguridad se envía un informe por email con el resultado de la copia. El responsable puede acceder directamente al NAS1 y NAS2 para comprobar los datos
- Supuestos que resuelve
  - Los discos NAS son discos de RED que tienen unas credenciales propias, por lo que son están expuestos a los virus de encriptación. Si entra un virus en la empresa al disco NAS no tiene porque afectar-le. La empresa dispone de una copia de seguridad de cada uno de los días de la semana, por lo que siempre puede recuperar archivos hasta 7 días de antigüedad. Además, con la copia extra semanal o mensual, conseguimos tener una copia de archivos más antiguos, por si nos damos cuenta más tarde. La empresa tiene la información tanto dentro como fuera de la empresa (el NAS2 está situado fuera de las instalaciones de la misma). Esto es importante porque muchas normativas lo exigen, al mismo tiempo que evitamos perdida de datos en casos de incendios, robos, catástrofes.

3 COPIAS DE SEGURIDAD – OCTUBRE 2022

OPCIÓN 4: GESTIÓN DE COPIAS DE SEGURIDAD EN LA NUBE RECOMENDADO PARA **VOLUMENES DE DATOS GRANDES**

ALMACENAMIENTO Y GESTIÓN DE DATOS PROFESIONALES EN LA NUBE

- Somos distribuidores oficiales de DROPBOX BUSINESS
- El sistema profesional de almacenamiento y gestión de archivos en la nube más usado
- Especialmente orientado a empresas que trabajan con altos volúmenes de datos
- Permite la creación de carpetas compartidas y el trabajo colaborativo de archivos
- Seguridad de los datos: sistema de versiones de archivos de hasta 120 días

Dropbox Business

- 180 días de recuperación de archivos
- Un único inicio de sesión de administrador para gestionar varios equipos
- Consola de administración y registro de actividades
- Cifrado SSL/TLS y AES de 256 bits
- Permisos detallados de uso compartido
- Grupos administrados por la empresa y por usuarios
- Borrado remoto de dispositivos
- Doble autenticación (2FA)
- Envía archivos de hasta 2 GB con Dropbox Transfer
- Recuperación de cuentas con Rebobinado de Dropbox de 180 días
- Bloqueo de archivos
- Sincronización inteligente
- Marcas de agua de documentos
- Herramientas administrativas de Dropbox Paper

- TARIFA DE PRECIOS SEGÚN EL TAMAÑO DE LOS DATOS
  - 5000 GB DE ALMACENAMIENTO: 50,00€ + IVA (cuota mensual)
  - ALMACENAMIENTO ILIMITADO: 60,00€ + IVA (cuota mensual)

4 AUDITORIA DE SEGURIDAD INFORMÁTICA – OCTUBRE 2022

AUDITORIA DE SEGURIDAD INFORMÁTICA

En una auditoria de informática se deben revisar los siguientes aspectos para garantizar la seguridad de sus sistemas ante posibles fallos o ataques.

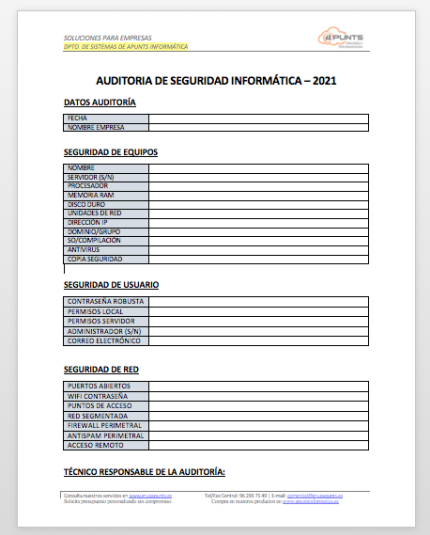
- Seguridad de equipos
  - Software de equipos y servidores
  - Hardware de equipos y servidores
- Seguridad de Redes
  - Asegurar red física
  - Seguridad del sistema físico y de red
  - Tráfico de la red aprobado
  - Tráfico de red no aprobado
  - Desarrollo de creación y mantenimiento de cuentas de los usuarios.
- Seguridad de Usuario
  - Limitación de los recursos
  - Limitación en la conexión a la red
  - Registros de actividad
  - Revisión periódica
- Seguridad de Administración del sistema
  - Control de tamaño y ubicación de los archivos
  - Ejecución de herramientas cracking
  - Comprobar la vulnerabilidad del sistema de forma manual
  - Mantener a los usuarios informados sobre las modificaciones y la seguridad
- Seguridad a nivel de Almacenamiento de Datos de Seguridad
  - Reconocimiento de los diferentes niveles de protección
  - Estructura general de los sistemas de archivo
  - Restricción de acceso
  - Revisión de seguridad de los protocolos
  - Copias de seguridad
  - Base de datos solo accesible para usuarios autorizados
- Seguridad a nivel de Protocolo y Servicios
  - Actualización de software de seguridad
  - Reconocimiento de los nuevos softwares
  - Comprobar configuración de instalación de software
  - Almacenamiento seguro
  - Controlar la sobrecarga del sistema
  - Reconocimiento de programas y almacenamiento
  - Seguimiento de los patrones típicos de software

4 AUDITORIA DE SEGURIDAD INFORMÁTICA – OCTUBRE 2022

AUDITORIA DE SEGURIDAD INFORMÁTICA (RESUMEN Y EJEMPLO PRÁCTICO)

A continuación vemos un ejemplo simplificado de los puntos a revisar una en una auditoria de informática que permita detectar vulnerabilidades con el objetivo de mejorar el sistema informático de la empresa.

- Seguridad de Equipos
  - En este punto nos centramos en revisar los propios equipos informáticos de la empresa
  - Determinar las características hardware de los servidores y equipos de la empresa: para encontrar posibles equipos obsoletos o componentes que puedan fallar.
  - Determinar los sistemas operativos, antivirus y programas propios de los servidores y equipos de la empresa: para encontrar posibles versiones con vulnerabilidades.
- Seguridad de Redes
  - En este punto se revisa el cableado estructurado, router, firewall, switches, puntos de acceso, etc.
  - Revisar posibles accesos no autorizados a la red: por cable o por wifi, desde fuera de la empresa (hackers) o desde dentro (trabajadores no autorizados)
  - Revisar segmentación de la red por departamentos, políticas de contraseñas de acceso, revisar asignación de IP estática o por DHCP
  - Revisar accesos remotos mediante VPN, Terminal Server o programas (Anydesk, Teamviewer)
- Seguridad de Usuario
  - En este punto se revisa como autentica cada usuario, y a que información tiene realmente acceso
  - Comprobación de dominio: políticas de seguridad, permisos de instalación, etc.
  - Revisión de permisos de usuario y registros de actividad
  - Asegurar la correcta gestión y uso del correo electrónico por parte de los usuarios
- Seguridad de almacenamiento y copias de seguridad
  - Almacenamiento de datos
  - Copias de seguridad
- Comunicación a los usuarios de la empresa
  - Mantener a los usuarios informados y formados sobre la seguridad en la empresa
  - Establecer protocolos de actuación ante amenazas externas habituales



