Actualizaciones de software y seguridad en un sistema Windows

En este ejercicio tienes que responder a todas las preguntas que se plantean a continuación.

***Al igual que en ejercicios anteriores, contéstalas lo mejor que puedas, dedica tiempo a verificar que tu respuesta se ajusta a la pregunta, ya que cualquiera de estos datos podrá preguntarse en exámenes futuros. De la misma forma, apunta las dudas para que, tras la finalización del plazo dado para terminar el ejercicio, las pongas en común con toda la clase.***

***METER PREGUNTAS CONCRETAS DE CONFIGURACIONES EXACTAS, EXCEPCIONES, ETC.***

1. Para preservar la seguridad del sistema, una de las cosas que se debe hacer es mantenerlo actualizado.
   1. ¿Qué es Windows Update y para qué sirve?

Windows Update es una característica del sistema operativo Windows que nos gestiona de la manera que nosotros le indiquemos las actualizaciones del sistema y los componentes. Este sistema de actualizaciones ha ido evolucionando a medida que se han actualizado los sistemas operativos Windows, al principio simplemente era una web donde conseguir temas de escritorio, drivers y algunos complementos para los sistemas Windows 95 y Windows 98, para pasar a ser la plataforma automática (o manual) que instala y prioriza las actualizaciones del sistema operativo, de los drivers y de algunos programas en Windows 10, podéis conocer [todo sobre este sistema operativo aquí](https://www.geeknetic.es/Guia/1668/Windows-10-Todo-lo-que-necesitas-saber.html).

Windows Update se ha ido incorporando poco a poco a los sistemas Windows, desde Windows 2000 ya existía Automatic Updates que permitía instalar las actualizaciones de manera transparente para el usuario, ahora se integra en el panel de control donde podemos acceder a esta función para controlar las actualizaciones según nos permita la versión del sistema operativo Windows que estemos ejecutando, además de instalar las actualizaciones para el sistema, lo hace para otros módulos como Windows Defender y así mantener actualizada la base de datos de virus y amenazas.

Esta parte del sistema operativo gestiona las actualizaciones de manera eficiente, primero da prioridad a las actualizaciones importantes o de seguridad, luego añade las mejoras o arreglo de errores que puede tener el sistema operativo y deja paso por último a las opcionales que simplemente se instalarán si nosotros las iniciamos. Las actualizaciones se pueden activar para que funcionen automáticas, desactivarlas temporalmente o [desactivarlas para siempre](https://www.geeknetic.es/Noticia/16532/Como-desactivar-las-actualizaciones-automaticas-en-Windows-10.html).

Este módulo del sistema operativo Windows puede funcionar, si lo configuramos para que funcione de manera automática, cuando no usamos el equipo, nosotros podemos configurar que se realicen automáticamente pero cuando no estemos usando el ordenador, en el sistema podemos configurar unas horas activas, en las que normalmente usamos el ordenador, para cuando vaya a realizar una actualización no interfiera durante nuestro trabajo.

Windows Update sirve para instalar todas las actualizaciones de Windows de una manera sencilla, simplemente tendremos que entrar en la utilidad Windows Update, dentro del apartado de configuración de Windows, ponerla a nuestro gusto y empezar a recibir las últimas novedades, las mejoras y arreglos en fallos del sistema operativo, incluso mantener al día la base de datos de Windows Defender para estar protegidos en todo momento.

