GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Taller formativo

Seguridad en dispositivos Windows y macOS

017 TU AYUDA EN CIBERSEGURIDAD
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
CIBERCOOPERANTES incibe_

LICENCIA DE CONTENIDOS

ÍNDICE

1. OBJETO DEL DOCUMENTO

El presente documento constituye una herramienta didáctica que servirá de apoyo al docente para la planificación del **taller formativo de "Seguridad en dispositivos para sistemas operativos Windows y macOS"**.

Esta herramienta supone un **instrumento específico de planificación, desarrollo y evaluación** de cada una de las áreas de las que se compone la acción formativa, y requiere de la labor docente para concretar los distintos elementos curriculares adaptándolos a las características del alumnado.

A lo largo de la guía docente, se profundizará en los **objetivos generales y específicos de la acción formativa, sus contenidos, criterios de evaluación y aquellos materiales y recursos adicionales** que se requieran para la impartición de las competencias recogidas en el taller.

2. ORGANIZACIÓN Y ESTRUCTURA

La estructura del taller estará compuesta por 6 temas que comprenderán los contenidos teóricos y actividades para el trabajo individual de cada alumno.

La estructura completa del taller es la siguiente:

1. **Roles y usuarios: aspectos de seguridad y privilegios.**
2. **Actualizaciones automáticas: sistemas operativos y aplicaciones.**
3. **Antivirus y herramientas de protección básica.**
4. **Características y gestión de las contraseñas.**
5. **Copias de seguridad.**
6. **Redes inalámbricas en el ordenador.**
7. **Seguridad básica en redes**.

3. OBJETIVO

Este taller tiene como objetivo principal **proporcionar a los alumnos las competencias necesarias para gestionar la seguridad y protección de sus dispositivos a través de las opciones de configuración de sus equipos (Windows y macOS)**. Dado el enfoque teórico-práctico, así como el nivel de profundidad de sus contenidos, el taller va dirigido a un colectivo de usuarios con conocimientos muy básicos sobre tecnología y seguridad.

A lo largo del taller, se ofrecerá a los alumnos recursos de ampliación en forma de enlaces de la OSI, con el fin de expandir sus competencias y satisfacer su curiosidad. Del mismo modo, servirán al docente para enriquecer los contenidos del taller.

4. METODOLOGÍA Y RECURSOS

La metodología empleada en el desarrollo de este taller es de **carácter teórico-práctico, visual y buscando la participación activa del alumnado** durante la impartición del taller:

- **Teórico-práctica**: Los contenidos teóricos vendrán acompañados en todo momento de ejemplos reales que aterricen la teoría. A través de casos reales y actividades, el alumnado pondrá en práctica la información transmitida a través del taller.
- **Visual**: Las imágenes técnicas y decorativas abundarán a lo largo de todo el taller. Además, para dinamizar aún más los talleres, se incluirán recursos audiovisuales relacionados con el contenido (al menos 1 vídeo por taller).
- **Participación activa**: El alumnado tendrá un papel fundamental en los talleres, pues no se limitarán a escuchar. Los contenidos están preparados para que se pongan en práctica desde el comienzo del taller en cada uno de los equipos del alumnado.
    - Además, se busca enriquecer la experiencia formativa a través de las dudas y comentarios que se expongan durante su desarrollo.

El taller cuenta con diferentes **actividades y recursos** al servicio del docente para la impartición:

- **Presentación en Power-Point**. Se trata de una presentación con comentarios en texto para apoyar al docente, y los contenidos a compartir con el alumnado.
- **Actividades**. Se trata de pequeñas actividades que permiten al alumnado poner en práctica los conocimientos recién adquiridos, y que acompañan a los apartados principales.
- **Vídeos y enlaces para ampliar**. Servirán para afianzar los contenidos desarrollados mediante ejemplos y contenidos para ampliar, con los que enriquecer la acción formativa.
- **Cuestionario de evaluación**. Cuestionario final del taller formado por 15 ítems con opción múltiple con el que realizar la evaluación final de los alumnos.

5. CONTENIDOS

A continuación, se muestra el contenido del taller ordenado en diapositivas para facilitar la tarea al docente.

5.1. Diapositiva 1. Presentación del taller

Presentación del taller “Seguridad en dispositivos Windows y macOS”. Debe mencionarse la labor de INCIBE y el teléfono de ayuda 017.

5.2. Diapositiva 2. Índice

Presentación del índice de contenidos del taller:

1. Roles y usuarios: aspectos de seguridad y privilegios.
2. Actualizaciones automáticas: sistema operativo y aplicaciones.
3. Antivirus y herramientas de protección básica.
4. Características y gestión de las contraseñas.
5. Copia de seguridad.
6. Redes inalámbricas en el ordenador: wifi y *Bluetooth*
7. Seguridad básica en las redes.

5.3. Diapositiva 3. Introducción

Nuestros dispositivos son una parte fundamental en nuestro día a día.

Por ello es tan importante que conozcamos algunas de sus funciones de seguridad básicas, así como las tareas de mantenimiento o configuraciones de seguridad que podemos llevar a cabo junto a los procesos automáticos que la mejoran.

5.4. Diapositiva 4. Roles y usuarios

Si nuestro equipo es compartido con varias personas, puede que nos interese crear distintas cuentas de usuarios con distintos niveles de privilegios. Si no las gestionamos adecuadamente, corremos el riesgo de:

- Que terceros puedan acceder a nuestros archivos y eliminar/modificar información personal, como imágenes, música, documentos importantes, etc.
- Modificar configuraciones de seguridad o usabilidad de nuestro sistema, como, por ejemplo, desactivar el antivirus o *firewall*.
- Conectarse a determinados servicios con nuestras credenciales, como el correo electrónico o nuestra red social.

Por seguridad, lo ideal es mantener un único usuario administrador por dispositivo y mantener al mínimo los privilegios del resto de cuentas de usuario para evitar riesgos. No queremos que, por error, otro usuario pueda llegar a instalar *software* malicioso o a desactivar determinadas medidas de seguridad en nuestro equipo.

