

Entorno Informático, Sistemas y Seguridad en la UPV

El Entorno Informático para el trabajo

Concepto de Entorno Informático para el Trabajo

El Entorno Informático para el Trabajo se define como el **conjunto completo de recursos, tanto físicos como lógicos, necesarios para que un usuario pueda realizar sus tareas de manera digital** en una organización. En esencia, es la combinación de la máquina y el programa que permite procesar la información.

Su principal objetivo es permitir la gestión, procesamiento y comunicación de datos para el cumplimiento de los objetivos laborales.

Componentes Esenciales

El entorno informático se divide fundamentalmente en dos grandes categorías, inseparables para su funcionamiento:

- **Hardware** (Componente Físico): hace referencia a todos los **elementos** tangibles o **físicos** que se pueden ver y tocar. Son la estructura y la base material del entorno. Es la máquina y se compone de Unidad Central (CPU, Memoria, Disco duro) y Periféricos (Monitor, Teclado, Impresora, web cam, micrófono). Procesa datos, almacena información y permite la interacción física con el usuario.
- **Software** (Componente Lógico): hace referencia a todos los **elementos** intangibles o **lógicos**. Son las instrucciones, reglas y programas que le dicen al hardware cómo funcionar y qué tareas ejecutar. Es un código binario que da instrucciones al hardware de cómo actuar. Se compone de Software de Sistema, o Sistema Operativo y Software de Aplicación que bien puede ser genérico como Word, Excel o Outlook, o específico como las aplicaciones UPV, Hominis, Serpis, Vinalopó, Xuquer, etc. Permite al usuario interactuar con la máquina y llevar a cabo tareas específicas.

UPVNET

Dentro del entorno de trabajo es necesario hablar también de la red informática. En el caso de la Universitat Politècnica de València se trata de UPVNET. A través de ella es posible acceder a impresoras, servidores, discos duros, o escritorio remoto a otros equipos.

Más adelante, en el tema, profundizaremos en el entorno de red de la UPV

Dispositivos (Hardware)

Dentro del entorno de la informática y la ofimática, un dispositivo se entiende como cualquier componente físico (hardware) que se conecta o forma parte de un sistema informático y que tiene una función específica para procesar, introducir, almacenar o mostrar información.

Es un término amplio que abarca tanto a la Unidad Central como a cualquier Periférico.

La Unidad Central y Periféricos

La Unidad Central

La Unidad Central (o Unidad del Sistema) es el corazón físico del ordenador. Se refiere a la caja o chasis principal que alberga los componentes electrónicos fundamentales responsables de realizar el procesamiento, la memoria y el almacenamiento de todos los datos y programas.

Los componentes fundamentales de la Unidad Central son estos elementos:

- La Unidad Central de Procesamiento (CPU) o simplemente **procesador**, su función clave es la **ejecución de las instrucciones** de todos los programas (el software), y la realización de los cálculos necesarios y controlar el funcionamiento de todos los demás componentes del sistema. La CPU es el "cerebro" del ordenador.

Las tres fabricantes y diseños principales son los Intel, los AMD y los Apple ARM. Además, Intel y AMD enumeran los modelos que saca al mercado según su potencia, según la siguiente tabla

Gama	Intel Core	AMD Ryzen	Uso Típico
Básica / Acceso	Celeron, Pentium, Core i3	Ryzen 3	Tareas administrativas básicas, navegación, ofimática ligera.
Media / Estándar	Core i5	Ryzen 5	Estándar para el trabajo diario, multitarea (varios programas a la vez).
Alta / Profesional	Core i7, Core i9	Ryzen 7, Ryzen 9	Trabajos exigentes, procesamiento de grandes datos, diseño gráfico.

Y los tres fabricantes también enumeran la generación a la que pertenecen, siendo las últimas la generación 14 de Intel, la 9000 de AMD y la M4 de Apple ARM.

La velocidad de procesamiento (medida en GHz) determina la rapidez con la que el equipo puede realizar tareas y procesar información.

- La **Placa Base** (Motherboard) es la tarjeta de circuito impreso más grande y vital de la Unidad Central. Actúa como el sistema nervioso central o la columna vertebral del ordenador, ya que es el medio físico que **conecta, coordina y permite la comunicación eléctrica y lógica de todos los demás componentes** (CPU, memoria, almacenamiento, periféricos).

La Placa Base define la compatibilidad de hardware del equipo porque contiene las interfaces (enchufes y ranuras) necesarias para albergar los componentes esenciales:

- El Socket, zócalo o receptáculo físico situado en la placa base donde se inserta y conecta el procesador (CPU). El socket determina qué modelos y qué generaciones de procesadores son compatibles con esa placa base específica.
- Ranuras de Memoria (Memory Slots o DIMM), que son las ranuras alargadas donde se insertan los módulos de Memoria RAM. El número de ranuras (comúnmente dos o cuatro) y el tipo de tecnología (DDR4 o DDR5) limitan la cantidad máxima de memoria que el equipo puede utilizar.
- Ranuras de Expansión (PCI y PCIe), que son conectores largos que permiten añadir tarjetas de expansión para mejorar o agregar funcionalidades al sistema. Proporcionan una conexión de alta velocidad para componentes que requieren mucha transferencia de datos. Se utilizan principalmente para la tarjeta gráfica (en equipos que la necesitan) y

para conectar tarjetas de red avanzadas o unidades de almacenamiento SSD de alta velocidad.

