AF4: Seguridad en la red

Cómo proteger la red. Robo de datos

Digitalización aplicada al sector productivo.
Módulo formativo sobre competencias digitales transversales básicas.

Gobierno de España · Ministerio de Educación y Formación Profesional
Plan de Recuperación, Transformación y Resiliencia
AxFP Alianza por la Formación Profesional
Financiado por la Unión Europea NextGenerationEU

Proyecto financiado por el Ministerio de Educación y Formación Profesional - *U.E. Next Generation*

Índice

1. INICIO

1.1 Introducción

La seguridad de la información es una labor de todas las personas que usan los medios informáticos.

Las relaciones personales y profesionales se enfrentan día a día a los mismos riesgos: filtración, robo o extravío de información. Utilizar claves seguras, poner barreras informáticas y proteger los datos son algunas de las medidas que en estos tiempos todas las personas deberían conocer.

Crear hábitos, organizar medidas de seguridad, formar al personal y entregar herramientas de calidad son algunos de los medios que las organizaciones, empresas o instituciones deberían ofrecer a su personal, y así poder resguardar la información que manejan.

La organización "Un mundo mejor" donde nuestra protagonista es trabajadora social ha dispuesto diversas medidas con el fin de interiorizar algunos modos de seguridad en el uso de claves, conexiones y protección de datos y, de esta forma, mantener la información custodiada en todo momento.

En esta Unidad Didáctica Marta conocerá los temas relacionados con el cuidado y la seguridad de las contraseñas, el trabajo con dispositivos compartidos, las medidas de seguridad en el entorno físico laboral y las sugerencias para establecer un desempeño seguro en plataformas digitales. Se revisarán también las propuestas de tareas compartidas, así como, el empleo de dispositivos con **certificados digitales**. Para acabar, se proporcionará información sobre la seguridad en las redes wifi y las estrategias para poder usarlas con precaución.

Os damos la bienvenida a esta nueva unidad.

¿Qué vas a aprender en esta unidad?

OBJETIVO GENERAL DE LA ACCIÓN FORMATIVA

- Proteger la información y datos personales; proteger la identidad digital, de los contenidos digitales y de las aplicaciones informáticas; conocer las medidas de seguridad, así como el uso responsable y seguro de la información digital.

OBJETIVOS ESPECÍFICOS DE LA UNIDAD DIDÁCTICA

- Identificar formas de proteger dispositivos y contenidos digitales, diferenciando riesgos y amenazas en entornos digitales.
- Conocer medidas de seguridad y protección, identificando formas de asegurar la fiabilidad y la privacidad.
- Identificar cómo compartir información personal identificativa sin exponerse a uno mismo ni a terceros a riesgos.
- Conocer las políticas de privacidad sobre cómo se trata la información personal que se utiliza en servicios digitales.

2. MECANISMOS DE SEGURIDAD

2.1 Contraseñas en dispositivos personales.

En el mundo digital son enormemente valiosos los datos sobre usuarios y usuarias: contraseñas, correos electrónicos, identificación personal...

Para las empresas el robo de los datos que custodian es, posiblemente, **una de las cuestiones que más puede dañar su reputación**, por eso el cuidado de dichos datos es una prioridad. A continuación, podrás ver un ejemplo de un reconocido caso que da cuenta de ello:

Robo masivo de datos a Uber

En 2017, se dio a conocer el robo de datos a 57 millones de usuarios y usuarias de la empresa de transporte Uber en Estados Unidos y que había ocurrido un año antes. Como la aplicación requiere una gran cantidad de información personal de quienes la utilizan, al apropiarse de estas bases de datos, piratas informáticos lograron obtener 25,6 millones de nombres y direcciones de correo, 22,1 millones de números de teléfono y 607.000 licencias de conducir.

La compañía creyó que podría ocultar el robo de datos pagando 100.000 dólares a los hackers, pero no fue así y tuvo que pagar una multa de 148 millones de dólares. La compañía también despidió a las personas responsables de seguridad que ocultaron el robo de los datos.

Los datos son valiosos para cualquier persona u organización que quiera operar con ellos de forma ilícita, pero también para desarrollar campañas publicitarias, establecer estrategias de marketing o prever tendencias de mercado. Por esa razón, podemos decir que los DATOS son el nuevo PETRÓLEO.

Tanto en el entorno personal como en el entorno laboral es **necesario convertir en costumbres algunas prácticas que pueden mejorar la seguridad.** En la mayor parte de las ocasiones, estas pérdidas de datos se producen por incumplir las normas de seguridad con conductas que es necesario evitar.

Algunos de esos hábitos están relacionados con la forma de elegir y guardar contraseñas; otros, con el uso que se hace de los dispositivos.