SOLUCIONES PARA EMPRESAS
DPTO. DE SISTEMAS DE APUNTS INFORMÁTICA

AUDITORIA DE SEGURIDAD INFORMÁTICA – 2021

DATOS AUDITORÍA

FECHA	
NOMBRE EMPRESA	

SEGURIDAD DE EQUIPOS

NOMBRE	
SERVIDOR (S/N)	
PROCESADOR	
MEMORIA RAM	
DISCO DURO	
UNIDADES DE RED	
DIRECCION IP	
DOMINIO/GRUPO	
SO/COMPILACIÓN	
ANTIVIRUS	
COPIA SEGURIDAD	

SEGURIDAD DE USUARIO

CONTRASEÑA ROBUSTA	
PERMISOS LOCAL	
PERMISOS SERVIDOR	
ADMINISTRADOR (S/N)	
CORREO ELECTRÓNICO	

SEGURIDAD DE RED

PUERTOS ABIERTOS	
WIFI CONTRASEÑA	
PUNTOS DE ACCESO	
RED SEGMENTADA	
FIREWALL PERIMETRAL	
ANTISPAM PERIMETRAL	
ACCESO REMOTO	

TÉCNICO RESPONSABLE DE LA AUDITORÍA:

5 DOSSIER DE SEGURIDAD INFORMÁTICA Y BUENAS PRÁCTICAS EN EL USO DE LAS NUEVAS TECNOLOGÍAS PARA EMPRESAS Y USUARIOS PARTICULARES – OCTUBRE 2022

INTRODUCCIÓN Y ALCANCE DE ESTE MANUAL

Soy Xavi Gómez, responsable del departamento de Sistemas y Servicio Técnico de la empresa Apunts Informática y Telecomunicaciones SL.

Los clientes que ya nos conocen, saben que periódicamente enviamos manuales informáticos de ayuda realizados por nuestros técnicos para mejorar el funcionamiento interno de las empresas y los usuarios particulares. Estas publicaciones son totalmente gratuitas y están elaboradas en base a nuestra experiencia. La finalidad de estas guías de autoayuda es la de mejorar el uso y la integridad de los sistemas informáticos de nuestros clientes. Si no nos conocen, simplemente les diré que Apunts Informática es una empresa de L'Alcúdia (Valencia), que ha experimentado un fuerte crecimiento en los últimos años, gracias a que nuestra filosofía se basa en establecer una relación de confianza y ayuda mutua con nuestros clientes, lo que nos ha hecho crecer y evolucionar junto con ellos. Pueden consultar información sobre nuestro grupo de empresa en la web www.grupapunts.es.

En esta ocasión, queremos presentarles nuestra última aportación para mejorar el uso de los sistemas informáticos en las empresas, para los trabajadores y para los usuarios particulares. Se trata del **Manual de Seguridad Informática y Buenas Prácticas en el uso de las Nuevas Tecnologías**. Como hemos indicado anteriormente, este manual está pensado para mejorar el uso de los equipos informáticos por parte de cualquier usuario; haciendo especial hincapié en la seguridad, en la ética del uso de los ordenadores en el trabajo, en la prevención de delitos informáticos, en la prevención de riesgos, etc.

Consideramos que esta guía debe ser de lectura "obligada" por parte de cualquier empresa y de sus trabajadores. A través de este manual, no solo queremos prevenir a las empresas de los peligros más habituales a los que están expuestos hoy en día, sino que pretendemos establecer unas pautas de control dentro de las empresas para que los trabajadores sean conscientes de lo que deben hacer (y no deben hacer), para el correcto funcionamiento del sistema informático de la empresa. Tanto a nivel de seguridad, como a nivel de uso de la información, como a nivel de cumplimiento y ética profesional en sus horas de trabajo. Además, este documento es totalmente aplicable a los usuarios particulares en cualquiera de sus ámbitos personales, ya que los virus no entienden de situaciones personales y nos afectan a todos.

Siempre desde el punto de vista de uso de las nuevas tecnologías, este manual pretende ser un referente actual en temas tan importantes del uso de las nuevas tecnologías como son:

- Seguridad informática
- Suplantación de identidad
- Virus informáticos
- Acciones preventivas
- Integridad y seguridad de los datos
- Recuperación de archivos
- Ética profesional y personal
- Copias de seguridad

5 MANUAL DE SEGURIDAD INFORMÁTICA – OCTUBRE 2022

SEGURIDAD INFORMÁTICA

La seguridad informática es fundamental hoy en día cuando hablamos de las nuevas tecnologías. Un uso inadecuado nuestros equipos informáticos puede desencadenar en problemas muy importantes para nosotros mismos o para las organizaciones en las que trabajamos. El mal uso de nuestros ordenadores puede provocar perdida de información, el *hackeo* de cuentas personales, la ejecución de un delito informático o, incluso, directamente la pérdida de dinero en una rápida transacción.

Para evitar muchos de estos problemas, los usuarios deben de estar atentos y seguir unas pautas de conducta básicas en el uso de las nuevas tecnologías, que les permita anticiparse y en muchos casos evitar, estos peligros. Parece ciencia ficción, peor nada más lejos de la realidad, nuestros técnicos pueden confirmar que todos los procesos que veremos en este manual están pasando día a día en muchas de las empresas que nos rodean.

- **A nivel de empresa, estos son los principales problemas de seguridad informática actuales:**
  - Encriptación de documentos por virus informáticos
  - Acceso al contenido de cuentas de correo empresariales por parte de hackers informáticos
  - Suplantación de identidad sobre todo en el procedo de pagos/cobros de facturas
  - Perdida de datos de la empresa por errores propios o por usuarios malintencionados
  - Acceso a datos confidenciales por parte de la empresa de personas no autorizadas
  - Extracción de información confidencial o estratégica por parte de espías informáticos

- **A nivel de usuarios particulares,** estos errores anteriormente citados también se producen de igual modo, y además, encontramos otros problemas concretos de este tipo de usuarios como son:
  - Acceso a cuentas e informaciones personales
  - Compras y estafas en páginas web fraudulentas
  - Engaños informáticos a través del correo
  - Engaños informáticos a través de una página web
  - Descarga de virus y archivos dañinos en páginas web

Estas situaciones y peligros de seguridad informática son algunas de las muchas que se contemplan en este manual. Por lo que recomendamos la lectura del mismo ya que se establecen protocolos a seguir y pautas de comportamiento por parte de los usuarios para minimizar los riesgos de sufrir cualquiera de estos percances.

Como es lógico, estos ejemplos de problemas de seguridad informática están muy perseguidos por las autoridades, por lo que es recomendable siempre que nos encontremos en un caso similar denunciarlo inmediatamente a la dependencia de Delitos Informáticos de la Guardia Civil más cercana. Pero es cierto que en muchos casos, el nivel de sofisticación de los hackers informáticos hace muy difícil solucionar cualquier de estos problemas de forma rápida y satisfactoria. Por este motivo es tan importante que los trabajadores de las empresas, así como los usuarios particulares, tomen en consideración una serie de medidas preventivas y unas pautas básicas, para evitar en la medida de lo posible este tipo de problemas.

5 MANUAL DE SEGURIDAD INFORMÁTICA – OCTUBRE 2022

SUPLANTACIÓN DE IDENTIDAD

Un problema habitual hoy en día es la suplantación de identidad en el ámbito de Internet, que es básicamente hacerse pasar por otra persona. Este delito es muy frecuente, esta principalmente asociado a cuentas de correo electrónico empresariales y tiene como único objetivo conseguir dinero de forma ilícita.