- La **Memoria RAM** (Memoria Principal o Memoria Temporal) La RAM (Random Access Memory) es la "memoria de trabajo a corto plazo". **Guarda temporalmente todos los datos y programas** que el usuario y el sistema están utilizando en el momento actual.

Es una memoria volátil, y todos los datos almacenados en ella se pierden en cuanto se apaga o reinicia el equipo. Cuanta más RAM tenga un equipo, mejor podrá manejar la multitarea (tener varios programas abiertos como Word, el navegador y el correo electrónico) sin ralentizarse.

- El **Almacenamiento** (Disco Duro/SSD) son los elementos que archivan y conservan permanente la información. Su función es **guardar el Sistema Operativo, las aplicaciones y todos los archivos** del usuario (documentos, imágenes, etc.) de forma permanente.

Es una memoria no volátil. Los datos se conservan, aunque el equipo esté apagado.

Sus principales tipos son:

- HDD (Disco Duro Clásico): Más lento, basado en platos magnéticos que giran.
- SSD (Unidad de Estado Sólido): Más moderno, mucho más rápido y eficiente que el HDD, ya que utiliza chips de memoria flash, similar a una memoria USB grande.
- M.2, que no son solo un tipo de disco duro, sino un factor de forma (un formato físico) que se utiliza principalmente para las unidades de Almacenamiento de Estado Sólido (SSD). Son más modernos, más rápidos y más compactos.

Periféricos

Un periférico es **cualquier dispositivo de hardware que se conecta a la Unidad Central** de un ordenador o forma parte integral de ella, y cuya función es facilitar la comunicación con el usuario y con el mundo exterior.

En términos sencillos, actúan como puertas de entrada y salida de información, permitiendo al ordenador recibir datos (ej. un teclado), mostrar resultados (ej. un monitor) o almacenarlos.

Periféricos de Entrada

Los dispositivos de entrada son aquellos que se utilizan para introducir datos o comandos en el ordenador para que puedan ser procesados.

- Teclado: El dispositivo fundamental. Se utiliza para la introducción de texto y para ejecutar comandos a través de combinaciones de teclas.
- Ratón (Mouse): Permite la navegación y selección gráfica de elementos en la pantalla. Controla el puntero para interactuar con el software.
- Escáner: Convierte documentos físicos (imágenes o texto en papel) a un formato digital (ej. PDF o JPG) para su almacenamiento y gestión electrónica.
- Micrófono: Capta el sonido o la voz para convertirlos en datos digitales. Es esencial para videoconferencias, dictado de texto y asistentes virtuales.

- **Cámara Web:** Captura imágenes y video en tiempo real. Esencial para reuniones virtuales y vigilancia.
- **Lector de Códigos de Barras:** Dispositivo que lee e interpreta la información codificada en un código de barras (generalmente números de referencia o precios), introduciendo esos datos directamente en el sistema de inventario o gestión.
- **Lector de Tarjetas/Carnets Inteligentes (Smart Card Reader):** Se utiliza para leer la información incrustada en el chip de tarjetas como el DNI electrónico o carnets de identidad profesional. Es fundamental para la firma digital y la autenticación segura del usuario en sistemas corporativos (como podría ser en la UPV).
- **Pantalla Táctil:** Aunque también es un periférico de salida (muestra imágenes), funciona como dispositivo de entrada al permitir al usuario interactuar y seleccionar elementos directamente con el dedo.
- **Tableta Digitalizadora:** Permite al usuario dibujar o escribir a mano alzada con un lápiz óptico, convirtiendo esos trazos en datos digitales.

Periféricos de Salida

Los dispositivos de salida son aquellos que se utilizan para mostrar o entregar la información procesada por el ordenador al usuario, o para enviarla a un medio físico.

- **Monitor (Pantalla):** El dispositivo de salida esencial. Muestra de forma visual la interfaz de usuario, los programas abiertos y los resultados del procesamiento de datos (documentos, imágenes, etc.).
- **Impresora:** Convierte la información digital (documentos, informes, gráficos) en un formato físico (en papel). Es crucial para la documentación y archivo tradicional.
- **Plotter:** Una impresora de gran formato especializada, utilizada para imprimir planos, mapas o gráficos de ingeniería. Aunque no es de uso diario en la administración básica, es común en entornos técnicos universitarios como la UPV.
- **Altavoces / Auriculares:** Convierten la información digital de audio en sonido audible. Son necesarios para videollamadas, notificaciones y contenido multimedia.
- **Proyector:** Muestra la imagen generada por el ordenador sobre una superficie o pantalla grande. Fundamental para presentaciones, reuniones y docencia.

Periféricos de Entrada/Salida (Mixtos)

Estos dispositivos pueden tanto introducir información en el sistema como mostrarla o entregarla al usuario, a menudo utilizando un solo componente.

- **Pantalla Táctil:** Permite al usuario introducir datos o comandos directamente con el dedo o un lápiz (sustituyendo al ratón). Actúa como monitor, mostrando la información visual al usuario.
- **Dispositivo Multifunción (MFP):** Permite escanear documentos físicos (Entrada) y enviarlos al ordenador. Permite imprimir documentos digitales (Salida) en papel.

- **Módem / Router:** Recibe información y datos del Internet o de la red externa. Envía datos desde el ordenador a la red o a Internet.
- **Unidades de Almacenamiento:** Graban o escriben datos en el medio (Entrada de datos para guardar). Leen los datos guardados en el medio (Salida de datos para usar).
- **Casco de Realidad Virtual (VR):** Puede incorporar sensores que captan el movimiento de la cabeza o la voz (Entrada).