El uso de ordenadores compartidos en el trabajo de Marta es algo muy común, ya que la ONG no tiene los suficientes recursos para otorgar un dispositivo a cada persona. Esto puede convertirse en una brecha de seguridad importante si no se toman las medidas adecuadas.

No solo las personas deben gestionar el buen uso de las contraseñas, la organización o la empresa también tienen la responsabilidad de asegurar los datos que almacenan.

Es debido a ello que resulta tan importante aprender a crear y proteger las contraseñas para evitar que sean robadas.

Errores más comunes en la gestión de contraseña

Te has dado cuenta de que, en muchas ocasiones, la elección de una contraseña no viene motivada por la seguridad sino por otras situaciones. Entre ellas encontramos dos cuestiones:

- Que sea fácil de recordar.
- Que sea fácil de introducir en el dispositivo.

A continuación, podrás identificar algunos de los errores más comunes que se cometen al gestionar las contraseñas.

Paso 1:

Cuando una contraseña es **fácil de recordar**, suele ser también **fácil de adivinar**. Sobre todo, si está compuesta por **combinaciones de datos personales o familiares**.

Este tipo de contraseñas (fechas de cumpleaños o aniversarios, matrículas…) son, normalmente, las que primero se prueban en un ataque.

Paso 2:

Aunque parezca extraño que alguien pueda tener como contraseña la palabra “contraseña” o “123456”, se ha descubierto en las filtraciones que estas son las contraseñas más comunes.

Paso 3:

Por otro lado, si se realizan combinaciones simples de letras y números, incluso secuencias, será sencillo un ataque de prueba masiva.

Estos ataques se conocen como **"ataques de fuerza bruta".** Lo que hacen quienes practican la ciberdelincuencia, con la ayuda de diversas herramientas, es probar el mayor número de combinaciones posibles hasta dar con la contraseña correcta.

Ranking de las peores contraseñas o "las más evidentes"

Has visto cuáles son las contraseñas más comunes y que son una puerta abierta para los ciberdelincuentes. Observa el siguiente ranking de las peores contraseñas que puedes utilizar:

1. 12345123456
2. Password (contraseña)
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. football (fútbol)
8. 1234
9. 1234567
10. Baseball (béisbol)

Consejos para mejorar la seguridad de las contraseñas

Criterio de seguridad
Usa contraseñas con el **mayor criterio de seguridad posible**. Se deben **evitar** referencias personales, nombres de mascotas, nombres de familiares o fechas de cumpleaños.

No apuntar las contraseñas en ningún espacio visible
Si el número de contraseñas es elevado, es conveniente que **utilices alguna estrategia** que te permita tener la certeza de que nadie podrá tener acceso al lugar donde las almacenas.

Utilizar la verificación en dos pasos
La mayor parte de los servicios proponen la activación, incluso por defecto, de esta verificación. Esto permite darle un plus de seguridad a la cuenta, ya que se introduce también la necesidad de escribir un **código de confirmación** que ha sido enviado al teléfono móvil u otro dispositivo con el que estemos trabajando.

Usar distintas contraseñas para los diferentes servicios
Aunque sea complicado recordar varias, **no debes usar la misma contraseña para los diferentes servicios que utilices**. Una vez que la entrada en una plataforma en línea es vulnerada usando una contraseña, inmediatamente quienes hayan concretado esta acción probarán con la misma clave en el resto de los servicios.

Recomendaciones de seguridad

Para tener la certeza de que la contraseña es robusta y puede resistir un ataque de "fuerza bruta", se debe intentar que dicha contraseña siga estas recomendaciones.

Extensión de la contraseña
Utilizar un mínimo de ocho caracteres.
Las contraseñas cortas son más vulnerables.

Mayúsculas y minúsculas
Conviene combinar mayúsculas y minúsculas para dificultar su descifrado.

Contraseñas comunes
No utilizar cadenas de letras que se repitan, por ejemplo "asdfasdf".
Evita también el nombre de tu mascota, fechas importantes para ti o códigos postales.
Tampoco hagas cambios obvios como un 3 por una e o un 0 por una o.

Caracteres especiales
Utilizar caracteres especiales, como “-“, “_”, “+”.

Combinar números y letras
Utilizar números además de letras añade dificultad a las vulnerabilidades.

No reutilizar las contraseñas
No reutilizar las mismas contraseñas en más de una web ni cambiarlas secuencialmente (siempre las mismas), y menos si el cambio es una numeración consecutiva.

2.2 Seguridad en dispositivos compartidos

Uno de los riesgos más comunes en los espacios de trabajo es el uso de dispositivos compartidos.