- **Suplantación de identidad "Man in the middle":** Dentro de las suplantaciones de identidad destacamos esta práctica que se produce de forma constante y puede ocasionar una perdida importante de dinero.
  - Todo se inicia cuando abrimos un correo electrónico que contiene un virus
  - El virus no afecta al funcionamiento del equipo pero es capaz de descifrar la contraseña del correo
  - Una vez la clave del correo está al alcance del hacker, se queda a la escucha y monitoriza el correo del usuario a la espera de un posible negocio. Cuando ve una oportunidad de negocio, por ejemplo el pago de una factura es cuando actúa.
  - El hacker se mete de lleno en la conversación y se hace pasar por la empresa que emite la factura, indicando que ha habido un cambio en el numero de cuenta y que el ingreso del importe lo deben realizar a una cuenta concreta (la del propio hacker).
  - El usuario que recibe esta petición la atiende normalmente y realiza el ingreso del importe en una cuenta que no es la correcta. A partir de ahí, empiezan disputas entre los dos usuarios por ver quien tiene la responsabilidad, pero el mal ya está hecho, porque suelen ser cuentas extranjeras que cuando se reclama el dinero ya no están operativas en muchos casos.
  - Este sistema que parece a priori poco peligroso, debido al gran volumen de facturación y al ajetreo del día a día, se ha podido comprobar que es muy factible incurrir en este error y que en ese momento no lo tengamos en cuenta y haga el ingreso en la cuenta fraudulenta. Además, es importante remarcar que los hackers son capaces en muchos casos de copiar la firma de correo del usuario, o crear un documento bancario con los datos del usuario, etc. Por lo que puede crear un perfil muy exacto para hacerse pasar por otra persona y esto ayuda a realizar el engaño.

- **Como evitamos la situación y los peligros de la suplantación de identidad de "Man in the middle":**
  - Análisis periódico de los equipos en busca de nuevos virus informáticos
  - Protocolo de seguridad en el que NUNCA se atienda a un cambio de cuenta bancaria sin hablar antes personalmente con el cliente/proveedor propietario de esa cuenta
  - Revisión de filtros de correo (a nivel de servidor de correo) en vistas a que el hacker no haya puesto una redirección o respuesta automática (para que no nos lleguen los correos de un usuario y le reboten al propio hacker). En definitiva, revisar que no tenemos filtros indeseados en el correo electrónico, sobretodo a nivel de correos corporativos.

- Otras situaciones de suplantación de identidad pueden verse en el hackeo de cuentas de redes sociales y cuentas de correo electrónico personales, por lo que siempre debemos tener una mínima duda de que la persona con la que estamos tratando pueda no ser realmente aquella con la que creemos interactuar. Esta duda nos hará estar en guardia y en situaciones

5 MANUAL DE SEGURIDAD INFORMÁTICA – OCTUBRE 2022

VIRUS INFORMÁTICOS

Los virus informáticos siguen siendo un problema fundamental tanto para empresas como para los usuarios particulares. Es imposible estar libre de la actuación de los virus, ni teniendo el antivirus más eficiente del mundo, por lo tanto debemos ser conscientes del problema que esto supone y debemos tener en cuenta unas pautas de seguridad básicas para estar lo menos expuestos posible.

- A continuación indicamos algunos ejemplos de los principales virus informáticos de la actualidad, y en concreto, de aquellos más peligrosos y que más afectan a todo tipo de usuario:

  - **Virus del correo electrónico**
    - El virus del correo electrónico es un virus muy extendido en los últimos meses. Se trata de un virus que entra a través del correo electrónico de un cliente/proveedor conocido por nuestra empresa. El hecho de recibir un correo de una persona conocida nos motiva a abrir el fichero adjunto que en realidad es un virus. El virus accede a nuestra bandeja de entrada de correo y se auto reenvía a todos nuestros contactos, motivando así su rápida propagación.
    - Este virus no causa pérdida de datos, pero al enviarse a todos nuestros contactos empeora nuestra reputación. Al mismo tiempo, puede quedar latente a la espera de abrir puertas a nuevos virus o en el peor de los casos a encriptar los datos de nuestro equipo.
    - Si abrimos un correo electrónico y/o un archivo adjunto del mismo y vemos que el archivo no se abre ni "hace nada", debemos sospechar de este tipo de virus. Aunque parezca que no ha pasado nada, el virus estará actuando en segundo plano infectando y propagándose a nuestros contactos. Ante cualquier duda, debemos apagar el equipo o desconectarlo de Internet y solicitar ayuda inmediata a nuestro responsable o asesor informático.

  - **Virus encriptador**
    - El virus encriptador es un tipo de virus muy peligrosos que afecta a empresas y particulares de todo el mundo. Este virus puede acceder a nuestro sistema por varios procesos:
      - Al hacer click en un enlace de un email fraudulento: el email puede parecer de Correos, BBVA, Apple, de un proveedor/cliente nuestro, pero en realidad es un virus.
      - Al entrar en páginas web dudosas y ejecutar algún programa que queremos descargar e instalar en nuestro equipo.
      - De forma automática si tenemos puertos abiertos en el servidor, por ejemplo para acceder desde fuera de la oficina de forma remota.
    - Este virus causa una importante perdida de datos. Se encriptan los archivos del ordenador donde entra y de todas las carpetas de la red a la que tiene acceso ese ordenador. Incluso las versiones más peligrosas se propagan por toda la red y pueden llegar a causar infecciones masivas de equipos. Al encriptar los archivos nos aparece un mensaje con una cuenta y un importe para recuperar dichos archivos.
    - Para prevenir la ejecución de este tipo de archivos debemos seguir la norma de no abrir correos que no estamos seguros, nunca debemos descargar o instalar archivos de Internet que no

estemos seguro que son totalmente fiables, debemos minimizar la apertura de puertos externos en nuestro router y por supuesto, debemos limitarnos a acceder a páginas seguras que tengan que ver con nuestro trabajo.

- Actualmente este virus tiene pocas soluciones, aunque siempre hay opciones, tal y como explicamos en el punto de recuperación de archivos de este manual.

- **Programas basura**
  - Los programas basura son aquellos programas que se instalan en nuestro ordenador (en el propio sistema, en los navegadores, etc.) y ralentizan todo nuestro equipo e incluso toda nuestra red. Este tipo de programas tienen la misión de emitir publicidad, redirigir nuestras búsquedas a páginas de Internet nocivas, consumir recursos de nuestra red en beneficio propio.
  - Este tipo de programas-virus no producen perdida de datos. Simplemente son programas que no sirven para nada y que consumen recursos y ralentizan y perjudican a nuestro sistema. Pero si no controlamos su ejecución, podemos ver como van aumentando su incidencia en los equipos donde están instalados, hasta llegar al punto que no se puede trabajar con el equipo e incluso que rompe el propio sistema e impide que arranque con normalidad.
  - Para evitar la instalación de este tipo de programas no debemos nunca instalar programas por nuestra cuenta a no ser que seamos usuarios especializados y que tengamos la autorización del responsable informático de la empresa. Este tipo de programas se instalan muchas veces dentro de paquetes de instalación de otros programas habituales que parecen "gratuitos" pero que nos están instalando publicidad guiada en nuestro equipo de forma indirecta.
  - En el caso de que los programas ya estén instalados en nuestro equipo, hay que desinfectar tanto la instalación de programas del sistema (agregar o quitar programas), como la configuración de los navegadores (dentro del Chrome, iExplorer, Firefox), ya que ahí también se instalan como complementos o pluggins.

