**Ficha de formación JUST: Interactuar de manera segura en un entorno digital**

|  |  |  |
| --- | --- | --- |
| **Título** | Interactuar de manera segura en un entorno digital | |
| **Palabras clave** | Ciberseguridad, La Nube, Privacidad, Netiqueta | |
| **Proporcionado por** | Internet Web Solutions | |
| **Idioma** | Español | |
| **Objetivos** | Los objetivos de este módulo son **explicar la importancia** de mantener buenas **prácticas de ciberseguridad**, destacar la importancia de **proteger la información personal** y proporcionar una idea general de las **herramientas de ciberseguridad más prácticas y eficaces**. | |
| **Resultados de aprendizaje** | * Familiarizarse con la ciberseguridad: los protocolos son tan importantes como las aplicaciones. * Desarrollar de manera responsable: la netiqueta y el sentido común son especialmente importantes. * Saber cómo mantener la privacidad: ten mucho cuidado con lo que compartes en Internet. * Entender las herramientas de utilidad, como las VPNs, antimalwares y aplicaciones en la nube. | |
| **Área formativa** | **Protocolo empresarial** |  |
| **Habilidades digitales** | **X** |
| **Habilidades blandas** |  |
| **Smart Working** |  |
| **Índice de contenidos** | **Interactuar de manera segura en un entorno digital**  **Unidad 1: Trucos y consejos de ciberseguridad**  Sección 1.1: Introducción  Sección 1.2: Mantente actualizado  Sección 1.3: ¡Utiliza copias de seguridad!  Sección 1.4: Contraseñas y autenticaciones multifactor  **Unidad 2: Prácticas seguras**  Sección 2.1: Protege tu intimidad  Sección 2.2: Cuida tu netiqueta  **Unidad 3: Herramientas para mejorar la seguridad de las TIC**  Sección 3.1: VPNs  Sección 3.2: Antimalware  Sección 3.3: Nube | |
| **Contenido de formación** | **Interactuar de manera segura en un entorno digital**  **Unidad 1: Trucos y consejos de ciberseguridad**  **Introducción**  Vivimos en un mundo cada vez más interconectado. Esto comprende el sentir la necesidad de compartir lo mejor de nuestro último viaje en nuestro círculo de Instagram, o desplazar el tema del ocio al trabajo, cada llamada o intercambio de correos electrónicos en los que participamos durante nuestra vida educativa y/o laboral.  Sin saberlo, estos intercambios de información contienen multitud de datos sobre nosotros, a menudo sensibles, que pueden ser robados y recopilados por personas que quieren aprovecharse ilegalmente de ellos.  Por eso, contar con protocolos o simplemente prácticas de ciberseguridad (que no sólo significa instalar un antivirus y luego dejar de preocuparse) es fundamental para nuestra vida online.  **Mantente actualizado**  Nuestros dispositivos suelen molestarnos con incómodas notificaciones de "nueva actualización de software". A pesar de que a veces no cambian nada a primera vista, estas actualizaciones son muy útiles, ya que parchean errores y problemas de seguridad descubiertos recientemente que podrían suponer un riesgo para nuestros dispositivos y la información que contienen.  Sin embargo, estas actualizaciones de software podrían durar poco, ya que los hackers (o piratas informáticos) siempre están al acecho para encontrar vulnerabilidades de software, lo que subraya la importancia de mantener nuestros dispositivos actualizados.  **¡Utiliza copias de seguridad!**  Mantener una copia separada y adicional de tus archivos es una apuesta segura cuando, a pesar de nuestros esfuerzos, ocurre lo peor y los archivos se corrompen o nuestro sistema sufre un ciberataque. Para evitarlo, nuestros archivos pueden almacenarse de forma segura en un disco externo y/o en aplicaciones online en la nube.  Contrariamente a la creencia común, las versiones de copia de seguridad deben crearse durante el proceso de elaboración y no sólo una vez finalizado el archivo. De este modo, se puede volver fácilmente a iteraciones anteriores del archivo en caso de que algo vaya mal a mitad del borrador.  **Contraseñas y autenticaciones multifactor**  A menudo olvidadas, las contraseñas son una parte vital de la ciberseguridad. A pesar de la molestia que supone recordarlas e introducirlas, las contraseñas perfectas, largas y con tantos tipos de caracteres como sea posible son imprescindibles. Ni que decir tiene que utilizar tu fecha de nacimiento (y similares) no es una opción.  Además, debido a las frecuentes brechas de seguridad, las contraseñas pueden verse fácilmente comprometidas, así que mantén contraseñas diferentes en cada dispositivo o cuenta, ¡y recuerda cambiarlas con regularidad!  La autenticación multifactor es un sistema que dificulta la tarea de los ciberdelincuentes al exigir credenciales adicionales a la contraseña para acceder a su cuenta, por ejemplo, un código SMS, una llamada o el uso de una aplicación específica.  **Unidad 2: Prácticas seguras**  **¡Protege tu intimidad!**  Tendemos a asociar la ciberseguridad con piratas informáticos que utilizan herramientas de última generación para entrar en nuestras cuentas. La verdad es que la mayor parte de su éxito proviene de googlear y recopilar "información pública" de las redes sociales, blogs y foros.  De este modo, si nos gusta utilizar para nuestras contraseñas una combinación del nombre de nuestra mascota, el apellido de nuestra madre, el número de la puerta, etc., es cuestión de tiempo que un hacker pueda reunirlo todo de aquí y de ahí, recombinarlo y vulnerar la seguridad.  Reconsidera qué significa para ti "información privada". Vuelve a tu(s) línea(s) de tiempo, busca cualquier foto de tu DNI/tarjeta de crédito/documentos personales (podrían ser despedidas, agradecimientos o mensajes de burla) y bórralas. Presta atención también a los perfiles que contengan demasiada información personal innecesaria.  Recuerda: si no quieres que la información sea vista por extraños, ¡no la publiques!  **Cuida tu netiqueta**  La “netiqueta” es un conjunto de normas de cortesía diseñadas para facilitar la convivencia online, igual que tenemos convenciones sociales para el mundo offline, como saludar con la mano o decir “por favor”.  Además, como en la vida real, ten en cuenta que este código de conducta no es inmutable y depende del contexto. Un buen ejemplo de ello es el conjunto de normas que suelen pegarse en los grupos o foros de Facebook.  Las reglas de "netiqueta" originales de Virginia Shea (1994) siguen siendo válidas con algunas actualizaciones, como en el siguiente ejemplo:   * Evita utilizar las comunidades en Internet como sustitutos de Google. Básicamente, intenta buscar entradas o hilos anteriores que ya hayan respondido a la cuestión. * Restringe el uso de signos de puntuación adicionales, abreviaturas, emojis, mayúsculas y grafías alternativas – XQ NAD13 K13R3 L33R M3NSAJ3S AS1, vd???? 😃😃😃 * No hagas spam de tus propios productos o servicios – Normalmente, hay espacios separados y específicos para ello. Si no los ves, es que no estás en el lugar adecuado. * No envíes información personal o privada – Consulta la sección anterior. * Da el debido crédito a los autores – No sólo desde el punto de vista legal, sino también porque, aunque la gente odia que la plagien, le encanta que compartan su trabajo.   **Unidad 3: Herramientas para mejorar la seguridad de las TIC**  **VPNs**  No todo van a ser medidas, normas y hábitos. Afortunadamente, existen multitud de herramientas diseñadas para combatir las ciberamenazas como VPNs, Antimalware y aplicaciones en la nube.  Las VPN son filtros que enmascaran la identidad en Internet y cifran los datos. Para ello, se conectan a un servidor privado que codifica los datos, bloqueando el acceso externo a ellos y haciéndolos ilegibles en caso de robo.  Además, la mayoría de las VPN tienen servidores en varios países, lo que significa que tenemos muchas opciones para disfrazar nuestra IP de extranjera y acceder a contenidos geobloqueados no disponibles en nuestro país:   * NordVPN y Access son dos opciones de pago razonables que nos permiten navegar con seguridad. * Además, Surfshark y Tunnelbear también ofrecen planes gratuitos atractivos y fiables.   **Antimalware**  A pesar de ser comúnmente llamado "Antivirus", el software Antimalware está diseñado para detectar, poner en cuarentena y eliminar cualquier amenaza cibernética, no sólo virus.  Mientras que los virus están diseñados para replicarse y hacer que los dispositivos funcionen mal, el malware es un término general para cualquier tipo de software malicioso que difunde spam y anuncios y roba información y contraseñas (¡e incluso puede pedir un rescate!).  Hoy en día, es cierto que la mayoría de los software antimalware disponen de una aplicación antivirus y viceversa, con una gran variedad de funcionalidades y modalidades:   * En cuanto a las opciones de pago, destacan ESET, Norton y Avast. * Además, las versiones gratuitas de Malwarebytes y Bitdefender también ofrecen un servicio de primera clase.   **Nube**  “La Nube" es un servicio de alojamiento online que permite a los usuarios subir, modificar, almacenar y compartir sus archivos.  Almacenar los ficheros online en servidores privados salvaguarda dichos archivos frente a cualquier ataque local o corrupción, además de evitar problemas con los discos duros físicos como falta de espacio, pérdidas o deterioro. A pesar de su nombre, "la Nube" no es una entidad única, sino que cada proveedor tiene la suya propia y por eso hay varias opciones:   * Dropbox, una opción popular a pesar de virar hacia los planes de pago, ofrece un plan gratuito de 2 GB. * Con 5 GB y 15 GB respectivamente, OneDrive de Microsoft y Google Drive también ofrecen una integración total en sus entornos. * Por último, aunque se utiliza principalmente para compartir archivos, MEGA permite a los usuarios gratuitos almacenar hasta 20 GB. | |
| **Glosario** | **Copia de seguridad**: Copia digital de un archivo almacenada por separado y utilizada en caso de que el original se pierda o se dañe.  **Autenticación multifactor:** Una modalidad de acceso que exige presentar dos o más pruebas para mayor seguridad.  **VPNs:** Filtros que enmascaran tu identidad online y cifran tus datos. Para ello, se conecta a un servidor privado que codifica tus datos, bloqueando el acceso externo a ellos y haciéndolos ilegibles en caso de robo.    **Antimalware:** Software diseñado para detectar, poner en cuarentena y eliminar cualquier ciberamenaza, no sólo virus.    **Nube:** Servicio de alojamiento en línea que permite a los usuarios subir, modificar, almacenar y compartir sus archivos, lejos de ataques locales o corrupción. | |
| **Autoevaluación (preguntas y respuestas tipo test)** | 1. La netiqueta no aboga por:   1. Buscar respuestas anteriores que puedan ayudarte. 2. **Utilizar muchas abreviaturas.** 3. Dar el debido crédito a los autores.   2. Postear información personal es lo más seguro si:   1. Se publica en privado. 2. **No se publica.** 3. Se sube a la nube.   3. Los hackers recopilan la mayor parte de la información sobre los usuarios medios a través de:   1. **Buscar sus nombres en Google.** 2. Utilizar software sofisticado. 3. Extorsionar.   4. ¿Es lo mismo un virus que un malware?   1. Sí, son sinónimos. 2. En absoluto. 3. **Los virus son solo un tipo de malware.**   5. ¿Cuál tiene más espacio?   1. Google Drive 2. Dropbox 3. **Mega** | |
| **Bibliografía** | * <https://www.ionos.es/digitalguide/online-marketing/redes-sociales/netiquette/#:~:text=Este%20t%C3%A9rmino%20hace%20referencia%20a,t%C3%A9rmino%20netiqueta%2C%20su%20traducci%C3%B3n%20directa> * <https://www.avast.com/es-es/c-malware-vs-virus#:~:text=%C2%BFCu%C3%A1l%20es%20la%20diferencia%20entre,que%20un%20tipo%20de%20malware> * <https://www.trellix.com/en-au/security-awareness/ransomware/malware-vs-viruses.html#:~:text=Malware%20is%20a%20catch%2Dall,its%20code%20into%20other%20programs> | |
| **Recursos (vídeos, enlace de referencia)** |  | |