El Sistema Operativo (SO) Windows 11

Un Sistema Operativo (SO) es el **software base y esencial que actúa como intermediario entre el hardware del equipo y el usuario** (o las aplicaciones). Su función principal es administrar todos los recursos de la computadora (el procesador, la memoria, el disco duro, los periféricos) de manera eficiente, y al mismo tiempo, proporcionar una interfaz gráfica sencilla (como Windows) que permite al usuario interactuar, ejecutar programas y gestionar archivos sin necesidad de conocer los complejos lenguajes internos de la máquina. Sin un SO, el hardware simplemente no puede funcionar.

La importancia del SO se encuentra en que es la plataforma que hace posible el trabajo. El Sistema Operativo (como Windows 11) es el responsable de:

- **Garantizar la Multitarea:** Permite trabajar en el correo, tener Word abierto y acceder a la aplicación de gestión al mismo tiempo sin que el sistema colapse.
- **Organizar la Información:** Proporciona el Explorador de Archivos, la herramienta esencial para gestionar y encontrar documentos, informes y expedientes digitales.
- **Habilitar las Aplicaciones:** Es la base sobre la que se instalan y ejecutan todas las herramientas de ofimática (Office) y las aplicaciones específicas de la UPV (Portal del Empleado, gestión de alumnos, etc.).
- **Estabilidad y Seguridad:** El SO gestiona la seguridad básica, permitiendo la autenticación del usuario y siendo el primer punto de defensa contra malware.
- En definitiva, es el gerente de recursos del equipo que asegura que el hardware y el software trabajen en armonía para completar las tareas administrativas.

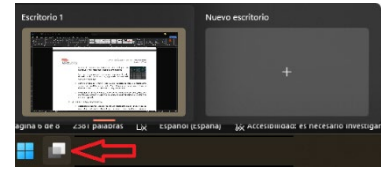
Aspectos Clave de Windows 11 para el Trabajo Administrativo

- **Productividad y Multitarea:** Windows 11 introduce herramientas específicas para optimizar el trabajo simultáneo (multitarea).
 - **Diseños y Grupos Acoplados:** Permite al usuario **organizar automáticamente varias ventanas abiertas** (ej. Word, Excel, navegador) en diseños predefinidos en la pantalla con un solo clic. Un Grupo Acoplado recuerda ese diseño para que puedas volver a él rápidamente desde la Barra de Tareas.



Los grupos acoplados se crean situando el cursor sobre el cuadro de maximizar de cualquier ventana y eligiendo la combinación de aplicaciones que desees.

- **Escritorios Virtuales:** Permiten crear **múltiples espacios de trabajo** completamente separados dentro del mismo ordenador. Puedes tener un Escritorio para el trabajo con documentos y otro para el correo y reuniones, sin mezclarlos.
- **Integración de Microsoft Teams:** La aplicación de Teams está integrada en la parte derecha de la barra de tareas, permitiéndote cambiar el estado de forma rápida y sencilla, o cerrar la aplicación.
- **Gestión de Archivos y Almacenamiento.**
 - **Explorador de Archivos (Diseño):** Presenta una interfaz simplificada y modernizada. La principal novedad para la gestión es la **introducción de pestañas** (similar a un navegador web), lo que permite trabajar con múltiples carpetas o drives de red en una sola ventana.
 - **OneDrive Integrado:** El almacenamiento en la nube de Microsoft está profundamente integrado. **Es la herramienta por defecto para guardar y sincronizar documentos** de forma segura, siendo esencial para el trabajo remoto.
- **Seguridad y Actualizaciones.**
 - **Windows Defender y Seguridad:** El sistema de seguridad (antivirus y firewall) integrado por defecto es Windows Defender. Aunque la UPV tiene su propio sistema; ESET end point, que estudiaremos más adelante.
 - **Windows Update:** El sistema de actualizaciones.
 - **Requisitos de Hardware (TPM 2.0):** Windows 11 requiere un chip de seguridad física llamado TPM 2.0. Esto asegura que los equipos que ejecutan Windows 11 cumplen con un estándar de seguridad moderno, algo relevante para la gestión de activos informáticos en la universidad.



Conexión en Red (Networking)

La conexión en **red** permite que el ordenador no sea un sistema aislado, sino que **se integre en una infraestructura que facilita la colaboración y el acceso a la información global**.

Red Informática en general

Una Red Informática es un **sistema de equipos** (ordenadores, servidores, impresoras) **que se encuentran interconectados**, ya sea por cable o de forma inalámbrica, con el objetivo principal de compartir recursos (archivos, impresoras) y facilitar la comunicación entre los usuarios.

UPVnet

UPVnet se refiere a la **Red de la Universitat Politècnica de València**. Es la infraestructura de comunicaciones que interconecta todos los equipos, servidores y servicios de los diferentes campus y departamentos de la UPV.

- Es la puerta de entrada a todos los servicios internos (Intranet). El acceso se realiza mediante la identidad corporativa (usuario y clave), garantizando que solo el personal autorizado acceda a datos sensibles.
- UPVnet proporciona servicios esenciales como el Correo Electrónico Personal y la conexión a las Carpetas Compartidas departamentales y servidores de la Universidad.
- La red interna de la UPV está conectada a la red global de Internet, pero esta conexión está gestionada y filtrada por el Servicio de Informática (ASIC) para asegurar la seguridad y limitar su uso a actividades relacionadas con el trabajo.
- UPVNET también permite el acceso a las aplicaciones corporativas de la Universidad. Es necesario estar conectado a la red para poder validar las credenciales de acceso.