- **Aspectos a tener en cuenta para estar lo menos expuesto posible a virus informáticos:**
  - No abrir ningún correo electrónico que no to tengamos claro su procedencia
  - En caso de abrir un correo electrónico para ver el contenido, si no conocemos al remitente, no hacemos clic en ningún enlace o no descargar ningún archivo adjunto
  - No entrar en el correo electrónico personal ni en redes sociales desde los equipos de la empresa, ya que son nichos en cuanto a la instalación de programas publicitarios en segundo plano.
  - No entrar en páginas web marcadas como no seguras, y sobre todo no entrar en páginas web fraudulentas, de descargas, de contenidos online pirateados, etc.
  - No descargar archivos ni programas no originales, ni instalar en los equipos programas propios sin el consentimiento del responsable de sistemas.

- **Prevención y solución de problemas ocasionados por virus informáticos:**
  - Análisis periódico de los equipos en busca de nuevos virus informáticos
  - Protocolo de seguridad en el que establecemos que nunca se abra ningún correo de remitente desconocido, ni archivos adjuntos, ni hacer click en ningún enlace contenido en este tipo de emails.
  - Avisar al responsable informático de una posible detección de virus, mal funcionamiento del equipo, lentitud extrema en algunos procesos y todo lo que pueda suponer la infección de un virus.
  - En casos extremos es conveniente, ante cualquier duda, apagar el equipo o desconectarlo de la red

5 MANUAL DE SEGURIDAD INFORMÁTICA – OCTUBRE 2022

ACCIONES PREVENTIVAS

A continuación les ofrecemos un resumen de las pautas de prevención para el correcto uso de las nuevas tecnologías dentro y fuera de la empresa, tanto para entornos profesionales como para usuarios particulares. Siguiendo estas recomendaciones evitaremos muchos de los problemas que se han indicado en este informe (virus informáticos, suplantación de identidad, perdida de datos, etc.)

Pautas de prevención relacionadas con el uso de Internet:

- Aspectos a tener en cuenta cuando navegamos por Internet
  - Entrar solo a aquellas páginas web que necesitemos para desempeñar correctamente nuestro trabajo
  - Acceder a las páginas web marcadas como seguras (HTTPS), dudar en caso contrario.
  - No descargar ni ejecutar archivos de páginas web que desconozcamos

- Aspectos a tener en cuenta al comprar en Internet
  - Identificar la localización y procedencia de la web donde queremos comprar
  - Imprescindible entrar en páginas con certificado seguro HTTPS siempre que vamos a pagar
  - Utilizar métodos de pago seguros y establecidos que permitan reclamar: PAYPAL, pagos con tarjeta en pasarelas de pago de bancos conocidos por nosotros, contra reembolso, etc.
  - Nunca bajo ningún concepto ofrecer o enviar nuestros datos de tarjeta de crédito a nadie, solo introduciremos dichos datos en formularios seguros de pasarelas de pago de bancos conocidos.

Pautas de prevención relacionadas con el uso correo electrónico:

- Aspectos a tener en cuenta al usar el correo electrónico
  - En el correo electrónico podemos revivir emails de todo tipo. Antes de abrir cualquier correo electrónico, aunque sea de una persona conocida, debemos realizar un pequeño análisis de lo que nos están enviando. En caso de no tener clara su validez, hablar con el remitente y confirmar.
  - Tenemos que desconfiar de los servicios de aviso de compañías como Correos, Hacienda, Seguridad Social, Bancos, Grandes empresas, etc. Muchas veces los virus se enmascaran en mensajes fraudulentos que se intentan hacer pasar por estas empresas. Analizar el contenido antes de abrir.
  - Comprobar enlaces. Si nos situamos encima de un enlace dentro de un correo, podemos ver donde apunta ese enlace. Desconfiemos de los enlaces de dominios o palabras extrañas.
  - Comprobar archivos adjuntos. De la misma forma, si nos situamos sobre un fichero adjunto o lo descargamos (nunca lo ejecutemos directamente), podemos ver el tipo de archivo de que se trata. Desconfiemos de archivos ejecutables, analicemos si realmente estamos esperando que esa persona o entidad nos envía algún documento. Siempre análisis previo antes de ejecutar.

- Cambio de contraseñas
  - El cambio periódico de contraseñas de cualquier sistema, y por supuesto del correo electrónico, siempre es beneficioso. Puede ser que nuestra contraseña haya sido descubierta por cualquier

programa informático y si cambiamos la misma impediremos que sigan visualizando o accediendo a nuestros datos.
    - Un cambio de contraseñas cada tres meses seria lo ideal, pero en aquellas personas u organizaciones más reticentes a cambiar, deberíamos plantear un cambio de contraseña cada seis meses, o en los casos más extremos de un año. El cambio periódico de contraseñas es fundamental.

- Revisión de filtros
    - Los filtros de correo son unas herramientas que nos permiten crear respuestas automáticas, redirecciones, etc. Pero estas funciones también las aprovechan los hackers, por ejemplo para entrar en conversaciones ajenas o recibir correos que van dirigidas a otras cuentas.
    - Es importante que entremos en la configuración de estos filtros (nosotros o nuestro responsable informático) y revisemos de forma periódica que no hay ningún filtro nocivo o ajeno a nosotros.
    - Esta revisión, al igual que el cambio de contraseñas, también debe ser un protocolo periódico. En caso de no poder ser realizada por el usuario, lo habitual es que se realice por el responsable de sistemas de la empresa.

Pautas de prevención relacionadas con el uso de datos y archivos:

- Aspectos a tener en cuenta con datos en nuestro ordenador
    - Los datos almacenados en nuestro ordenador deben de estar incluidos en la copia de seguridad de nuestro sistema. De no ser así, o incluimos estos datos en la copia de seguridad, o guardamos estos datos directamente en el servidor o en otra carpeta que esté dentro del sistema de copias. Lo que no puede ocurrir es que nuestra empresa trabaje con un servidor y guardemos los datos en nuestro equipo (que es ajeno a cualquier tipo de copia), porque en ese caso, en caso de cualquier problema informático, podríamos perder toda la información del equipo.
    - Las datos de empresa que hay en nuestro equipo y los que tenemos acceso desde el mismo (a carpetas de la red), son datos muy importantes y los debemos tratar con el máximo cuidado. Debemos estar atentos al trabajar con archivos porque una mala acción puede provocar la perdida de información, con la perdida de tiempo y dinero que ello supone. Por lo tanto, máxima atención.