5.5. Diapositiva 5. Roles y usuarios Windows

Existen distintos tipos de cuentas de usuario en Windows:

- **Usuario administrador**. Este tipo de usuario tendrá todos los privilegios y permisos sobre el dispositivo, con lo cual podrá realizar todos los cambios que desee en la configuración (dentro de los límites del fabricante). Para determinados cambios el sistema, nos solicitará la contraseña de administrador como medida de seguridad. Dentro de sus privilegios, está la instalación de *software*, por ejemplo. Este es el motivo por el que se convierten en el objetivo de los ciberdelincuentes.
- **Usuario "Tu familia"**. Esta categoría tiene por objetivo dividir a los miembros de la familia entre adultos y menores para diferenciarlos entre sí y aplicar restricciones de permisos y privilegios a estos últimos. Es necesario vincular la cuenta a alguno de los servicios de Microsoft, como es Outlook. En cuanto a privilegios, pueden tener los mismos privilegios que un usuario administrador, ya que su función principal es la de limitar las funcionalidades a aquellos usuarios menores de edad.
- **Otros usuarios**. Estos usuarios no necesitan vincular ningún tipo de servicio a sus cuentas y sus privilegios se tratan del mismo modo que la categoría anterior (administrador o usuario estándar). Puede crearse un perfil facilitando únicamente el número de teléfono móvil, en lugar de una cuenta de Outlook, si es que el usuario invitado no dispone de una.

5.6. Diapositiva 6. Roles y usuarios Windows

Para crear cuentas tendremos que:

- Ir a la imagen de Windows en la parte inferior izquierda.
- Ahora clic en **Configuración > Cuentas > Familia y otros usuarios** u **Otros usuarios**.

Luego, si quieres crear un usuario local o un administrador, los pasos serán distintos. Una vez creada, podrás volver a modificar su perfil para darle o quitarle privilegios de administrador del dispositivo.

Más información en: Cómo cambiar los usuarios (cuentas) en Windows 10

5.7. Diapositiva 7. Roles y usuarios macOS

Debemos tener en cuenta que esta configuración solo la puede realizar un administrador del sistema y para hacerlo tendremos que proceder del siguiente modo:

- Iremos al logo Apple y haremos clic en **Preferencias del sistema > Usuarios y Grupos**.
- Luego haremos clic sobre el candado para que se desbloquee.
- Ingresaremos con el nombre del administrador y contraseña de acceso.
- Seleccionaremos en el menú **Nueva carpeta** y elegiremos el tipo de usuario que queremos crear.
- Estos usuarios pueden ser:
    - **Administrador:** Puede crear o eliminar usuarios, estándar o administradores de un mismo dispositivo.
    - **Estándar***:* Este perfil de usuario puede instalar aplicaciones y modificar su propio perfil, no podrá hacerlo en otros perfiles de usuario.
    - **Solo compartir***:* Este tipo de usuario solo podrá acceder a los archivos de manera remota, pero no tienen ninguna función sobre el dispositivo, como ingresar en algún perfil.

Más información en: Configurar usuarios, invitados y grupos en el Mac

5.8. Diapositiva 8. Roles y usuarios macOS

Ahora que tenemos idea del tipo de perfil que podemos crear:

- Introduciremos el nombre completo para el nuevo perfil.
- Asignaremos una clave para dicho perfil. Esta clave debemos confirmarla y escribir una pista para ayudarnos a recordarla.
- Crearemos el usuario. Podremos elegir si puede o no administrar el dispositivo o si el nuevo usuario puede hacer uso del panel de preferencias para compartir archivos del dispositivo.
- Si el dispositivo cuenta con funciones de inicio de sesión por medios biométricos, el nuevo perfil podrá hacer uso de este.

Antes de continuar, debemos saber que un usuario estándar puede ser convertido en administrador del dispositivo, basta con indicarlo en la lista de usuarios, seleccionando **Permitir al usuario administrar este ordenador**.

5.9. Diapositiva 9. Roles y usuarios macOS

1. **Crear un grupo**. Este tipo de perfil permite que varios usuarios puedan tener acceso al dispositivo o simplemente a un archivo específico, sin el nivel administrativo.
    - Volveremos a **Usuarios y grupos** y haremos clic sobre el candado para que se desbloquee.
    - Ingresaremos con el nombre del administrador y contraseña de acceso.
    - Haremos clic en **Añadir** e iremos al menú **Nueva cuenta > Nuevo grupo**.
    - Ahora pondremos un nombre al nuevo grupo y seleccionaremos clic en **Crear grupo**.
    - Debemos elegir los usuarios o grupos que tendrán acceso al nuevo grupo.
    - Podemos utilizar el panel **Preferencias** para indicar si los usuarios pueden compartir archivos o la pantalla.

2. **Usuarios ocasionales**. Este tipo de usuario es específicamente para aquellos que solo hacen uso del dispositivo de manera temporal. Estos no requerirán ningún tipo de contraseña para el inicio de sesión, ni tampoco tendrán privilegios de usuarios estándar. Los archivos creados por este tipo de usuario serán de carácter temporal y no estarán en el dispositivo hasta el momento en que este cierre la sesión.

   En caso de que tengamos activo el **FileVault**, el usuario invitado solo podrá hacer uso del navegador “Safari”, no tendrá acceso a nuestros archivos.

5.10. Diapositiva 10. Actividad 1

Diapositiva para introducir a los usuarios la actividad. El tiempo aproximado de duración será de entre 3-5 minutos. Los pasos habrán sido descritos en las diapositivas anteriores.

La labor del docente será la de acompañar a los usuarios y ayudar en caso necesario. Se debe valorar la iniciativa, la resolución de la actividad y la proactividad.

