**Ficha de formación**

|  |  |
| --- | --- |
| Título  | Ciberseguridad y protección de datos para operadores de EFP |
| Ref. DigCompEdu  | Área 6: Desarrollo de la competencia digital de los estudiantes |
| Palabras clave (meta tag) | Ciberseguridad, ciberdelito, antivirus, protección de datos, *phishing*, *spam*, Internet |
| Idioma | Español |
| Objetivos / Metas / Resultados de aprendizaje | * Conocer los peligros de Internet.
* Aprender a navegar de forma segura y evitar los ciberdelitos.
* Proteger nuestros datos de posibles ataques.
* Entender qué es un antivirus: criterios, tipos y opciones gratuitas.
 |
| Descripción | El mundo online ofrece una innumerable cantidad de recursos e información que nos pueden ayudar tanto en nuestro aprendizaje como en nuestro día a día. Sin embargo, también posee una serie de peligros que pueden comprometer nuestra seguridad. En este curso, aprenderás como identificar estas ciberamenazas, así como a evitarlas, protegiendo tu identidad y garantizando tu seguridad en Internet. |
| Contenidos organizados en 3 niveles | 1. **Ciberseguridad y protección de datos para operadores de FP**
	1. **Ciberseguridad**
		1. **Qué es la Ciberseguridad**

Desde el inicio de la pandemia, la formación profesional se ha volcado en el uso de recursos digitales, para adaptarse a esta nueva realidad a distancia. Así, ha aumentado la oferta de plataformas y formación telemática, pero sigue existiendo un desconocimiento generalizado en torno a los peligros que existen en Internet. Es por eso que es imprescindible formar a educadores y alumnos acerca de la ciberseguridad, la protección de datos y la navegación segura. Comprender los peligros y cómo evitarlos supone un desarrollo de la competencia digital de los profesionales, permitiendo una formación segura y un aprovechamiento óptimo de los recursos digitales. El mundo *online* posee ciertos peligros que pueden comprometer nuestra seguridad y conocer cómo evitar posibles fraudes, delitos y estafas. La ciberseguridad consiste en un conjunto de prácticas para defender los sistemas informáticos de los ciberdelitos. Esta abarca muchos ámbitos: seguridad en red, en *apps*, protección de datos… * + 1. **Peligros en Internet**

Para saber cómo evitar los posibles peligros, primero debemos conocerlos. Los riesgos más comunes en internet son:* *Spam:* Correos sin ningún tipo de interés o utilidad real. La mayoría de proveedores de correo tienen carpetas para este “correo basura” y opciones para enviar ciertos correos sospechosos directamente a dicha carpeta.
* *Phishing*: Correos electrónicos provenientes de una fuente aparentemente legítima que tienen el objetivo de robar información, dinero o introducir *malware*. Se pueden presentar ofreciendo un producto, servicio o un premio; o, por el contrario, amenazando con consecuencias o peligros de no cumplir con lo especificado en el mensaje. Recuerda: si es demasiado bueno para ser verdad, probablemente sea mentira (y potencialmente peligroso).
* Malware: Es la abreviación de *Malicious Software*. Es un programa o código diseñado para causar daños al sistema o usuario, ya sea mediante el robo de información, merma o alteración en la funcionalidad del software o eliminación de datos. En algunos casos, los atacantes exigen un pago a cambio de desbloquear dichos datos, archivos o accesos (*ransomware*).

Existen diversos tipos de *malware*: virus, gusanos, *spywares, botnets*… * Ciberacoso: Se trata de acoso realizado a través de la red. Mediante el uso de perfiles en las redes sociales, se difunden mensajes hostiles o contenido ofensivo para otros usuarios. Normalmente, aunque el agresor se esconda tras una cuenta falsa o anónima para ocultar su identidad, sigue siendo posible descubrirla. Es una práctica dañina que está creciendo entre los jóvenes.
* Piratería: Se entiende por piratería a la copia y distribución de contenido multimedia protegido por derecho de autor, siendo ilegal cuando se hace con ánimo de lucro. Esto puede perjudicar al creador del contenido, que, aunque llega a más público, no recibe dinero directamente por ello. Los usuarios también pueden verse perjudicados al descargar archivos de páginas poco seguras, pudiendo ser contenido falso o con *malware*.