- Aspectos a tener en cuenta con datos en un servidor
    - Simplificando conceptos, podríamos definir que un servidor no es más que un ordenador potente que nos permite unificar la ubicación de archivos, carpetas y permisos para trabajar en equipo. Es muy importante organizar bien los datos cuando estamos trabajando con entornos de servidor, para no duplicar informaciones, no perder archivos, no eliminar datos por error, etc.
    - Cuando eliminamos un archivo de un ordenador, este pasa automáticamente a la “papelera”, pero cuando eliminamos un archivo del servidor desde un ordenador, este archivo se elimina directamente sin pasar por la papelera. Por eso hay que estar atento y trabajar con el máximo cuidado. Si ocurre esto, por cierto, aun podemos recuperar el archivo desde el servidor o a través de la copia de seguridad, pero tenemos más posibilidad de perdida de datos.
    - Debemos asegurarnos periódicamente que todos los datos que hay en el servidor (archivos, documentos, programas, bases de datos) se encuentran correctamente almacenados y actualizados en nuestras copias de seguridad.
    - El acceso a los datos por parte de un usuario a un servidor debe de estar limitado en función de las necesidades de cada trabajador. No tiene sentido, por ejemplo, que un técnico acceda a las carpetas

de administración, o que un comercial acceda a las carpetas de dirección. Estos fallos de seguridad deben de ser informados porque puede provocar grandes problemas a nivel interno de la empresa. Pero no solo eso, porque si entra un virus en nuestro ordenador, podemos encriptar los archivos a los que tenemos acceso del servidor, por eso es importante tener acceso limitado solo a aquellos ficheros con los que realmente trabajamos, para minimizar riesgos al máximo. Avisaremos por lo tanto al responsable del sistema y le indicaremos dicho fallo de seguridad.

- Aspectos a tener en cuenta con datos en la nube
    - El almacenamiento de datos en la nube es tendencia en los últimos años y son las bases del trabajo del futuro. Pero todavía es pronto para confiar plenamente en la nube, hay que ir con precaución.
    - No por tener los datos en la nube estamos exentos de virus o de perdida de datos. Además, en caso de errores de Internet nos podemos ver sin acceso a los mismos, con todos los problemas que ello supone. Por lo tanto es importante prevenir estas situaciones también.
    - Debemos tener copia de seguridad "en local", para evitar perdidas de datos en el propio proveedor que ofrece el servicio, así como poder trabajar en momentos puntuales en los que haya perdida de conexión a Internet.
    - Debemos conocer que sistema de datos en la nube tenemos contratado. No es lo mismo un servicio plano de almacenamiento, donde podemos tener un virus y que este se propague a la nube y perderlo todo; a tener un sistema de datos con copias de seguridad automáticas y distintas versiones, que nos permita restablecer directamente los datos en caso de propagación de virus.

Pautas de prevención relacionadas con el pago y cobro de facturas:

- Aspectos a tener en cuenta al realizar el pago de una factura de proveedor
    - Si vamos a realizar el pago de una factura a un proveedor nuestro debemos asegurarnos al 100% de que la cuenta donde se va a realizar el ingreso es la correcta. En cuentas que ya hemos utilizado en anteriores ocasiones ya tenemos la certeza de que esto ocurre, pero en cuantas nuevas o cuentas que modifican los clientes, hay que asegurarse personalmente de que este cambio es correcto.

- Aspectos a tener en cuenta al esperar un cobro por parte de un cliente
    - Lo mismo ocurre para aquellos cobros que estamos esperando de clientes. Debemos avisar que nuestra empresa no cambiará nunca el numero de cuenta donde se deben realizar los ingresos. Y que en el caso de que exista algún cambio, lo notificará personalmente para que no haya ninguna duda.

- Otros aspectos a tener en cuenta
    - En cualquier transacción debemos asegurar que los números de cuenta son correctos, porque si realizamos transferencias a cuentas erróneas que están controladas por hackers, el dinero desaparece rápidamente y es muy difícil recuperarlo. Esto puede crear un problemas entre nosotros y el cliente/proveedor, y por este motivo ajeno a todos, crear un problema en la relación comercial entre ambos. Hay que ir con extremo cuidado en estos casos.

Pautas de prevención relacionadas con los programas del equipo:

- Ejecución de programa antivirus
  - Todos los ordenadores deben de tener el antivirus correctamente instalado y configurado
  - Los antivirus analizan de forma continua toda la actividad del equipo, pero es importante que de forma periódica se realice un análisis completo de todos los equipos. Este análisis debe obtener los resultados esperados (equipo limpio y sin problemas). De no ser así, se deben revisar los resultados y ante la duda indicarlo al responsable o asesor informático.

- Ejecución de programas antimalware
  - En algunas ocasiones, no es obligatorio pero si muy recomendable, los ordenadores deben de tener un programa antimalware que complemente al antivirus y ayude a resolver los problemas y restos de virus que este no pueda limpiar.
  - Estos programas (habitualmente son gratuitos, como por ejemplo el programa Malwarebytes) permiten encontrar restos de virus que los propios antivirus consideran como "buenos". Des esta manera atacamos las amenazas desde dos puntos de vista y por lo tanto mejoramos la seguridad de nuestro sistema.

- Actualizaciones de programas
  - Las actualizaciones de Windows y de los programas que usamos en nuestro día a día son muy importantes. En gran medida, las actualizaciones se centran en cubrir falos de seguridad, que a priori parecen poco importantes, pero que realmente son los "agujeros" que utilizan los virus para acceder a nuestros sistemas.
  - En la medida de lo posible nuestros equipos deben de estar perfectamente actualizados.

- Revisión de sistemas de copias de seguridad
  - Las copias de seguridad son de vital importancia para cualquier empresa y usuario de hoy en día
  - Las copias de seguridad deben estar bien configuradas y se deben supervisar periódicamente para comprobar que se ejecutan según el plan previsto, que contienen todos los archivos correctos, etc.
  - Dada su importancia, hemos dedicado un punto específico a las copias de seguridad al final de este manual, con todos los aspectos a tener en cuenta, para su correcta realización y supervisión.

5 MANUAL DE SEGURIDAD INFORMÁTICA – OCTUBRE 2022

INTEGRIDAD Y SEGURIDAD DE LOS DATOS

Los datos de una empresa o de un usuario particular son su bien más preciado. En los datos de una organización encontramos años y años de esfuerzo que se deben de proteger de forma correcta para evitar cualquier perdida o cualquier aspecto que pueda comprometer la integridad de los mismos.

- **Acciones que pueden afectar a los datos de una empresa**
  - Perdida de datos por fallo del sistema (hardware o software)
    - Se pierde acceso a la información por fallo de disco duro, fallo del PC, siniestro, catástrofe, etc.
  - Perdida de datos por un virus (encriptación)
    - Entra un virus en el sistema y encripta todos nuestros archivos
  - Robo de datos o acceso a datos confidenciales por una persona no autorizada
    - Una persona externa a la empresa accede y roba datos
    - Un trabajador borra o modifica datos por error
    - Un trabajador extrae datos de forma ilícita o incluso borra documentos de la empresa de forma malintencionada
- **Como evitamos esta pérdida de datos**
  - Copias de seguridad
    - Una vez mas, vemos que las copias de seguridad son la principal arma contra un desastre informático en la que tenemos perdida de datos (por cualquier motivo)
    - Tenemos que tener un sistema de copias de seguridad bueno, eficiente e infalible.
  - Permisos de Usuario
    - No vale café para todos. Cada usuario debe de acceder única y exclusivamente a la información que necesite para desempeñar sus funciones dentro de la empresa
    - Hay que revisar los permisos de acceso que tiene cada usuario a la información de la empresa
  - Acceso a los datos
    - Los usuarios deben de tener acceso a los datos, pero no deben poder extraer dicha información de la empresa. En este sentido se pueden establecer protocolos para no conectar dispositivos de almacenamiento externo por parte de los trabajadores, no conectar cuentas de correo electrónico personales, no instalar programas de archivos en la nube, etc.
  - Protocolos de seguridad
    - Debemos establecer unos protocolos de seguridad que deben cumplir todos los trabajadores de la empresa. En este manual se citan muchos de ellos, pero deben de adaptarse a cada tipo de negocio, a cada tipo específico de tarea dentro de la empresa, etc.
    - Debemos proteger a la empresa no solo de virus y acciones internas, sino también de posibles errores intencionados o no de los trabajadores de la misma.