Actividad 1:

Configurar los usuarios en el dispositivo ayudará a evitar que se le realicen modificaciones al sistema sin nuestra autorización, con lo cual la seguridad sobre el dispositivo mejorará, así que vamos a crear nuestro propio usuario y asegurémoslo con una contraseña robusta.

5.11. Diapositiva 11. Actualizaciones automáticas

Las actualizaciones son modificaciones realizadas sobre el sistema operativo o el *software* instalado en nuestros dispositivos. Su función es la de mejorar aspectos de funcionalidad, seguridad y corregir vulnerabilidades o errores encontrados.

5.12. Diapositiva 12. Actualizaciones automáticas Windows

Para realizar la actualización del sistema operativo del dispositivo:

- Iremos a **Configuración > Actualización y Seguridad > Buscar actualizaciones**.

Lo más recomendable es configurar el dispositivo para que las actualizaciones se apliquen de forma automática. Del mismo modo, deberemos actualizar el resto de las aplicaciones instaladas en nuestro equipo, pero recordemos:

- Utilizar siempre *software* original y no pirata.
- Descargar las actualizaciones desde la página oficial.
- Habilitar las actualizaciones automáticas si es posible.

Hemos de ser conscientes del riesgo que corre un sistema no actualizado, ya que las posibilidades de acabar infectado se multiplican. Al detectarse una vulnerabilidad no corregida, los ciberdelincuentes no tardarán en descubrir el modo de explotarla.

Si no mantenemos nuestros equipos al día, nos exponemos a todo tipo de riesgos: robo de información, pérdida de privacidad, perjuicio económico, suplantación de identidad, etc.

5.13. Diapositiva 13. Actualizaciones automáticas macOS

Es necesario entender que las actualizaciones del sistema son importantes porque permiten no solo mejorar el rendimiento del dispositivo, sino también su seguridad:

- Iremos al logo de Apple.
- Haremos clic en preferencias del sistema.
- Verificaremos si hay actualizaciones del sistema, haciendo clic en actualizaciones del *software*.
- Si hay actualizaciones disponibles, haremos clic en actualizar para que estas se instalen.
- Al terminar, veremos un mensaje que indicara que el dispositivo está actualizado.

Las actualizaciones de las aplicaciones deberemos hacerlas desde la Apple Store. Bastará con hacer clic en la pestaña **Actualizaciones**, pero además podremos permitir que estas

actualizaciones se realicen de forma automática, simplemente dejando seleccionado **Mantener el macOS actualizado automáticamente**. Una vez hecho, saldrá un mensaje que nos indicará que es necesario reiniciar el dispositivo.

5.14. Diapositiva 14. Actividad 2

Diapositiva para introducir a los usuarios la actividad. El tiempo aproximado de duración será de entre 3-5 minutos. Los pasos habrán sido descritos en las diapositivas anteriores.

La labor del docente será la de acompañar a los usuarios y ayudar en caso necesario. Se debe valorar la iniciativa, la resolución de la actividad y la proactividad.

Actividad 2:

Un dispositivo actualizado es un dispositivo preparado para defenderse de todo tipo de virus y ataques al sistema. Tomemos unos minutos, accedamos a la configuración de nuestro dispositivo y asegurémonos de que está actualizado a la última versión, así como el *software* que tengamos instalado.

5.15. Diapositiva 15. Antivirus y herramientas de protección básicas

Las herramientas de protección de nuestro dispositivo tienen como objetivo evitar que los ataques a nuestro sistema logren causar daño o robar información, como:

- **Antivirus**. Se trata de *software* cuyo propósito es evitar que nuestro sistema se infecte e identificar cambios que pudieran ser realizados por algún *malware*. También permite que el usuario informe sobre los posibles ataques que ha sufrido su dispositivo y la desinstalación de aplicaciones instaladas en su navegador Internet Explorer.
- ***Firewall***. Sirve como filtro de las comunicaciones que se dan a través de la red en las que interviene el dispositivo, haciendo que las comunicaciones que entran o salen sean analizadas y verificadas, en búsqueda de agentes maliciosos que pudieran afectar al sistema operativo o la información personal, archivada en nuestro dispositivo, evitando así, una posible intrusión.

5.16. Diapositiva 16. Antivirus y herramientas de protección básicas Windows

Microsoft incorpora en sus sistemas operativos un servicio de antivirus integrado, conocido como Windows defender. Además, también tiene integrado un *firewall* que podemos activar y desactivar a nuestro gusto. Nuestros equipos disponen de un **Centro de Seguridad** para configurar estas medidas de protección:

- Haremos clic en el icono de Windows que está en la parte inferior izquierda.
- Ahora, iremos a **Configuración > Actualización y Seguridad**, allí veremos una lista de funciones que podremos activar, desactivar y modificar.

Además, la OSI pone a nuestra disposición una gran variedad de herramientas de protección aparte de la incluida en el propio sistema.

5.17. Diapositiva 17. Antivirus y herramientas de protección básicas macOS

En el caso de Apple, estas herramientas, así como las funciones destinadas a mejorar la protección de nuestro sistema, han evolucionado mucho desde sus primeras versiones:

- **Chip M1:** Este dispositivo viene integrado a partir de macOS Big Sur. El chip M1 ofrece las prestaciones de seguridad más avanzadas. El arranque seguro está verificado por *hardware*. El cifrado automático de alto rendimiento se aplica a todos los archivos. Y hay nuevas protecciones de seguridad integradas en la arquitectura de ejecución de código del M1.
- **Protección en la aplicación:** Desde la llegada de macOS Catalina y gracias a un *software* integrado de antivirus, estos impiden que *software* dañinos se ejecuten.
- **App Review y Gatekeeper:** Gracias a estos dos mecanismos de protección de Apple, se puede descargar la aplicación, bien desde el Apple Store o desde Internet, dando la seguridad a que serán analizadas en búsqueda de algún *software* peligroso para nuestro dispositivo.
- **Control sobre aplicaciones:** Siempre habrá una consulta sobre los permisos que queramos darle a las aplicaciones que instalemos en el dispositivo.
- **FileVault2:** Con esta función, disponible desde los primeros sistemas macOS, el disco duro de nuestro dispositivo estará encriptado, lo que, sumado al Chip T2 (a partir de macOS Catalina), los convierte en una de nuestras mejores defensas.