Todos estos ciberdelitos pueden traer graves consecuencias: * Suplantación de identidad.
* Robo o “secuestro” de información.
* Daños en el equipo informático.
* Interrupción de las comunicaciones.
* Corrupción de archivos.
* Denegación de servicios.
* Daños personales.
	+ 1. **Consejos para mantener la seguridad en Internet**

Una vez conocemos los diversos peligros que existen en la red, podemos implementar una serie de medidas para mantener nuestra seguridad y proteger nuestra información. Aquí hay una serie de consejos que podemos seguir: * Mantén actualizado tu *software*, navegador y demás aplicaciones que tengan acceso a tu información.
* Valora tu privacidad. No compartas información personal en Internet.
* Desconfía de los enlaces y correos sospechosos (podríamos estar siendo víctimas de *phishing*). No abras correos electrónicos que se identifiquen como una empresa conocida, pero a la que no has proporcionado tu contacto o información. Un detalle que puede ayudarnos a detectar un mensaje falso son los errores de redacción y ortografía: una corporación oficial no comete estos errores. Además, los *scammers* (los que envían estos correos fraudulentos) suelen emplear un tono impersonal y evitan emplear nombres propios.
* No abras ningún enlace que se adjunte en correos no solicitados o con remitentes extraños. Podemos saber que una página es segura si empieza por https://, aunque tenemos que tener en cuenta que no todas las páginas seguras tienen contenido auténtico o válido.
* Infórmate antes de descargar archivos o instalar aplicaciones, pues es posible que puedan infectar tu dispositivo. Descarga información y archivos solo desde fuentes de confianza.
* Utiliza contraseñas seguras, con más de 8 caracteres y que combinen números, letras y símbolos. Evita emplear información personal (como tu nombre o tu cumpleaños). No escribas tus contraseñas en ningún sitio: la mayoría de plataformas ofrecen métodos de recuperación en caso de olvidarla.

En el siguiente enlace podrás comprobar la seguridad de tus contraseñas:* + - <https://password.kaspersky.com/es/>

De ser posible, configura un número máximo de intentos en tus cuentas, de esta forma bloquearás el acceso si algún extraño intenta acceder a tu perfil. Otra opción es la autenticación en dos pasos, que requiere otra verificación adicional, como por ejemplo desde el móvil. Esto último es especialmente útil cuando se accede desde dispositivos nuevos o inusuales. * Practica la netiqueta. La netiqueta es un conjunto de normas y consejos para garantizar una convivencia sana en la red. Esto incluye una comunicación educada, tratar a los demás como lo harías en la vida real y respetar el tiempo de otros usuarios.
	1. **Protección de datos**
		1. **¿Qué es la protección de datos?**

Todo dispositivo electrónico posee información y datos a proteger de los peligros de Internet, como por ejemplo datos personales, contraseñas de los perfiles, ubicación, dirección IP… Debido a esto, no solo debemos navegar seguros en Internet, sino proteger nuestro ordenador de toda amenaza externa….* + 1. **Consejos para la protección de datos**

Para asegurar que toda esta información confidencial esté protegida de cualquier ciberamenaza, podemos seguir una serie de consejos: * Instala un antivirus. Un antivirus es un programa que detecta *malware*, lo bloquea y elimina para evitar que infecte el dispositivo. En la siguiente sección, aprenderemos como escoger un antivirus.
* Ten copias de seguridad. Son imprescindibles para evitar perder nuestros archivos e información. Existen dos formas de almacenar nuestra copia de seguridad: en la nube (así será accesible en cualquier momento y lugar, y desde cualquier dispositivo) o en un disco duro externo. Es recomendable poseer ambas.
* Actualiza tu *software*. Tanto tu sistema operativo como tus aplicaciones deben mantenerse actualizadas para que puedan brindarte el mayor nivel de seguridad posible.
* Evita conectarte a redes wifi públicas o a dispositivos desconocidos. Desactiva la conexión automática, pues tus dispositivos podrían vincularse a redes extrañas sin que seas consciente.

Asegúrate de que sean 100% fiables antes de conectarte. De lo contrario, los ciberdelincuentes podrían acceder a tus datos e información. * Las redes wifi privadas o para uso personal deben ser configuradas. Cambia las contraseñas por defecto del *router* (pues son fáciles de hackear) y deshabilita la función de gestión remota. Para una mayor protección podemos permitir la configuración WPA2 o WPA3.