En el caso de que la perdida de datos se haya producido, necesitamos saber los mecanismos que tenemos para la recuperación de esos datos. En el punto siguiente se aborda dicha actuación.

5 MANUAL DE SEGURIDAD INFORMÁTICA – OCTUBRE 2022

RECUPERACIÓN DE ARCHIVOS

Que ocurre si no hemos tomado ninguna medida y hemos perdido nuestros datos? Que podemos hacer si aun tomando todas las medidas antes mencionadas ocurre una catástrofe no prevista y perdemos nuestra información? Existen algunas posibilidades de recuperar los datos aún cuando todo parece perdido, y es lo que vamos a comentar a continuación con varios ejemplos y casos reales que han documentado nuestros técnicos.

Recuperación de archivos ante eliminación (malintencionada o no) de los archivos de un disco duro:

- Puede ocurrir que por error nuestro, o por el acto malintencionado de otro usuario, se eliminen del ordenador o de nuestro sistema de archivos unos datos muy importantes para nosotros.
- En estos casos es fundamental determinar las causas reales de la perdida de datos, no tanto para exigir responsabilidades, sino simplemente para evitar la misma situación en el futuro.
- A nivel de recuperación de estos datos existen varias posibilidades:
    - Acceder a las versiones anteriores de la carpeta raíz donde estaban esos datos
    - Utilizar un programa de recuperación de archivos eliminados del disco duro
    - Y por supuesto, y la más recomendable de todas, acceder a la ultima copia de seguridad de esos datos. Puede darse la posibilidad que realizando las dos recuperaciones anteriormente citadas tengamos los datos más recientes que de la propia copia de seguridad; porque podríamos recuperar los datos exactos mientas que en la copia pueden ser del día anterior. Si esto sucede daremos prioridad a las dos primeras opciones, pero es importante indicar que las dos primeras opciones pueden fallar (porque son automáticas y aleatorias y no tenemos control sobre ellas), mientras que nuestro sistema de copias debe de ser estable y totalmente fiable.

Recuperación de archivos ante fallo electrónico o físico del disco duro del ordenador/servidor/memoria USB:

- Puede ocurrir que por error físico del ordenador o del propio disco duro perdamos todo acceso a la información contenida en el mismo.
- A nivel de recuperación de estos datos existen varias posibilidades:
    - En los casos menos severos, las tiendas de informática tienen los mecanismos suficientes para recuperar la información (mediante programas de recuperación, accediendo al disco duro a través de otro PC, etc.). En este caso concreto, los costes de recuperación son bastante aceptables, en torno a los 50-100€.
    - En los casos en los que el dispositivo ha sufrido daños mas fuertes, las empresas de informática en general no disponen de los mecanismos necesarios para recuperar los datos discos parcial o totalmente dañados físicamente, y tienen que recurrir a empresas especializadas que disponen de la tecnología adecuada para recuperar esta información. En este caso, los costes de recuperación son bastante elevados, porque son empresas especializadas que tienen cámaras de vacío para recuperar la información interna del disco duro. El precio de recuperación está en torno a los 500-700€. Bien es cierto que este tipo de recuperaciones solo se paga el importe si se consiguen recuperar los datos.

Recuperación de archivos ante encriptación de datos por virus encriptador:

- Los virus encriptadores cifran la información de las empresas y los usuarios y ofrecen la posibilidad a los afectados de "recuperar" dicha información a través del pago de una cantidad de dinero, normalmente en bitcoins o monedas similares.
- Por nuestra experiencia, el pago de estas cantidades que pueden rondar entre los 300€ y los 500€ no garantizan en ningún caso la recuperación de los archivos dañados. Por lo que se recomienda NO PAGAR estas cantidades bajo ningún concepto.
- Si nuestro equipo de empresa o nuestro ordenador personal ha sufrido un ataque de virus encriptador, debemos contactar inmediatamente con nuestro asesor informático para que nos indique como proceder. Pero como es un problema que requiere atención inmediata para reducir al máximo la expansión del virus, indicamos a continuación las acciones que debemos realizar:
    - Lo primero es detectar cuando estamos siendo atacados por un virus. Los síntomas propios de un virus que nos tienen que alertar y poner en guardia son estos:
        - Lentitud extrema en todos los procesos del equipo
        - No podemos abrir archivos o programas que normalmente son accesibles
        - Vemos los nombres de los archivos con coletillas o extensiones del raras o extrañas
    - En el momento que pensemos que estamos siendo atacados, o incluso aunque ya hayamos sufrido el ataque hay que hacer los siguientes procesos de forma inmediata:
        - Desconectar el ordenador de la red (quitar el cable de red)
        - Apagar el ordenador de forma inmediata
        - Avisar a nuestro responsable o asesor del sistema informático de la empresa
        - En caso de redes pequeñas, y si estamos seguros de que hay un posible virus encriptador, por ejemplo si vemos archivos encriptados con extensiones ratas, debemos apagar todos los equipos de la red y el propio servidor. Y de nuevo, avisar al responsable del sistema para que reinicie de forma controlado todo el sistema.

- A continuación indicamos las opciones de recuperación que podemos tener cuando somos atacados por un virus encriptador:
    - En el mejor de los casos, podremos recuperar los archivos desde el propio ordenador, a través de las copias de versiones anteriores que se generan automáticamente en nuestros sistemas
    - En otros casos, y esta es la opción más recomendada, se trata de acceder a nuestra copia de seguridad y recuperar los datos antes de su encriptación. Aunque la experiencia nos dice que no siempre nos encontramos con los datos actualizados al acceder a las copias, por eso es tan importante revisar nuestro sistema de seguridad de forma periódica.
    - En el peor de los casos, no tendremos acceso a una copia de seguridad ni a versiones anteriores de archivos y nos encontraremos que todos nuestros datos se han encriptado definitivamente. En estos casos, existen empresas especializadas (a las que se puede contactar a través de su tienda de informática habitual) que ya disponen de algoritmos de recuperación de muchos de los virus encriptadores actuales. Y en el caso de que no se haya podido recuperar, debemos almacenar los datos encriptados a la espera de que en los próximos meses, y una vez descubierto la clave de recuperación, ya los podamos recuperar.

5 MANUAL DE SEGURIDAD INFORMÁTICA – OCTUBRE 2022

ÉTICA PROFESIONAL Y PERSONAL

En este apartado queremos enumerar una serie de conductas que deberían seguir los trabajadores de cualquier empresa en beneficio del correcto funcionamiento del sistema informático de la misma. Evidentemente, este punto está mayoritariamente dedicado a los trabajadores de las empresas, pero también es perfectamente aplicable a nivel de usuarios particulares.