Además, la OSI pone a nuestra disposición una gran variedad de herramientas de protección aparte de la incluida en el propio sistema.

5.18. Diapositiva 18. Actividad 3

Diapositiva para introducir a los usuarios la actividad. El tiempo aproximado de duración será de entre 3-5 minutos. Los pasos habrán sido descritos en las diapositivas anteriores.

La labor del docente será la de acompañar a los usuarios y ayudar en caso necesario. Se debe valorar la iniciativa, la resolución de la actividad y la proactividad.

Actividad 3:

Las herramientas de protección de nuestro sistema nos protegen de una gran variedad de riesgos. Quizás sea el momento de asegurarnos que nuestras defensas están activadas. Vamos a entrar al sistema y comprobar que las herramientas mencionadas anteriormente están activadas y funcionando.

5.19. Diapositiva 19. Características y gestión de las contraseñas

Las contraseñas sirven para mantener seguros nuestros equipos y la información almacenada en ellos. Una correcta gestión de las contraseñas es, por tanto, algo

fundamental para tener en cuenta, y que comienza con la creación de una contraseña robusta:

- Entre 8 o 10 caracteres mínimo.
- Que sea una combinación de letras mayúsculas, minúsculas, números y caracteres especiales.
- Evitar usar palabras comunes e información personal.
- No repetir contraseña y actualizarla cada cierto tiempo.
- Un gestor de contraseñas nos ayudará a gestionarlas de forma más eficiente.
- Y, siempre que el servicio lo permita, utilizar el doble factor de autenticación.

Más información sobre la gestión segura de contraseñas en la campaña de concienciación publicada en la web de OSI: https://www.osi.es/es/campanas/contrasenas-seguras

5.20. Diapositiva 20. Características y gestión de las contraseñas Windows

En nuestro equipo, no será necesaria la creación de una contraseña para asociarla a la cuenta de nuestro usuario, pero si hará que el dispositivo y la información estén más protegidos. Si queremos agregar/modificar la contraseña de inicio de sesión:

- Haremos clic en la ventana de Windows que se encuentra en la parte inferior izquierda.
- Luego, iremos a **Configuración > Cuentas > Opciones de inicio de sesión**.
- Seleccionaremos **Contraseña** y escribiremos la clave que queramos utilizar para desbloquear el dispositivo.

5.21. Diapositiva 21. Características y gestión de las contraseñas macOS

Podemos cambiar una contraseña de usuario ya creada. Para ello, iremos al menú con el **Logo Apple > Preferencias del sistema > Usuarios y grupos**. Elegiremos el usuario que deseemos y cambiaremos la contraseña desde el botón **Cambiar contraseña.**

- Desde **aplicaciones > Utilidades** podremos acceder a la aplicación de **Acceso a llaveros**, podemos seleccionar mostrar llaveros.
- Seleccionaremos el llavero que queramos abrir, haciendo doble clic sobre él y luego sobre el ítem que queramos ver. Por ejemplo, “Obtener información”, “Mostrar contraseña”, “Control de acceso”, “Solicitar contraseña del llavero” o un “certificado”. Así podremos ver la información que contiene cada uno de los ítems y encontrar lo que necesitemos.

5.22. Diapositiva 22. Actividad 4

Diapositiva para introducir a los usuarios la actividad. El tiempo aproximado de duración será de entre 3-5 minutos. Los pasos habrán sido descritos en las diapositivas anteriores.

La labor del docente será la de acompañar a los usuarios y ayudar en caso necesario. Se debe valorar la iniciativa, la resolución de la actividad y la proactividad.

Actividad 4:

¿Tenemos una contraseña robusta? Si no estamos seguros, no pasa nada, más vale tarde que nunca. En el siguiente enlace encontraremos un recurso con el que poner a prueba nuestros conocimientos.

5.23. Diapositiva 23. Copias de seguridad

En vista de que ningún sistema está exento de tener fallos, bien sea por errores propios, virus o incluso debido al error humano, es recomendable disponer de una copia de seguridad con el fin de recuperar la información perdida o corregir algún daño existente.

La copia de seguridad evitará que perdamos la información (fotos, videos, música etc.) que hemos almacenado en nuestro dispositivo a través del tiempo, por daño, robo del dispositivo o simplemente pérdida de la información.

5.24. Diapositiva 24. Copias de seguridad Windows

Podemos crear una copia de seguridad de nuestro sistema fácilmente, solo necesitaremos disponer de un dispositivo externo de almacenamiento en el que podamos guardar la copia o espacio de almacenamiento suficiente. Una vez conectado a nuestro equipo, deberemos:

- Hacer clic en el icono de Windows, abajo izquierda de la pantalla. Luego en **Configuración > Actualización y Seguridad > Copia de seguridad.**
- Seleccionaremos **Agregar una unidad** y el lugar donde queramos que se almacene la copia de seguridad.
- Posteriormente, podremos configurar la copia de seguridad activando esta opción, o desactivándola. Si lo activamos, generará una copia de manera automática.
  Para configurarlo, deberemos hacer clic en **Más opciones**. Allí, podremos elegir:
  - Hacer una copia.
  - Elegir cada cuanto queremos que se genere una copia o durante cuánto tiempo tener guardada la copia.
  - También podremos elegir una carpeta de la que deseamos una copia o eliminar las carpetas de archivos de las que no deseemos una copia. Para ello, basta con tocar la carpeta y luego hacer clic en **Quitar**.