Conceptos básicos: LAN, WLAN

LAN (Ethernet) es una red informática que conecta ordenadores y dispositivos dentro de un área geográfica limitada, como un edificio, una oficina o un campus. Su objetivo es el intercambio de datos y el uso compartido de recursos como impresoras o servidores de archivos.

Su conexión se realiza a través de los puntos de acceso a la red (rosetas), cables de red, que pueden transmitir desde 1 Gbps (Cat 5e o Cat 6), 10 Gbps (Cat 6a), o entre 10 y 40 Gbps (Cat7 y Cat 8), y conectores RJ45.

WLAN (Wi-Fi), es esencialmente una LAN que utiliza tecnología inalámbrica en lugar de cables para la conexión. Permite la movilidad dentro de un área geográfica limitada y es el método que utilizas para conectar tu portátil o móvil a internet dentro del campus.

La conexión Wi-Fi se realiza habitualmente a través de la propia UPVNET, o Eduroam (la red académica internacional), utilizando siempre las credenciales corporativas para la autenticación.

Internet

Internet es la red de redes mundial, pública y descentralizada, que utiliza la familia de protocolos TCP/IP para enlazar miles de millones de dispositivos y redes (como UPVnet) en todo el mundo. Su función principal es proporcionar acceso a una vasta cantidad de información, servicios y recursos (como correo electrónico, sitios web y servicios en la nube), permitiendo la comunicación global e instantánea.

Internet es el vehículo de comunicación global, mientras que las redes internas (como UPVnet) son la forma en que el usuario se conecta a ese vehículo.

Servicios de Internet

- World Wide Web (WWW): Es la colección de documentos y recursos enlazados (páginas web) a los que se accede mediante un navegador. Es el servicio que permite la consulta de información pública (webs oficiales, diarios, documentación, etc.).
- Correo Electrónico (E-mail): El servicio fundamental para la comunicación escrita asíncrona (no en tiempo real) entre personas o sistemas. Permite el envío de mensajes y archivos adjuntos de forma rápida y formal.

- **Transferencia de Archivos (FTP/SFTP):** Un protocolo utilizado para la transferencia de archivos grandes o el mantenimiento de sitios web. Permite a los usuarios autorizados (administradores o personal técnico) subir o descargar conjuntos de datos de forma segura entre equipos remotos.
- **Mensajería Instantánea:** Permite la comunicación de texto y voz/vídeo en tiempo real (síncrona). En el entorno UPV, esto se realiza principalmente a través de plataformas corporativas como Microsoft Teams.
- **Voz sobre IP (VoIP):** Tecnología que permite realizar llamadas de voz o videollamadas utilizando la conexión a Internet en lugar de la red telefónica tradicional. Es la base de las videoconferencias y las llamadas de Teams.
- **Computación en la Nube (Cloud Computing):** Se refiere al acceso a servicios, aplicaciones y almacenamiento (ej. Google Drive, OneDrive, software de gestión UPV) que no se encuentran en el disco duro local, sino en servidores remotos conectados a Internet.

Navegadores web principales

Los navegadores web son las aplicaciones de software que permiten a los usuarios acceder a la información de la World Wide Web.

Microsoft Edge Microsoft: El navegador por defecto en Windows 11. Ofrece una integración profunda con los servicios de Microsoft y herramientas de productividad (como la integración con Bing AI y colecciones de pestañas). Es a menudo el navegador corporativo recomendado.

Google Chrome Google: Es el navegador más utilizado a nivel mundial. Ofrece una gran velocidad, alta compatibilidad con todos los sitios web y una sincronización excelente si se usa una cuenta de Google (marcadores, contraseñas).

Mozilla Firefox Mozilla Foundation: Destaca por su fuerte enfoque en la privacidad y la seguridad. Es una opción popular para usuarios que buscan evitar el ecosistema de Google. Es código abierto.

Apple Safari: El navegador por defecto para todos los dispositivos Apple (Mac, iPhone, iPad). Es conocido por su alta eficiencia energética y su velocidad, ya que está optimizado para su propio hardware.

Motores de búsqueda

Un Motor de Búsqueda es una herramienta web diseñada para localizar y recuperar información alojada en otros sitios web. El usuario introduce una o varias palabras clave y el motor devuelve una lista de páginas (resultados) que son relevantes para esa consulta.

Ecosia: El Motor de Búsqueda Sostenible de la UPV

Ecosia es un motor de búsqueda que destina todos sus beneficios generados por la publicidad a proyectos de reforestación a nivel global.

A partir de junio de 2023, la UPV adoptó a Ecosia, estableciéndolo como el buscador predeterminado en los ordenadores del Personal Técnico, de Gestión, y de Administración y Servicios (PTGAS). La UPV fue la primera universidad en España en implementar este cambio.

La adopción de Ecosia responde al compromiso de la UPV con la Sostenibilidad (Plan SIRVE) y la meta de ser una universidad neutral en carbono, demostrando que acciones administrativas sencillas (como buscar en Internet) pueden tener un impacto positivo en el medio ambiente.¹

Ecosia se diferencia de otros grandes buscadores porque no vende datos personales a terceros, lo cual es una ventaja desde el punto de vista de la privacidad.

Otros Motores Relevantes

- Google: El motor más utilizado a nivel global, conocido por la calidad y rapidez de sus resultados.
- Microsoft Bing: Integrado en Windows y Microsoft Edge.
- **Buscadores Específicos de la UPV:** La universidad también cuenta con herramientas internas como poli[lupa] o Explora I+D+i UPV para realizar búsquedas específicas en sus propios sistemas y recursos documentales.