Es importante indicar en este punto que, en ningún caso se pretende establecer por parte de los técnicos de Apunts Informática un enfoque negativo en cuanto a las prácticas de los trabajadores en las empresas, ni mucho menos es nuestra intención. Entre otras cosas, porque confiamos plenamente en nuestros trabajadores y entendemos que en las empresas esta confianza mutua, entre el trabajador y la empresa, es fundamental para el correcto desempeño de cualquier trabajo. No obstante, nuestra experiencia nos indica que muchos de los problemas que encontramos en las empresas a nivel informático, como puede ser la entrada de virus, las suplantaciones de identidad, la perdida de datos, etc. se podrían haber evitado si el usuario hubiese sido conocedor de estas pautas de comportamiento (tanto pautas a seguir, como pautas a evitar).

Por este motivo, desarrollamos una serie de puntos que consideramos fundamentales para que los trabajadores tengan una idea clara de la gran importancia y responsabilidad que tienen en su trabajo. La intención es que pueda estar plenamente centrado en su trabajo y les ayude a ser conscientes del papel fundamental que tienen en el correcto funcionamiento de los sistemas informáticos en las empresas actuales.

Aspectos a tener en cuenta para el correcto uso de los equipos informáticos y las nuevas tecnologías por parte de los trabajadores en las empresas actuales:

- **Pautas a seguir (acciones recomendadas)**
  - Uso correcto de la información y los datos de la empresa
    - Los datos se deben guardar de forma ordenada y clara dentro de las carpetas correspondientes, ya que son las que tienen copias de seguridad configuradas.
    - La información de la empresa es confidencial y propia de la empresa, debe respetarse este principio en todo momento y manejar la información con mucho cuidado.
    - La información de los clientes/proveedores que se trata en la empresa, incluso la información propia de los servicios que realiza la empresa, debe ser confidencial y en la medida de lo posible no se debe acceder a revisar dicha información (solo en casos estrictamente necesarios)
  - Uso correcto del correo electrónico de la empresa
    - El correo electrónico de la empresa se debe usar solo para fines de la propia empresa
    - Ante cualquier duda de posible virus o fallos de comunicación que pueda suponer la posibilidad de un problema de suplantación de identidad, hay que avisar a los responsables del sistema
    - No debemos abrir los correos (ni enlaces, ni ficheros adjuntos) de aquellos remitentes que no conozcamos. Hay que ir con especial cuidado en este punto, porque es la entrada principal de todo tipo de virus hoy en día.
  - Protocolos de actuación ante transferencias comerciales
    - Los encargados de realizar transferencias comerciales dentro de las empresas deben extremar sus precauciones. No pueden consentir un numero de cambio de cuenta bancaria sin realizar la

confirmación personal con la otra empresa. Esta comunicación debe ser verbal porque cada la posibilidad de que el correo este interceptado y estemos hablando con otra persona.

- Detección temprana de posibles problemas o amenazas
  - Los usuarios son los primeros que pueden detectar un malfuncionamiento de su equipo, del sistema, del correo, etc. Ante la percepción de cualquier situación anómala deben avisar al responsable de su sistema informático para que revisen un posible problema.
- Ejecución de antivirus y antimalware recomendado por la empresa
  - Los equipos informáticos deben tener un antivirus y otros programas de protección (como antimalwares). Con el permiso del responsable del sistema informático, deben encargarse de revisar estos programas e incluso de realizar análisis semanales de sus equipos.

- **Pautas a evitar (acciones no recomendadas dentro del horario laboral)**
  - Uso incorrecto de los datos de la empresa
    - No podemos usar los datos de la empresa para fines personales en ningún caso
  - Acceso a datos confidenciales
    - Solo debemos acceder a los datos estrictamente necesarios para desarrollar las funciones que tenemos encomendadas en nuestro trabajo
    - Si detectamos que podemos acceder a documentos de otro departamento debemos comunicarlo al responsable del sistema. El hecho de que podamos acceder nos puede inculpar en futuros errores de seguridad internos.
  - Acceso remoto
    - Son muchos los programas que permiten hoy en día acceder de forma fácil y rápida a los equipos de la empresa de forma remota. Estos programas solo de sebe usar de forma controlada y con la autorización expresa del responsable de la empresa.
    - En ningún caso se deben usar para transferir información de la empresa al exterior de la misma
  - Extracción de datos de la empresa
    - En ningún caso podemos extraer datos de la empresa sin la correspondiente autorización
    - Estos datos son propiedad de la empresa y estaremos incurriendo en un delito informático
  - Entrada de datos a la empresa
    - En ningún caso podemos introducir datos de la empresa sin la correspondiente autorización
    - Junto con los datos podemos inyectar virus en el sistema informático y crear un gran problema
  - Uso incorrecto del correo electrónico
    - En el correo de la empresa no debemos acceder a todo lo que nos envían, tenemos que ser muy rigurosos en aquellos correos que abrimos y realizar un análisis previo del remitente, de la conveniencia o no de abrir un archivo adjunto, etc.
    - No podemos abrir nuestro correo personal porque podemos descargar virus en el equipo de la empresa.
  - Acceso a páginas web potencialmente peligrosas
    - En los equipos de la empresa no debemos acceder a páginas que no sean las estrictamente necesarias para el desempeño de nuestro trabajo. A parte de la evidente perdida de tiempo que esto supone, puedo ocurrir que se descarguen de forma automática virus y otros programas nocivos para el equipo y el sistema informático de la empresa.
  - Descargar archivos potencialmente peligrosos
    - Terminantemente prohibido descargar programas ajenos al desempeño de nuestro trabajo en la empresa. La descarga de archivos es otra entrada habitual de virus informáticos.
  - Uso de las redes sociales y de teléfonos personales

- El uso de redes sociales personales desde la propia empresa implica perdidas de tiempo en horario laboral y por lo tanto un descenso de la productividad y del nivel de atención del usuario en su trabajo.
- El uso del teléfono móvil personal tampoco es recomendable en horario laboral. Además de la perdida de tiempo, se minimiza la atención en tareas sensibles y se pueden generar problemas.
- Ambas prácticas producen una importante perdida de atención en lo que se está haciendo. Tal y como hemos incidido en este manual, es fundamental centrarse en el trabajo para evitar muchos de los problemas informáticos anteriormente citados.
- En ambos casos, el uso de aplicaciones no lícitas en los dispositivos y cuentas personales de los propios usuarios, junto con la localización del teléfono o de la propia conexión a Internet (que los proveedores identifican mediante la IP pública asociada a la empresa) pueden ocasionar problemas jurídicos y de grandes repercusiones para las organizaciones.

- Instalación de programas informáticos
  - El uso y sobretodo la instalación de los programas informáticos dentro de las empresas deben hacerse siempre con la autorización del responsable del sistema informático de la misma.
  - En ningún caso un usuario instalará una aplicación sin autorización dentro del sistema.

5 MANUAL DE SEGURIDAD INFORMÁTICA – OCTUBRE 2022

COPIAS DE SEGURIDAD

Esta demostrado que la mejor solución ante cualquier catástrofe o problema informático (de cualquier índole) es una buena gestión de las copias de seguridad. Para una empresa, disponer un sistema de copias de seguridad estable y eficiente es fundamental. Debemos revisar todas las posibles casuísticas que puedan ocasionar pérdida de datos y disponer de un sistema de copias de seguridad que permita recuperar los datos más importantes de la empresa ante cualquier situación comprometida.