Una opción que garantiza proteger la conexión en la navegación son las VPN (*Virtual Private Network*). Este servicio permite encriptar los datos transmitidos a través de Internet; de esta forma resultarán inaccesibles a terceros y podremos evitar el robo de información. * Si sospechas que tu dispositivo ya ha sido infectado (por funcionamientos anómalos, como la aparición continua de ventanas de *spam*) evita emplear o transmitir información sensible hasta que tu dispositivo haya sido analizado y limpiado.
* Ten cuidado con lo que publicas. Las redes sociales son accesibles por todo el mundo, por lo que todo el mundo puede ver el contenido que publicas. Vigila los comentarios y fotografías que publicas, y evita revelar en ellas información personal como ubicaciones o contraseñas. La mayoría de redes sociales permiten configurar la privacidad de tu perfil para que solo aquellos usuarios que aceptes puedan ver tus publicaciones. Sin embargo, esto no implica que estés seguro: los ciberdelincuentes tienen medios para acceder a estas publicaciones sin tu permiso. La forma más segura de protección de proteger tu información, es que dicha información no esté si ocurre un ciberataque.
	+ 1. **Aprende a escoger un antivirus.**

Existen 4 tipos principales de antivirus: * Antivirus preventivo: Analizan todo el movimiento de datos para lograr detectar amenazas, por lo que previenen del *malware*.
* Antivirus identificador: Rastrean el dispositivo para lograr encontrar el *malware*. Buscan comportamientos anómalos dentro de archivos y programas.
* Antivirus descontaminador: Elimina el malware una vez el dispositivo ya ha sido infectado.
* Antivirus heurístico: Simulan la ejecución de diversos programas para detectar comportamientos anómalos de forma aislada, de modo que estudian su ejecución y la posible infección del malware sin que llegue realmente a realizarse.

Existen cientos de antivirus disponibles; sin embargo, no todos son iguales. A la hora de escoger el antivirus, hay una serie de criterios a tener en cuenta. * Compatibilidad: Hay programas y aplicaciones incompatibles con ciertos sistemas operativos. Lo mismo ocurre con el antivirus.
* Funcionalidad: Es importante que nuestro antivirus nos proteja del malware, además de permitir el correcto funcionamiento del dispositivo sin mermas en su rapidez, capacidad o rendimiento.
* Confiabilidad: Lee las reseñas de los usuarios. Ten cuidado, pues los antivirus falsos están muy extendidos.
* Actualizaciones frecuentes: Los peligros en Internet están en constante evolución, por lo que el antivirus también debe estarlo. De lo contrario, podemos estar expuestos a nuevas amenazas.
* Versatilidad: El antivirus debe ser capaz de analizar todo tipo de archivos, programas, redes y elementos susceptibles de ser infectados con *malware*.
* Capacidad de actuación: No solo es importante reconocer la localización o procedencia del virus, sino saber erradicarlo y limpiarlo de nuestro dispositivo.

Entre los antivirus gratuitos más empleados podemos encontrar: * Avast Free Antivirus

* Avira Antivirus

* Bitdefender

* Microsoft Defender

QLS-00004 Microsoft Defender - цена, описание, купить* ClamAV

* Kaspersky Security Cloud

* McAfee

* MalwareBytes

Malwarebytes Anti-Malware 4.5.9.198 - Descargar para PC Gratis |
| Autoevaluación (preguntas y respuestas de elección múltiple) | 1. ¿Cuál es un ciberdelito?
2. VPN
3. Avira
4. **Phishing**
5. ¿Qué debemos tener en cuenta al buscar un antivirus?
6. La compatibilidad
7. La confiabilidad
8. **Ambas son correctas**
9. ¿Qué debemos hacer si recibimos un enlace de un remitente que desconocemos?
10. Abrirlo y comprobar qué es
11. **No abrirlo y reportar el mensaje**
12. Devolver otro enlace
13. ¿Cómo podemos proteger nuestros datos?
14. Publicando contenido frecuentemente
15. Enviando mails con nuestra información a nuestros conocidos
16. **Manteniendo el software actualizado**
17. ¿Qué debe incluir una contraseña segura?
18. Información del usuario
19. **Mayúsculas, minúsculas, números y caracteres especiales**
20. Palabras verosímiles
 |
| Herramientas (directrices, buenas prácticas, checklist, lecciones aprendidas…) | Nombre  | Herramienta *Checklist* de ciberseguridad |
| Descripción | Una herramienta *checklist* diseñada para garantizar la seguridad digital de tu negocio de potenciales ciberataques y amenazas. |
| Nombre del archivo |  |
| Recursos (vídeos, enlaces de referencia)  |  |
| Material relacionado |  |
| PPT relacionado |  |
| Bibliografía  | <https://www.incibe.es/protege-tu-empresa/blog/el-ataque-del-man-middle-empresa-riesgos-y-formas-evitarlo> <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security> <https://www.ncsc.gov.uk/section/board-toolkit/home> <https://latam.kaspersky.com/resource-center/preemptive-safety/antivirus-choices> <https://blog.malwarebytes.com/cybercrime/2018/08/under-the-hoodie-why-money-power-and-ego-drive-hackers-to-cybercrime/> <https://protecciondatos-lopd.com/empresas/suplantacion-de-identidad/>  |
| Proporcionado por  | Internet Web Solutions |