5.25. Diapositiva 25. Copias de seguridad macOS

En dispositivos Apple existe una función integrada conocida como **Time Machine.** Permite realizar copias de seguridad de todos nuestros archivos de forma automática. Para ello, solo necesitaremos un dispositivo de almacenamiento externo:

- Tras conectarlo y seleccionarlo como disco de copia de seguridad, la aplicación realizará automáticamente las copias de las últimas 24 horas, y poco a poco irá almacenando las copias por días del último mes y las copias por semanas de los

últimos meses, además se irán eliminando las copias más antiguas a medida que el dispositivo externo se llena.

5.26. Diapositiva 26. Copias de seguridad - VIDEO

En esta diapositiva se compartirá con los usuarios un vídeo que representará los pasos anteriormente descritos para realizar una copia de seguridad en dispositivos Windows y MacOS. La duración será de 1 min. aproximadamente.

5.27. Diapositiva 27. Actividad 5

Diapositiva para introducir a los usuarios la actividad. El tiempo aproximado de duración será de entre 3-5 minutos. Los pasos habrán sido descritos en las diapositivas anteriores.

La labor del docente será la de acompañar a los usuarios y ayudar en caso necesario. Se debe valorar la iniciativa, la resolución de la actividad y la proactividad.

Actividad 5:

Tener una copia de seguridad de archivos y aplicaciones instaladas en el ordenador nos protegerá en caso de pérdida, ya sea por un fallo en el sistema, un descuido por nuestra parte o por un ciberataque. Así que, dediquemos unos minutos a configurar nuestro sistema para que lo realice de manera automática.

5.28. Diapositiva 28. Redes inalámbricas en el ordenador

Entre las funciones de los ordenadores, se encuentran las redes inalámbricas. Tanto en dispositivos portátiles como de escritorio normalmente vienen integrados, pero en caso de no ser así, cabe la posibilidad vincularles un *hardware* para que cumplan la función inalámbrica, pudiendo hacer uso un sistema de red wifi o Bluetooth conectándolo al dispositivo, como por ejemplo un ratón o el teclado mismo. Existen diferentes tipos, como:

- **Bluetooth:** Normalmente viene integrado en los dispositivos portátiles, haciendo posible que este pueda conectarse de manera inalámbrica con otros dispositivos que cuenten con esta misma función. Tras realizar, lo que se conoce como emparejamiento, podremos compartir archivos o información con uno o más dispositivos, entre los que están: móviles, ordenadores o electrodomésticos, televisores, equipos de audios… que cuenten con la tecnología Bluetooth.
- **Wifi:** Este servicio, también incluido en los dispositivos portátiles, permite la conexión a los servicios de Internet a través de un *router*. Con este servicio activo podremos navegar por la red, compartiendo y descargando archivos de texto, video, audio, etc., a través de los navegadores web o de servicios de mensajería instantánea.

5.29. Diapositiva 29. Redes inalámbricas en el ordenador: wifi

Windows: Esta función la encontraremos en la esquina inferior derecha de nuestro escritorio, en el icono de red wifi, o en el **botón de inicio (esquina inferior izquierda) > Configuración > Wi-Fi**.

- Desde aquí podremos analizar las redes disponibles a las que conectarnos y activar/desconectar esta funcionalidad.
- En cuanto a los ordenadores que no cuentan con un sistema wifi integrado, cabe la posibilidad de agregarle un dispositivo hardware que cumpla con esta función.
    - Para activar el servicio podremos hacerlo desde **Configuración > Red e Internet.**

macOS: esta función la encontraremos en la barra superior (derecha) del menú de nuestro dispositivo. Aquí podremos observar el estado de nuestra conexión y, desplegando la lista, podremos elegir a que red conectarnos.

También desde ese menú podremos desactivar esta función simplemente haciendo clic **Desactivar wifi**. Para ello debemos saber que las redes que muestran un pequeño icono con forma de candado son las que requieren una clave de acceso.

En el caso de querer compartir nuestros datos de Internet del teléfono móvil con el dispositivo Mac:

- Iremos al icono wifi. Si su estado es **Desconectado**, entonces deberemos activarlo.
- Seleccionaremos la red wifi a la que queramos conectarnos y, en caso de que la red a la que queramos conectarnos esté oculta, haremos clic en **Acceder a otra red**. Allí, deberemos ingresar su nombre y clave de acceso.
- Luego seleccionaremos **Recordar esta red**.

5.30. Diapositiva 30. Redes inalámbricas en el ordenador: wifi

El principal riesgo de las conexiones wifi está a la hora de conectarnos a una red pública, ya que corremos el riesgo de infectar nuestros dispositivos y perder nuestras credenciales a manos de un ciberdelincuente que, mediante distintos tipos de ataque, puede monitorizar nuestra actividad online o engañarnos para acabar accediendo a una web fraudulenta.

El mejor consejo es no conectarnos a redes públicas a no ser que sea imprescindible, y siempre con una VPN. Además, no acceder a nuestras cuentas o servicios más personales, como la cuenta bancaria, correo electrónico o redes sociales, para evitar que acaben en manos de terceros.

5.31. Diapositiva 31. Redes inalámbricas en el ordenador: Bluetooth

Windows: para el caso de los dispositivos que no lo tengan integrado, cabe la posibilidad de agregarle un pequeño *hardware* a través de uno de los puertos USB que cumpla dicha función.

- Para activar el dispositivo, podremos hacerlo desde **Configuración > Dispositivos**

macOS: otros de los beneficios con los que cuenta el uso de Bluetooth en macOS, son:

- Recibir o compartir conexión a Internet, desde y hacia los dispositivos telefónicos iPhone o tablets de Apple a través de este medio.
- Explorar las carpetas públicas de otros dispositivos.
- Permitir que sean revisadas las carpetas públicas o la que elijas de nuestro dispositivo.

- Enviar y recibir ficheros con los dispositivos que se hayan vinculado previamente.

Podremos configurar y vincular los dispositivos Apple desde menú **Logo Apple > Preferencias del sistema > Bluetooth**

Si bien es una función muy útil a la hora de compartir información con otros usuarios o para sincronizar determinados dispositivos, como auriculares inalámbricos, su mayor riesgo reside en que un dispositivo que no conocemos acabe sincronizándose a nuestro dispositivo, pudiendo infectarlo o robarnos información. Para evitarlo, una vez hayamos terminado, **desactiva el Bluetooth**.