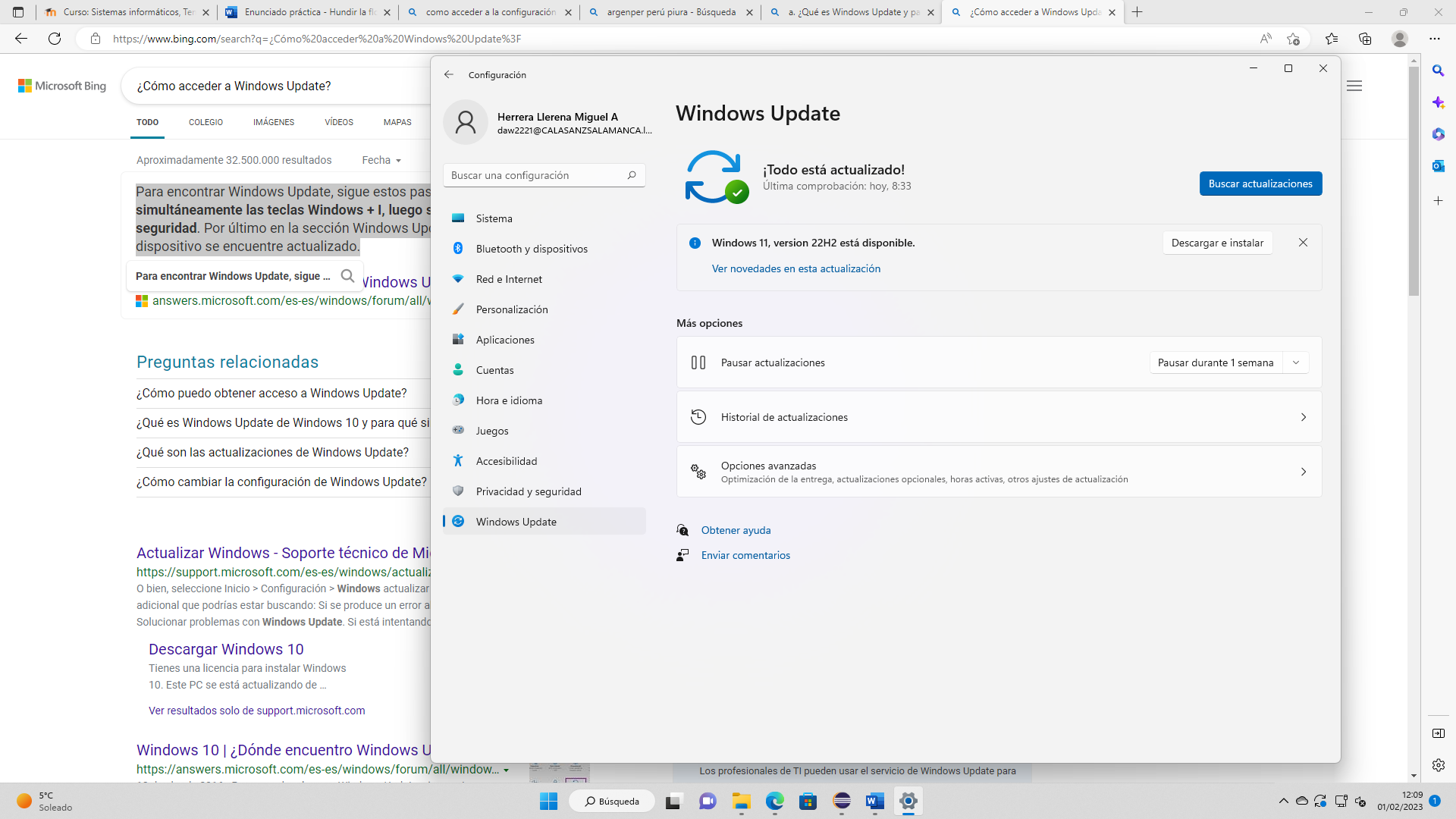
Con Windows Update podemos recibir las grandes actualizaciones que ofrece Windows 10 que normalmente son dos veces al año, así cuando toque instalar la nueva actualización de Windows 10 con las nuevas funciones que se han desarrollado para incluir en sistema, podemos ir al centro de control y seleccionar Windows Update para aceptar la nueva actualización, descargarla e instalarla de manera automática. Una vez finalizada el asistente nos indicará si es necesario reiniciar el equipo para completarla y dejarlo todo listo para seguir funcionando y poder usar las nuevas opciones añadidas.

Este módulo de actualizaciones también nos sirve para tener todos nuestros drivers actualizados, antiguamente teníamos que introducir los diferentes DVD´s de los fabricantes que se incluían con el hardware que comprábamos para poder instalar los, en la mayoría de los casos, obsoletos drivers que hacían funcionar los componentes de nuestro ordenador, ahora al instalar Windows es usual disponer de estos drivers actualizados al momento y simplemente tendremos que esperar que haya una actualización que corrija algún fallo o añada funciones para que se instalen de manera automática si así lo tenemos configurado.

Así de sencillo es mantener tu equipo al día, tanto tu sistema operativo Windows como todos los drivers y programas asociados a este, simplemente gracias a este módulo Windows Update, que gestiona todas las actualizaciones de la manera que nosotros configuremos, pueden ser actualizaciones automáticas o entrando en el apartado de Windows Update e iniciarlas nosotros manualmente.

* 1. ¿Cómo se accede a Windows Update?