Aquí tienes un [vídeo de la UPV sobre Search Engines](#) que puede resultar muy interesante para entenderlos.

Navegación Segura

La navegación web en un entorno corporativo como la UPV requiere especial cuidado, ya que **cada interacción en línea** (abrir un correo, hacer clic en un enlace o descargar un archivo) **presenta un riesgo potencial** para los datos y sistemas de la Universidad.

Navegar de forma segura es la **responsabilidad fundamental de todo el personal**. Se trata de minimizar la exposición a amenazas externas, como el robo de credenciales, la infección por virus y el compromiso de la información institucional, garantizando la confidencialidad, integridad y disponibilidad de los sistemas.

Certificados Digitales (SSL/TLS)

Un Certificado Digital (SSL/TLS) es una credencial de seguridad que se instala en los servidores de sitios web, y permite cifrar (encriptar) la comunicación entre el navegador del usuario y el servidor web.

Cuando navegas en un sitio seguro (como la Intranet de la UPV o una web bancaria), el certificado garantiza que nadie más pueda leer los datos que se envían (ej. tu contraseña) si son interceptados. La presencia de un certificado válido se identifica en el navegador con:

- Un candado cerrado  en la barra de direcciones.
- La dirección web comenzando con https:// (la 's' significa seguro).

Si un sitio web corporativo o de gestión administrativa no muestra el candado, no debes introducir información sensible.

¹ El autor no comparte la opinión y la considera propaganda, pero entiende necesario que el opositor conozca la versión oficial.

Principales Amenazas en la Navegación

- **Phishing:** Es una técnica de suplantación de identidad. El atacante intenta obtener información confidencial (credenciales, datos bancarios) haciéndose pasar por una entidad de confianza (ej. la UPV, un banco o un servicio de TI).
Consecuencia: Robo de la identidad corporativa y acceso a sistemas internos.
Prevención: Nunca hagas clic en enlaces de correos sospechosos que pidan actualizar contraseñas o datos personales. Revisa siempre la dirección del remitente.
- **Malware:** Término genérico que engloba cualquier software malicioso (virus, spyware, ransomware). Se introduce en el sistema para dañar, obtener datos o tomar el control del equipo.
Consecuencia: Pérdida de datos, cifrado de archivos (ransomware) o caída del sistema.
Prevención: Evita descargar archivos de sitios web no verificados. Confía en el Windows Defender y en el antivirus corporativo de la UPV para el escaneo constante.
- **Spyware:** Tipo de malware que se instala sigilosamente para monitorizar y registrar la actividad del usuario (ej. las pulsaciones del teclado para capturar contraseñas).
Consecuencia: Robo de información de forma silenciosa.
Prevención: Mantén el sistema operativo y el navegador siempre actualizados, ya que los parches de seguridad corrigen las vulnerabilidades que el spyware explota.

Seguridad Informática

El Consejo de Gobierno de la UPV aprobó una política de seguridad informática el 6 de junio de 2024.

A continuación, se muestra un resumen de los aspectos más destacados, y el documento completo se adjunta al final del capítulo como ANEXO I.

Resumen de Medidas de Seguridad para el Personal Administrativo (UPV)

El objetivo del personal es garantizar la confidencialidad, integridad y disponibilidad de la información y los servicios, de acuerdo con el Esquema Nacional de Seguridad (ENS).

Obligaciones y Responsabilidades del Personal

- **Concienciación y Formación Continua:**
 - Asistir a sesiones de concienciación en seguridad y protección de datos, al menos una vez al año.
 - La formación es obligatoria antes de asumir una nueva responsabilidad en el uso o administración de sistemas.
- **Control de Acceso (Principio de Mínimo Privilegio):**
 - Acceder solo a los activos de información y servicios para los que se tenga autorización expresa.
 - El acceso está limitado por mecanismos de identificación, autenticación y autorización.
- **Gestión de Incidentes:**
 - Asegurar la trazabilidad (registro) de la actividad en el sistema.

- Participar en la investigación y resolución de incidentes de seguridad y notificar cualquier anomalía, compromiso o vulnerabilidad.
- Seguridad Física y de la Información:
 - Mantener el sistema de información durante todo su ciclo de vida y detener el acceso si se detectan deficiencias graves de seguridad.
 - Proteger la información transmitida a través de redes de comunicaciones (uso de mecanismos que garanticen su seguridad).
- Requisitos de Contratación (Terceras Partes):
 - Si se trabaja con terceros (proveedores de servicios o software), estos deben cumplir con la Política de Seguridad de la UPV y garantizar un nivel de concienciación en seguridad al mismo nivel que el establecido.
- Protección de Datos:
 - Aplicar medidas técnicas y organizativas para cumplir con la legislación de Protección de Datos y Privacidad (riesgos derivados del tratamiento de datos personales).

Antivirus y Cortafuegos

Estos dos elementos son las principales líneas de defensa a nivel de software de un equipo y de una red.

Antivirus (Protección contra Malware)

El Antivirus es un software diseñado para detectar, prevenir y eliminar malware (código malicioso como virus, troyanos, ransomware y spyware) que intenta dañar el sistema o robar información.

ESET Endpoint Security Es la solución de seguridad antivirus centralizada utilizada por la Universitat Politècnica de València para todos los equipos corporativos.

El personal **no tiene que realizar la configuración ni la gestión de licencias**. La configuración (incluyendo escaneos periódicos y actualizaciones de la base de datos de virus) **se gestiona automáticamente y en remoto** por el Servicio de Informática (ASIC).