5.32. Diapositiva 32. Seguridad básica en redes

La seguridad de las redes inalámbricas de nuestros dispositivos es muy importante, pues por medio de ella, los ciberdelincuentes, de manera muy sencilla, podrían ver lo que hacemos en nuestros dispositivos o llegar a robarnos los datos personales.

A continuación, vamos a compartir una serie de medidas de seguridad que cualquier usuario puede empezar a implantar en sus equipos, principalmente desde nuestro *router*:

- **Modificar el nombre de la red wifi o (SSID)**: todas las redes cuentan con un nombre o SSID por defecto con el que se puede identificar el proveedor de Internet que tenemos contratado y/o al fabricante del *router* que tengamos instalado. Utilizando esta información un atacante podría llegar a saber cuál es la contraseña de acceso a la red wifi. Lo recomendable es cambiarla lo antes posible.
- **Desactivar WPS**: WPS es un mecanismo creado para facilitar la conexión de dispositivos a nuestra red wifi mediante un código de PIN de 8 dígitos. Esta opción puede facilitar el acceso a un atacante, por lo que lo más seguro es deshabilitarla.

Más información en: Guía para configurar el router wifi

5.33. Diapositiva 33. Seguridad básica en redes

- **Contraseñas de acceso y de administración**: la contraseña de acceso (perfil administrador) por defecto es muy fácil de adivinar en la mayoría de *routers*. Por ello, debemos modificar la contraseña para hacer de ella una clave robusta. Lo mismo ocurre con la contraseña de acceso a la red wifi.
- **Deshabilitar conexión remota**: Tampoco es seguro tener habilitada la administración remota. Esta función permite que podamos configurar el *router* fuera de nuestra red privada y para evitar que terceros puedan conectarse, lo mejor es deshabilitarla.

Más información en: Guía para configurar el router wifi

5.34. Diapositiva 34. Seguridad básica en redes

- **Cifrado**: los *router* disponen de distintos cifrados (WEP, WPA, WPA2) pero en la actualidad el más robusto y el que tenemos que habilitar en nuestro *router* es el cifrado WPA2-PSK.
- **Limitar conexiones, ancho de banda y tiempo de conexión**. Si vamos a compartir nuestra conexión, lo más seguro es llevar a cabo limitaciones en el número de conexiones a través de establecer un límite de direcciones IP que

nuestro *router* pueda manejar simultáneamente. También, es posible gestionar el ancho de banda que queremos que, por ejemplo, la red de invitados tenga disponible.
Y, finalmente, recuerda que, si estamos compartiendo nuestra conexión, podemos limitarla y desconectarla para evitar perder control sobre las actividades que se llevan a cabo.

Más información en: Guía para configurar el router wifi

5.35. Diapositiva 35. Seguridad básica en redes

Filtrado MAC: Otra buena práctica que podemos seguir es **revisar eventualmente los dispositivos que están conectados a nuestra red y realizar un filtrado por dirección MAC**. De esta forma, habilitaremos el acceso solo a aquellos dispositivos que conocemos. Existen varias formas de comprobar si tenemos un "invitado" en nuestra red. La dirección MAC actúa como un DNI del equipo y, aunque puede clonarse, nos otorgará una capa de seguridad extra:

- Lo primero será crear una lista blanca de dispositivos que vamos a permitir conectarse a la red.
- Para incluirlas en el filtro, deberemos recopilar las direccione MAC de estos dispositivos. Lo mejor es pedírsela a los usuarios que se quieran conectar o pedirles que se conecten para registrarlo.

La dirección MAC actúa como un DNI del equipo y, aunque puede clonarse, nos otorgará una capa de seguridad extra.

- Para conocer nuestra dirección MAC en **Windows**, accederemos a un intérprete de comandos MS-DOS como mostramos anteriormente y escribiremos **ipconfig /all** sin las comillas. En el apartado dirección física se encuentra la dirección MAC de nuestro dispositivo.
- Para conocer nuestra dirección MAC en **Apple**, abriremos **Preferencias del sistema** haciendo clic en el icono de la manzana de Apple situada en la esquina superior izquierda de la pantalla.
    - Seleccionaremos **Redes > AirPort o Ethernet incorporada**, según cómo nos hayamos conectado a Internet.
    - Si la conexión es Ethernet, haremos clic en **Avanzado > pestaña de Ethernet**. En la parte superior aparecerá la dirección MAC.
    - Si la conexión es AirPort, haremos clic en **Avanzado > pestaña de AirPort**. Ahí aparecerá la dirección MAC.

En cualquier *router* existe una opción para visualizar todos los dispositivos conectados a la red en tiempo real. Recuerda comprobarlo cada cierto tiempo e identificar aquellos dispositivos de confianza. Además, disponemos de aplicaciones que nos permiten hacer lo mismo a través de nuestros dispositivos.

Más información en: Guía para configurar el router wifi

5.36. Diapositiva 36. Seguridad básica en redes

Crear una red de invitados: No está disponible para todos los *routers*, pero si el nuestro lo permite es una opción muy interesante para compartir nuestra conexión a Internet en una red distinta a la que nosotros utilizamos. Para hacerlo, deberemos:

- Acceder a los ajustes de nuestro *router* y a nuestra dirección IP desde un navegador (suele ser 192.168.1.1). Si no lo sabemos, podemos consultarlo con nuestro proveedor de Internet (asegurándonos de que las credenciales para acceder a nuestro perfil de administrador son seguras).
- Una vez dentro, deberemos ir a la configuración de red inalámbrica y buscar Red para invitado. Es probable que los pasos varíen de un *router* a otro.
- Elegiremos un nombre y una contraseña segura para nuestra red de invitados, así como el método de autenticación (WPA2) y una red accesible para todos, por ejemplo, de 2,4 GHz.