Para encontrar Windows Update, sigue estos pasos: Presiona simultáneamente las teclas Windows + I, luego selecciona Actualización y seguridad. Por último en la sección Windows Update verifica que tu dispositivo se encuentre actualizado.



* 1. Indica qué puedes configurar en cuanto a actualizaciones del sistema.

Actualizaciones de calidad.

Actualizaciones de controlador.

Actualizaciones de definiciones.

Desinstalar las actualizaciones.

Opciones de recuperación.

* 1. ¿Qué podría pasar si no se actualizase, de forma periódica, el sistema?

Obtener información sensible y confidencial de nuestra empresa, como cuentas de acceso a otros servicios o bases de datos de clientes o de facturación; cifrar la información del servidor y solicitar un «rescate» por ella, el tan mencionado [ransomware](https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware" \o "Servicio Antiransomware); desconfigurar los sistemas de seguridad de la compañía para espiarnos, robar información o atacarnos más adelante; usar nuestros sistemas como plataforma de ataque hacia otros sistemas, se queda a vulnerabilidad

* 1. Indica dentro de que apartado se encuentra Windows Update y que información se puede ver nada más acceder a dicho apartado.

Configuración y se puede visualizar todo el historial de actualizaciones.

* 1. Teniendo en cuenta el apartado nombrado en el punto anterior:
     1. ¿Qué crees que aportan las secciones Copia de Seguridad y Recuperación?

La copia de seguridad y recuperación hace referencia a la práctica de crear y almacenar copias de sus datos que pueden usarse para restaurar los servicios de su organización en caso de una falla primaria a causa de un corte eléctrico, un ataque de ransomware u otro tipo de desastre.

* + 1. Recuperación Es más relacionado con el sistema operativo
    2. Nombra alguna del resto de secciones que puedes encontrar e indica que te ha parecido interesante de las funcionalidades que ofrece.

1. Seguridad: En el apartado Seguridad de Windows, puedes encontrar distintas opciones de configuración para hacer de tu equipo un dispositivo seguro.
   1. ¿Qué es Microsoft Defender o Windows Defender? ¿Cómo puedes acceder a ello?

Microsoft Defender (anteriormente conocido como Windows Defender) es un programa de seguridad antivirus cuyo propósito es buscar y solucionar amenazas, prevenir, quitar y poner en cuarentena software espía y malware en Microsoft Windows. Es incluido y activado por defecto en Windows 8, Windows 8.1, Windows 10 y Windows 11

* 1. A grandes rasgos, ¿qué te permite configurar el antivirus?

Windows Defender se incluye con Windows y ayuda a impedir que el malware infecte su PC de dos modos:

Protección en tiempo real.‍‍ Windows Defender notifica al usuario cuando alguna herramienta de malware intenta instalarse en su PC. También notifica al usuario cuando las aplicaciones intentan modificar valores de configuración importantes.

Opciones de examen en cualquier momento. Puede usar Windows Defender para examinar el equipo en busca de posible malware instalado, para programar exámenes regulares y para quitar automáticamente (o poner en cuarentena de manera temporal) cualquier elemento detectado durante un examen

* 1. ¿Para qué sirve un Firewall?

Un firewall es un programa informático que controla el acceso de un ordenador a una red con el objetivo de prohibir la entrada a usuarios no autorizados. El cortafuegos examina todos los mensajes que entran y salen de la red. De esta forma, bloquea la llegada de las comunicaciones que no cumplen con unos criterios de seguridad y permite la entrada de aquellas que sí están reglamentadas.

Para aclarar la definición de firewall también podemos utilizar una sencilla comparación: un cortafuegos es para una red informática lo que una puerta es para una casa. Mientras que la puerta impide la entrada a personas extrañas, el firewall bloquea el acceso de usuarios desconocidos

* 1. Indica si un antivirus y un Firewall es lo mismo, o no, y por qué.

No. Un antivirus es un software que se encarga de rastrear el sistema en busca de amenazas. Puede realizar un escaneo en un momento concreto o en tiempo real. De esta forma, nos avisaría en caso de que vea algo extraño en nuestro equipo. Por ejemplo si al rastrear encuentra un software malicioso nos lanzaría una alerta para que lo eliminemos o incluso de forma automática lo borraría.

* 1. Busca como incluir excepciones en el Firewall.

1. Como resumen, diremos que la configuración básica de seguridad del sistema pasa por:
   1. Activar las actualizaciones automáticas.
   2. Configurar el Firewall y tenerlo habilitado.
   3. Tener siempre habilitado Windows defender.