Para el sistema de copias de seguridad es fundamental tener un buen programa que gestione correctamente la automatización y supervise el correcto funcionamiento de las copias. A continuación indicamos los programas de copia más utilizados junto a su característica principal:

- Cobian bakcup: para la copia simple de datos (opción gratuita)
- Goodsync: para la copia profesional de datos y archivos (optimiza procesos incrementales)
- Acronis: para la copia profesional de imágenes completas de ordenadores, servidores, etc.

Una vez bien definido el programa de copias de seguridad, nos centramos en los dispositivos donde se tiene que almacenar la información. A continuación les indicamos los dispositivos más habituales en función del tipo de copias de seguridad, pasando de sistemas simples hasta llegar a sistemas profesionales más complejos:

- **Copias de seguridad a discos duros externos USB**
  - La copia de seguridad a discos externos USB es simple pero muy efectiva (si se hace bien)
  - Necesitamos un mínimo de dos discos externos USB que se van alternando días pares e impares
  - Es muy importante no dejar los dos discos conectados (porque si entra un virus, este se puede propagar al disco), e ir intercambiando los discos todos los días. Si además, el disco que no está conectado lo dejamos fuera de la oficina, tenemos un sistema muy completo a coste muy pequeño.
  - Tienen toda la explicación concreta de este tipo de copias en el ANEXO 5 de este manual

- **Copias de seguridad a discos duro externo NAS (disco de RED)**
  - Un disco de red o disco NAS son unidades de almacenamiento de alta capacidad y con discos redundantes que son accesibles a través de la red.
  - Es una copia más profesional porque permite más seguridad, sobretodo por el hecho de que los virus no se propagan al disco NAS en el momento de la infección (si se hace bien). Además permite disponer de más versiones de copias de seguridad de más días, por lo que se permite mas posibilidades de recuperación (en el caso de que nos demos cuenta de la eliminación de un archivo varios días después del siniestro, por ejemplo).
  - Necesitamos un disco duro de red NAS con capacidad suficiente para almacenar un mínimo de cinco días de copias de seguridad. El sistema copia de forma completa todos los archivos en una carpeta llamada “lunes”, “martes”, etc. y al siguiente lunes ya se sobrescribe. De esta manera tenemos una semana completa de copias de seguridad.
  - Tienen toda la explicación concreta de este tipo de copias en el ANEXO 1 de este manual

- **Copias de seguridad a discos duros externos NAS (INTERNO Y EXTERNO)**
    - En este caso necesitamos dos discos NAS. Uno situado en la propia empresa y otro situado en una ubicación fuera de la empresa (cualquier punto con conexión a Internet es válido).
    - Es un sistema muy profesional que permite tener el control de las copias de seguridad de la empresa cubriendo todas las casuísticas de recuperación ante posibles fallos del sistema, incluso en casos de catástrofes graves como robos o incendios, tendremos una copia actualizada fuera de la empresa.
    - Es el mismo sistema explicado anteriormente en el disco NAS (copias de seguridad de cada día de la semana que se sobrescriben semanalmente para aprovechar espacio), con la mejora de que todos los días se realiza una copia de seguridad externa en el otro disco NAS situado en otra ubicación de la empresa (incluso en casa del responsable de la misma).
    - Tienen toda la explicación concreta de este tipo de copias en el ANEXO 2 de este manual.

- **Copias de seguridad a sistemas CLOUD (en la NUBE)**
    - Cada vez las empresas opta más por realizar copias de seguridad en la nube. Este tipo de copias es perfectamente válido, pero es preferible reforzarlo con alguno de los sistemas de copia de seguridad en local visto anteriormente (porque permiten recuperaciones más rápidas).
    - Hay que tener en cuenta que todos los sistema de archivos en la nube no funcionan igual y no sirven para lo mismo. Los sistemas de archivos gratuitos normalmente no disponen de versiones (copias de seguridad en días anteriores) lo que limita la utilidad de la copia porque si un virus entra en la nube puede comprometer nuestros datos. Hay que tener en cuenta estas consideraciones a la hora de optar por un sistema de copias de seguridad en la nube.
    - Tienen toda la explicación concreta de este tipo de copias en el ANEXO 3 y 4 de este manual.

A nivel de empresa, y considerando la importancia de un buen sistema de copias de seguridad, vemos que los sistemas de copias de seguridad son redundantes y pueden utilizarse una o varios de los mecanismos indicados anteriormente. Y es que es de vital importancia para una empresa tener sus sistemas de archivos totalmente a salvo ante cualquier situación o problema informático.

Para usuarios particulares las copias de seguridad recomendadas no son tan sofisticadas, aunque en muchos casos la información que se maneja es igual de importante que en las empresas, sobretodo a nivel emocional. Aunque cualquiera de las soluciones anteriores es totalmente válida, en cualquier caso una copia de seguridad no es más que el almacenamiento a buen recaudo de una copia de los datos más importantes del usuario, por lo que solución perfectamente válidas y recomendable podrían ser estas opciones:

- Copias de seguridad en almacenamiento externo
    - Simplemente debemos copiar los datos importantes de nuestros equipos en uno o varios dispositivos externos (memorias USB externas, discos duros externos, etc.)
- Copias de seguridad en la nube
    - Existen planes de archivos de datos muy económicos o directamente gratuitos que nos permiten tener una copia de seguridad de todos nuestros archivos en la nube.

Lo importante, en cualquier caso, es que los usuarios sean conscientes de la importancia de tener almacenados sus datos en varios lugares diferentes, sea cual sea su escenario o situación concreta. Porque los datos están sujetos a la acción de virus y hackers informáticos y por lo tanto esa información puede peligrar. Y además la información se almacena en dispositivos electrónicos que por supuesto, también pueden fallar en cualquier momento.

REVISIÓN DE LAS COPIAS DE SEGURIDAD

Es muy importante indicar que los datos dentro de una empresa (o a nivel particular) son un ente vivo. Dicho de otra manera, los sistema de copias de seguridad tienen vida propia. En todos los sistemas de información actuales, los datos que forman parte de los mismos y por lo tanto, los datos que queremos guardar en nuestra copia de seguridad; van creciendo a lo largo del tiempo, se van añadiendo nuevos datos que antes no considerábamos importantes y ahora si, etc. Por este motivo, y aunque pensemos que tenemos el mejor sistema de copias de seguridad posible, es muy importante no dejar olvidado nuestro sistema de copias de seguridad e ir revisándolo todas las semanas.

Aspectos a tener en cuenta en la creación y posterior revisión de los sistemas de seguridad:

- Revisar que el proceso de copia de seguridad configurado inicialmente se hace correctamente
- Revisar que los nuevos datos que estamos almacenando en nuestro sistema se propagan a nuestra copia de seguridad mediante la comprobación aleatoria de recuperación de datos
- Revisar que los programas se están almacenando correctamente, ya que en muchas ocasiones, sobretodo en programas de gestión, se debe realizar una copia previa de la base de datos de los archivos (por ejemplo de la base de datos SQL) y no es suficiente con almacenar la carpeta o directorio principal del programa.
- Revisar que el tamaño de las copias de seguridad es suficiente para guardar varios días de copias de seguridad (no solo debemos tener una copia, porque si no estamos atentos y entra un virus, si no tenemos un margen de respuesta, cuando vayamos a ver la copia de seguridad nos podemos encontrar que se haya propagado el virus a la misma).