Con esto ya tendremos una red para invitados lista. Debemos recordar desconectarla cuando terminen de utilizarla nuestros vecinos y amigos y cambiar la contraseña para futuras ocasiones.

Para el resto de las redes inalámbricas, la mejor medida de seguridad siempre va a ser apagar la red una vez hayamos terminado de utilizarla. Además, debemos tener cuidado con lo que compartimos, y no aceptar sincronizarnos o recibir archivos de desconocidos, ya que pueden contener *malware* con el que infectar nuestro equipo.

Más información en: Guía para configurar el router wifi

5.37. Diapositiva 37. En INCIBE te ayudamos

Mostramos la información de INCIBE prestando especial atención a la Línea de Ayuda en Ciberseguridad de INCIBE a través de la cual cualquier menor o adulto puede contactar de manera gratuita y confidencial cuando tengan una duda o un problema en Internet, llamando al número de teléfono 017 o enviando un mensaje a través de la página web https://www.incibe.es/linea-de-ayuda-en-ciberseguridad.

Animamos a los participantes a visitar las diferentes webs de INCIBE en función del público (Ciudadanos, Menores o Empresas) y a seguirnos en redes sociales.

Además, explicamos que en la web pueden encontrar mucha información y actividades para trabajar cualquier tema de ciberseguridad, juegos y recursos pedagógicos.

5.38. Diapositiva 38. Cuestionario de evaluación 1

Lo más recomendable a la hora de crear cuentas en un sistema es:

A. Crear 1 cuenta administrador.
B. Crear 2 cuentas de administrador.
C. Crear 1 cuenta de administrador por cada usuario.

5.39. Diapositiva 39. Cuestionario de evaluación 2

¿Para qué sirve tener un sistema actualizado?

A. Para solucionar posibles vulnerabilidades.
B. Para disponer de la última versión de nuestros programas favoritos.
C. Para mejorar el rendimiento de nuestro sistema.

5.40. Diapositiva 40. Cuestionario de evaluación 3

La herramienta que analizar y verifica las conexiones entrantes y salientes se conoce como:

A. *Firewall*.
B. Antivirus.
C. *Router*.

5.41. Diapositiva 41. Cuestionario de evaluación 4

¿Cuál de las siguientes opciones es una contraseña robusta?

A. M1contr4s3na.
B. 20101990
C. 1234567890

5.42. Diapositiva 42. Cuestionario de evaluación 5

¿Es correcto utilizar la misma contraseña para más de 1 cuenta?

No, nunca.

No, excepto si son cuentas secundarias.

Si, así evitamos olvidarlas.

5.43. Diapositiva 43. Cuestionario de evaluación 6

Las copias de seguridad nos ayudan a:

A. Proteger nuestra información en caso de pérdida, daño o robo.
B. Organizar nuestra información en la nube.
C. Mejorar la seguridad de nuestras cuentas.

5.44. Diapositiva 44. Cuestionario de evaluación 7

La regla del 3-2-1 hace referencia a:

A. 3 copias en 2 soportes diferentes y 1 en un lugar físico distinto.
B. 3 copias de seguridad en 2 carpetas distintas y 1 cifrada
C. 3 copias de seguridad en 2 soportes diferentes y 1 en la nube.

5.45. Diapositiva 45. Cuestionario de evaluación 8

Cuando vinculamos dos dispositivos entre sí habilitando una conexión inalámbrica hablamos de:

A. Bluetooth
B. Wifi
C. VLAN

5.46. Diapositiva 46. Cuestionario de evaluación 9

Estas en un centro comercial con red wifi gratuita, ¿cuál de las opciones es la más segura?

A. Desactivar la opción que permite al dispositivo conectarse automáticamente.

B. Conectarse, así se ahorran datos móviles.
C. Revisar las redes wifi disponibles y conectarte solo a la que tenga mejor señal.

5.47. Diapositiva 47. Cuestionario de evaluación 10

¿Qué harías si encontrases varios dispositivos desconocidos conectados a tu red wifi?

A. Ambas respuestas son correctas
B. Cambiar la contraseña de acceso al *router*, así como de conexión a la red wifi.
C. Bloquearlos y hacer un filtro de direcciones MAC.

5.48. Diapositiva 49. Final del taller

¡Gracias por vuestra atención!

6. RECURSOS DE EVALUACIÓN

Las herramientas de evaluación del alumnado permitirán controlar la calidad del aprendizaje recibido, gracias a una serie de **criterios de evaluación**:

1. **Participación durante el taller**. La participación del alumnado mediante dudas u otro tipo de aportaciones resulta de un gran valor evaluativo (10% de la evaluación final).

2. **Actividades**. Estas actividades situadas al final de la mayoría de los apartados son uno de los medios de mayor potencial para la asimilación de las competencias recogidas en el taller. Además, permitirá al docente recibir u feedback directo sobre la evolución del alumnado (25% de la evaluación final).

1	Configurar los usuarios en el dispositivo, ayudará a evitar que se le realicen modificaciones al sistema sin nuestra autorización, con lo cual la seguridad sobre el dispositivo mejorará, así que vamos a crear nuestro propio usuario y asegurémoslo con una contraseña robusta.
2	Un dispositivo actualizado es un dispositivo preparado para defenderse de todo tipo de virus y ataques al sistema. Tomemos unos minutos, accedamos a la configuración de nuestro dispositivo y asegurémonos que está actualizado a la última versión, así como el *software* que tengamos instalado.
3	Las herramientas de protección de nuestro sistema nos protegen de una gran variedad de riesgos. Quizás sea el momento de asegurarnos de que nuestras defensas están activadas. Vamos a entrar al sistema y comprobar que las herramientas mencionadas anteriormente están activadas y funcionando.
4	¿Tenemos una contraseña robusta? Si no estamos seguros, no pasa nada, más vale tarde que nunca. En el siguiente enlace encontraremos un recurso con el que poner a prueba nuestros conocimientos.
5	Tener una copia de seguridad de archivos y aplicaciones instaladas en nuestro ordenador, nos protegerá en caso de pérdida, ya sea por un fallo en el sistema, un descuido por nuestra parte o por un ciberataque. Así que dediquemos unos minutos a configurar nuestro sistema para que lo realice de manera automática.