El usuario **debe asegurarse de que el programa está activo y ejecutándose en segundo plano** (normalmente visible en la barra de tareas) y **nunca desactivarlo** para no comprometer la seguridad de la red.

Cortafuegos (Firewall)

El Cortafuegos es un sistema de seguridad (puede ser hardware o software) que actúa como una barrera de filtrado entre la red interna de la UPV (UPVnet) e Internet.

Función Principal: Controlar el tráfico de red decidiendo qué información puede entrar o salir del ordenador o de la red interna.

- Permite el tráfico seguro (ej. navegar por webs autorizadas o recibir correo de la UPV).
- Bloquea el tráfico potencialmente peligroso o no autorizado (ej. intentos de conexión de hackers o comunicaciones de malware).

En los equipos de la UPV también usan el de ESET junto con las reglas de red corporativas. El personal no debe modificar las reglas del firewall local, ya que estas están preconfiguradas para proteger el entorno institucional. Si una aplicación necesaria es bloqueada, debe reportarse al servicio del CAU (Centre d'Atenció a l'Usuari).

Contraseñas

Guía de uso de las contraseñas en la Universitat Politècnica de València.

Aprobada por el Comité de Seguridad de la Información de la UPV el 9 de enero de 2025

Ámbito de aplicación

Esta guía está dirigida a todos los usuarios de los servicios y recursos informáticos de la Universitat Politècnica de València. Desarrolla las directrices sobre contraseñas establecida en la Normativa de Seguridad de la UPV, que es de cumplimiento obligatorio para todos los miembros de la institución.

Índice

1. Cómo crear contraseñas robustas y memorizables
2. Uso adecuado de las contraseñas
3. Renovación periódica de las contraseñas
4. Importancia de las contraseñas
5. Gestores de contraseñas

1. Cómo crear contraseñas robustas y memorizables

Las contraseñas robustas son aquellas que presentan una alta resistencia a ser adivinadas por un atacante, bien mediante fuerza bruta o con heurísticos dirigidos. A continuación, se ofrecen directrices detalladas sobre cómo crear contraseñas que cumplan con los estándares de seguridad exigidos por la UPV:

Contraseñas robustas

La robustez de una contraseña depende de dos factores clave:

- Longitud: Cuanto más larga sea una contraseña, más difícil será adivinarla. La UPV exige que las contraseñas tengan al menos 15 caracteres, y se recomienda que sean aún más largas cuando sea posible. Según las recomendaciones de NIST, una longitud de 64 caracteres es óptima para entornos críticos.
- Aleatoriedad: Las contraseñas deben componerse de caracteres de diferentes categorías (mayúsculas, minúsculas, números y símbolos). Cuanto más uniforme sea la probabilidad de aparición de cada símbolo, mayor será su robustez.

Condiciones mínimas para las contraseñas en la UPV:

- Al menos 15 caracteres.
- Utilizar caracteres de al menos tres de los siguientes grupos: letras minúsculas, letras mayúsculas, números y símbolos de puntuación.
- De estos, es obligatorio que al menos incluya un símbolo de puntuación.

- No se debe derivar de palabras del diccionario.
- No se debe derivar del nombre del usuario o de algún pariente cercano.
- No debe provenir de información personal (como por ejemplo el número de teléfono, DNI, dirección, fecha de nacimiento), ni del usuario ni de ningún pariente cercano.
- Evitar repetir caracteres de forma consecutiva (máximo 2 iguales seguidos).
- No debe contener espacios en blanco.

Consejo adicional: Si se prevé el uso de teclados internacionales, es importante evitar caracteres específicos de un idioma, como la «ñ» o el símbolo «€», ya que pueden no estar disponibles en los teclados de otros países.

Contraseñas memorizables

Aunque es recomendable el uso de un gestor de contraseñas, a menudo es necesario memorizar contraseñas que usamos de manera recurrente (por ejemplo, la contraseña de login del ordenador o la contraseña del propio gestor de contraseñas).

Estrategias para crear contraseñas memorizables:

- Crear una frase personal larga, fácil de recordar.
- Aplicar un método de transformación personal a esa frase para generar una contraseña segura.

Ejemplos de frases:

- «Los acertijos matemáticos son tan antiguos como la propia humanidad»
- «Murciélago o colúmpiame contienen todas las vocales»
- «No quiero recordar más contraseñas, ¡pero me obligan!»

Ejemplos de transformaciones:

- Tomar la primera y última letra de cada palabra de una frase.
- Seleccionar las primeras dos letras de cada palabra.
- Intercalar símbolos entre letras o palabras.

Es importante diseñar nuestras propias transformaciones.

Una vez se adquiere un poco de práctica, es muy fácil utilizar este tipo de contraseñas ya que solo es necesario pensar la frase mientras vamos aplicando la transformación.

Recomendamos la lectura de este breve documento del INCIBE con muchos ejemplos:
<https://www.incibe.es/ciudadania/tematicas/contrasenas-seguras>

2. Uso adecuado de las contraseñas

A parte de tener contraseñas robustas y memorizables, hay que cuidar la forma en las que las utilizamos, es por ello por lo que:

- No reutilizar contraseñas: Cada servicio debe tener una contraseña única. Evita usar la misma contraseña para cuentas de la UPV y servicios externos (por ejemplo, redes sociales o servicios de correo electrónico externos). Se han dado muchos casos de robos de contraseñas en servicios de poca importancia (y normalmente poco asegurados), que luego se han utilizado con éxito para hacer ataques importantes.
- Nunca compartir contraseñas con otras personas: Compartir una contraseña compromete el control y la seguridad sobre la misma. A parte de revelar la contraseña puede que estés dando información sobre la estrategia que utilizas para crear contraseñas.
- Comprobar la seguridad del entorno: Al ingresar una contraseña, asegúrate de que el entorno es seguro, evitando que otras personas puedan ver lo que escribes, o que haya cámaras grabando. Esto es especialmente importante cuando lo haces en el móvil, ya que suele utilizarse en lugares en los que se está más expuesto que cuando usamos nuestro ordenador personal.

3. Renovación periódica de las contraseñas

Todas las contraseñas en la UPV deben renovarse, al menos, una vez cada 12 meses. Esta periodicidad equilibra la usabilidad con la seguridad. Se recomienda un cambio más frecuente si hay indicios de que una contraseña pueda haber sido comprometida.

El cambio periódico de contraseñas limita mucho el tiempo que disponen los atacantes para descifrarla, en caso de haberla obtenido de un servidor, y utilizarla. Recordemos que, en muchas ocasiones, los que roban las contraseñas no solo los mismos que las utilizan, sino que las ponen a la venta en la deep web. Todo este proceso de descifrado y venta puede requerir meses o años.

Precaución ante intentos de phishing: Es frecuente que los atacantes utilicen correos electrónicos falsos para solicitar cambios de contraseña. Recuerda que los correos legítimos de la UPV no incluirán enlaces directos para el cambio de la contraseña.

4. Importancia de las contraseñas

En el ámbito de la informática, las personas somos el eslabón más débil. En especial, el uso de contraseñas débiles es todavía un gran problema de seguridad. Aunque existen más formas de autenticarse, y ha habido muchos intentos de substituir las contraseñas por otro mecanismo que sea más fácil de usar, no parece que en el corto plazo se vaya a conseguir.

Actualmente existen tres formas para autenticar a una persona:

- 1. Algo que sabes (se guarda en nuestra memoria): contraseñas.
- 2. Algo tienes (un objeto que solemos llevar con nosotros), y que siempre debe ser un segundo dispositivo distinto al equipo informático desde el que estamos trabajando.

Habitualmente es el móvil (llamada telefónica, SMS, etc.) o una aplicación (por ejemplo, las apps de autenticación de Microsoft y Google, entre otras).

- 3. Algo que eres (una característica única y difícil de replicar de nuestro cuerpo): huella dactilar, reconocimiento facial, etc.

La autenticación biométrica (algo que eres) es muy cómoda de utilizar, pero tiene el gran inconveniente de ser de un solo uso. Esto es, si nos roban las huellas y fabrican un dedo de goma con nuestras huellas, ya nunca podremos volver a utilizarlas para autenticarnos de forma segura. Por otra parte, los objetos que podemos utilizar para autenticarnos (algo que tienes) pueden perderse o estropearse. Por tanto, a fecha de hoy, las contraseñas (algo que sabes) son el mecanismo más robusto de autenticación, siempre que sean contraseñas robustas y memorizables.

5. Gestores de contraseñas

Dado el elevado número de contraseñas que manejamos a diario, se recomienda encarecidamente el uso de gestores de contraseñas. Estos permiten almacenar contraseñas complejas y únicas para cada servicio, sin necesidad de recordarlas todas.

Un buen gestor de contraseñas no impone límites de longitud, lo que permite generar contraseñas más largas y aleatorias para cada servicio.

Consulta la guía del CSIRT de la Generalitat Valenciana para más detalles sobre la elección y uso adecuado de un gestor de contraseñas: [Guía CSIRT](#).

Autenticación de dos factores (2FA).

El Doble Factor de Autenticación (2FA) o Autenticación Multifactor (MFA) es la segunda capa de seguridad más importante, diseñada para proteger la cuenta incluso si la contraseña es robada (por phishing).

Definición: Es un proceso de seguridad que requiere dos métodos diferentes de verificación de identidad de dos categorías distintas, generalmente:

- Algo que sabes (Tu Contraseña).
- Algo que tienes (Un móvil o token).

Funcionamiento en la UPV: Tras introducir tu usuario y contraseña de UPVnet, el sistema te pide un segundo código que se genera en tu dispositivo móvil (por ejemplo, a través de una app de autenticación, un SMS o una notificación push).

El 2FA se utiliza para acceder a los servicios más críticos (ej. sistemas de gestión, correo electrónico, acceso remoto). Es un requisito de seguridad crucial que debe configurarse obligatoriamente para evitar el robo de identidad por phishing o malware.

En la UPV, para acceder a la mayoría de servicios, se requiere un tridente de seguridad: Usuario + Contraseña (algo que sabes) + Código 2FA (algo que tienes).

Para todo el entorno de upv.edu.es es necesaria una doble autenticación a través de una llamada a tu teléfono de Microsoft o de la aplicación de móvil **autenticator de Microsoft**.

Trabajo Remoto Seguro

El Trabajo Remoto Seguro se refiere a las medidas que el personal debe aplicar al acceder a los sistemas y la información de la UPV desde una ubicación externa (fuera del campus), asegurando la misma protección que en la oficina.

El Dispositivo Aislado

- **Uso de Equipos Corporativos:** Siempre que sea posible, se debe utilizar el equipo proporcionado por la UPV. Esto garantiza que el ordenador tenga instalado el antivirus (ESET), las configuraciones de seguridad de Windows 11 y las políticas corporativas.