3. **Cuestionario de evaluación**. Este instrumento de evaluación proporcionará gran parte de la puntuación final del alumnado y pondrá a prueba a los alumnos al finalizar un taller (65% de la evaluación final).

EVALUACIÓN FINAL = Participación + Actividades aprendizaje + Cuestionario de evaluación

6.1. Cuestionario de evaluación

El cuestionario de evaluación está compuesto por 10 preguntas de tipo test "opción múltiple" (3 opciones). La respuesta correcta está destacada en color verde.

1	Lo más recomendable a la hora de crear cuentas en un sistema es:	Crear 1 cuenta administrador.
		Crear 2 cuentas de administrador.
		Crear 1 cuenta de administrador por cada usuario.
	Feedback: La respuesta correcta es Crear 1 cuenta administrador. De este modo evitaremos que otros usuarios puedan instalar *software* malicioso o desactivar las medidas de seguridad.	
2	¿Para qué sirve tener un sistema actualizado?	Para solucionar posibles vulnerabilidades.
		Para disponer de la última versión de nuestros programas favoritos.
		Para mejorar el rendimiento de nuestro sistema.
	Feedback: La respuesta correcta es Para solucionar posibles vulnerabilidades. Una actualización permite solucionar posibles brechas en la seguridad o errores que los ciberdelincuentes podrían aprovechar.	
3	La herramienta que analizar y verifica las conexiones entrantes y salientes se conoce como:	*Firewall.*
		Antivirus.
		Router.
	Feedback: La respuesta correcta es *Firewall*. Este *software* analiza y verifica las conexiones para asegurarse de que no contienen agentes maliciosos.	
4	¿Cuál de las siguientes opciones es una contraseña robusta?	M1contr4s3na.
		20101990
		1234567890
	Feedback: La respuesta correcta es "M1contr4s3na.". Cumple con todos los parámetros de una contraseña segura, como tener más de 10 caracteres y ser una combinación de letras, números y caracteres especiales.	
5	¿Es correcto utilizar la misma contraseña para más de 1 cuenta?	No, nunca.
		No, excepto si son cuentas secundarias.

		Si, así evitamos olvidarlas.
	Feedback: La respuesta correcta es No, nunca. De este modo evitamos que si una cuenta es vulnerada, se vulneren el resto con las que comparte contraseña.	
6	Las copias de seguridad nos ayudan a:	Proteger nuestra información en caso de pérdida, daño o robo.
		Organizar nuestra información en la nube.
		Mejorar la seguridad de nuestras cuentas.
	Feedback: La respuesta correcta es Proteger nuestra información en caso de pérdida, daño o robo. Ya que no solamente nos protegen de terceros, también de un borrado de archivos accidental.	
7	La regla del 3-2-1 hace referencia a:	3 copias en 2 soportes diferentes y 1 en un lugar físico distinto.
		3 copias de seguridad en 2 carpetas distintas y 1 cifrada
		3 copias de seguridad en 2 soportes diferentes y 1 en la nube.
	Feedback: La respuesta correcta es 3 copias en 2 soportes diferentes y 1 en un lugar físico distinto. Además, es la mejor forma de asegurarnos de que siempre vamos a disponer de una copia de respaldo de nuestros archivos.	
8	Cuando vinculamos dos dispositivos entre sí habilitando una conexión inalámbrica, hablamos de:	Bluetooth
		Wifi
		VLAN
	Feedback: La respuesta correcta es Bluetooth. Este tipo de conexión inalámbrica permite la comunicación entre dos dispositivos para el intercambio de información. También permite vincular determinados dispositivos, como auriculares inalámbricos.	
9	Estás en un centro comercial con red wifi gratuita, ¿cuál de las opciones es la más segura?	Desactivar la opción que permite al dispositivo conectarse automáticamente.
		Conectarse, así se ahorran datos móviles.
		Revisar las redes wifi disponibles y conectarte solo a la que tenga mejor señal.

<table>
<tr><td></td><td colspan="2">Feedback: La respuesta correcta es Desactivar la opción que permite al dispositivo conectarse automáticamente. Así evitaremos conectarnos a una red que no queramos.</td></tr>
<tr><td rowspan="4">10</td><td rowspan="3">¿Qué harías si encontrases varios dispositivos desconocidos conectados a tu red wifi?</td><td>Ambas respuestas son correctas</td></tr>
<tr><td>Cambiar la contraseña de acceso al router, así como de conexión a la red wifi.</td></tr>
<tr><td>Bloquearlos y hacer un filtro de direcciones MAC.</td></tr>
<tr><td colspan="2">Feedback: La respuesta correcta es Ambas respuestas son correctas. Las dos opciones nos permitirán eliminar dispositivos desconocidos y asegurarnos de que no vuelvan a acceder a nuestra red.</td></tr>
</table>

ANEXO

RECURSOS PARA AMPLIAR

Se recomienda la lectura de la siguiente selección de recursos complementarios, por parte del docente:

- Desbloqueando el usuario de Windows.
- Cuentas de usuario en Windows 10.
- Las cuentas de usuario.
- La importancia de las actualizaciones de seguridad.
- Antivirus siempre activados y actualizados.
- Cómo nos protegen los antivirus
- Microsoft Defender: el antivirus de Windows a tu servicio
- Firewall de Windows.
- Usar cortafuegos en nuestros equipos ¿si, no, depende?
- Campaña ¡Contraseñas seguras!
- Campaña ¿Es seguro dónde guardas y cómo envías la información?
- Protégete al usar wifi públicas
- Guía para configurar el router wifi