Si se utilizan equipos privados han de tener instalados Antivirus y Cortafuegos, recomendablemente los de la UPV, ya que la licencia permite el uso en equipos que sean propiedad de los miembros de la UPV (PAS, PDI, PI, Estudiantes...) durante el tiempo de su vinculación.

- **Actualizaciones al Día:** Antes de conectarse a los sistemas internos de la UPV, el ordenador de trabajo debe tener el Sistema Operativo y el Antivirus completamente actualizados para evitar que vulnerabilidades conocidas sean explotadas.

Seguridad del Entorno Físico Remoto

Aunque se trabaje desde casa, se deben mantener los controles físicos y de privacidad:

- **Bloqueo de Sesión (Siempre):** Mantener la práctica de bloquear la sesión (Windows+L) al dejar el puesto desatendido, incluso si se trabaja solo en casa.
- **Privacidad de la Información:** Asegurarse de que documentos sensibles mostrados en pantalla o impresos no son visibles por personas ajenas a la institución (por ejemplo, evitar el shoulder surfing en lugares públicos o en casa).

La Conexión a Internet

Redes de Confianza: Siempre que sea posible, utilizar una red Wi-Fi doméstica segura y protegida con contraseña.

Evitar Redes Públicas: Se deben evitar las redes Wi-Fi públicas o abiertas (cafeterías, aeropuertos) para acceder a información sensible o sistemas críticos de la UPV, ya que son entornos de alto riesgo donde los datos pueden ser fácilmente interceptados.

(Este contexto establece la necesidad de la VPN, que abordaremos en el siguiente epígrafe).

VPN (Red Privada Virtual)

La Red Privada Virtual (VPN) es la herramienta tecnológica que permite establecer una conexión segura y cifrada entre el equipo del personal administrativo y la red corporativa de la UPV (UPVnet) a través de Internet (un medio no seguro).

Una VPN crea un "túnel" lógico y privado a través de la red pública, y su función clave es que una vez autenticado, el usuario tiene un nivel de acceso casi idéntico a los recursos de la UPV al que tendría si estuviera físicamente en el campus, garantizando que la información transmitida a través de Internet viaje de forma cifrada y segura.

Casos de Uso Obligatorio en la UPV

El personal administrativo debe utilizar la VPN obligatoriamente en los siguientes escenarios de trabajo remoto:

- Planes de Teletrabajo: Es el requisito fundamental para participar en cualquier plan de teletrabajo de la universidad.
- Acceso a Recursos Internos: Cuando se accede desde fuera del campus a recursos que no son públicos, como:
 - La unidad personal W: (almacenamiento en red).
 - Servidores de licencias de software.
 - Revistas y bases de datos científicas de la Biblioteca.
- Escritorio Remoto: Si se necesita acceder al propio ordenador del puesto de trabajo en la UPV mediante herramientas como Escritorio Remoto de Windows.
- Mejorar la Seguridad: Para hacer más segura cualquier transmisión de información sensible entre el hogar (Internet) y la red de la universidad.

Requisito de Acceso

Doble Factor Imprescindible: Para poder conectar por VPN, es absolutamente imprescindible que el usuario haya activado previamente la Autenticación de Doble Factor (2FA) en su cuenta UPV.

Compartir Escritorio

El concepto de Compartir Escritorio se refiere a las funciones que permiten que una persona autorizada (colega o personal técnico) pueda visualizar e incluso tomar el control del escritorio de un equipo de Windows 11. Esto es esencial para el soporte técnico y la colaboración en el teletrabajo.

En el entorno de la UPV, esta función se realiza principalmente a través de dos herramientas:

Microsoft Teams (Colaboración)

La herramienta de comunicación corporativa más utilizada permite ceder la vista del escritorio en tiempo real para colaborar en tareas compartidas, reuniones y presentaciones.

Durante una llamada o reunión o a través del chat, el usuario puede seleccionar la opción "Pantalla Compartida" o "Compartir Pantalla".

Puede optar por compartir:

- Toda la Pantalla: Muestra el escritorio completo, ideal para demostrar un proceso.
- Una Ventana Específica: Muestra solo una aplicación (ej. Excel), ocultando el resto del escritorio, lo que aumenta la privacidad.

Escritorio Remoto y Aplicaciones de Soporte (ISL)

Estas herramientas permiten el acceso o la toma de control total para fines de soporte o acceso a recursos fijos:

- Escritorio Remoto de Windows: Permite al usuario administrativo acceder a su propio ordenador físico del puesto de trabajo en la UPV desde una ubicación remota. Requiere conexión VPN previa y es fundamental para acceder a software o datos que solo residen en el equipo de la oficina.
- ISL (Soporte Técnico): Es una aplicación específica (o similar) que puede ser utilizada por el personal de soporte técnico (ASIC) de la UPV para:
 - Diagnosticar y resolver problemas de software o configuración.
 - Tomar el control del equipo (con permiso del usuario) para aplicar parches, instalar software corporativo (como el ESET) o modificar configuraciones que el administrativo no puede cambiar.

Requisito de Seguridad: Estas sesiones siempre requieren el permiso y la supervisión del usuario que cede el control.

Actualitzat a data de 22 d'octubre.

Recorda revisar-lo de nou: Sis mesos abans de la primera prova. O, si la prova es convoca amb menys de sis mesos, quan acabe el termini de sol·licituds. Així t'asseguraràs que el temari està al dia.

Bona sort... A PER TOTES!

www.stepv.upv.es/axtotes