En muchos espacios de trabajo se comparten ordenadores, discos duros **USB**, impresoras o discos online para copias de seguridad. Esto implica una serie de elevadas **brechas de seguridad**, no tanto por el diseño de las estrategias tecnológicas sino por el factor humano en su uso.

Lo lógico, cuando se utiliza cualquier dispositivo compartido, es **abrir y cerrar la sesión**. Lo normal es que gran cantidad de usuarias y usuarios se olviden de cerrar la sesión, y esto permite que cualquier otra persona que utilice ese ordenador pueda acceder a la información de su cuenta. Tal es el caso de una colega de Marta, quien dejó el ordenador encendido y un informe abierto minimizado en el escritorio sin darse cuenta.

Muchos servicios de Internet incluyen accesos a otra serie de aplicaciones online con la misma cuenta. Esto presenta un problema: si una persona se ha dado de alta en diversos servicios utilizando una cuenta de correo, y esa cuenta de correo se ve comprometida, todos los servicios a los que dé entrada dicha cuenta estarán comprometidos también.

Bloqueo de dispositivos

Es importante que los dispositivos estén siempre bloqueados cuando no se utilicen, de forma que solamente puedan usarse cuando lo indique quien gestiona el dispositivo.

De la misma forma, la contraseña que da acceso al ordenador (o a los distintos perfiles dentro del mismo) debe ser guardada con mucho cuidado. **Nunca ha de facilitarse a nadie esa contraseña**, cuestión que no siempre se cumple cuando se debe realizar una gestión rápida con un dispositivo. **Si en algún momento se ha dado, o se sospecha que otra persona puede haber visto la contraseña del perfil, conviene cambiarla cuanto antes.**

También se pueden presentar conflictos sobre los **dispositivos de escaneado e impresión**. Si dichos dispositivos hacen uso de memorias USB, suele ser bastante común que dichas memorias se queden olvidadas en la máquina. Si se han de usar este tipo de memorias es altamente recomendable que tengan solo lo necesario para el uso que se desea hacer de ellos.

En el caso de que en estos dispositivos se guarde información confidencial y sensible, deben utilizarse USB con contraseña.

Seguridad en espacios físicos

Cuando se trabaja en entornos compartidos por necesidades laborales o personales, hay que cuidar la seguridad de nuestros equipos y de la información que tenemos en ellos.

Cuando estemos en un espacio compartido de la organización o empresa para la que trabajamos (oficinas, almacenes, tiendas, etc.) debemos conocer y respetar las normas y protocolos de seguridad que se hayan establecido.

En los espacios compartidos que usemos por motivos personales (por ejemplo, coworkings o cibercafés) también hay que conocer las normas de seguridad informática del lugar por nuestro propio interés.

En todos los casos es bueno utilizar estrategias de prevención como las que te indicamos a continuación.

Uno de los espacios donde más información relevante se suele introducir son los tablones de anuncios, o los tablones con documentos usuales de trabajo. En dichos tablones, de forma ocasional, pueden incluso encontrarse listados de contactos, así como referencias personales de los distintos departamentos. Estas actuaciones hacen posible que cualquier persona que deba esperar, durante unos minutos, en una zona próxima a dicho tablón pueda acceder a datos restringidos.

Cualquier espacio con datos reservados **ha de estar en un entorno donde no se reciban visitas externas**. Es mucho más conveniente tener un listado que se guarda bajo llave

que utilizar un tablón para dejar ese tipo de datos. Aunque ralentice los procesos de trabajo, debemos tener rigor ante estas actuaciones para evitar problemas mayores.

Códigos QR con contraseñas

Otra cuestión común es tener carteles o **códigos de realidad aumentada** con las contraseñas de red. Aunque esta dinámica puede facilitar el flujo de trabajo, es conveniente que esa información no esté tan a la vista.

Consejos para mantener la seguridad de la información en los espacios de trabajo

A continuación, te presentamos algunos consejos para proteger la información en los espacios de trabajo, ya que, **si una persona obtuviera acceso a la red, podría tener también la posibilidad de intervenir en los dispositivos de la misma**, sobre todo si existieran sistemas de carpetas compartidas.

Así pues, si se quiere mantener una seguridad adecuada, es importante recordar estas cuestiones.

Alertar de pérdidas de información o extravío

En caso de extravío de algún dispositivo, avisar rápidamente a quienes estén a cargo de la seguridad para que puedan actuar cuanto antes.

Bloquear dispositivos electrónicos

Al salir del puesto de trabajo, bloquear la pantalla del ordenador presionado las teclas Windows + L. De este modo, se protege el ordenador de miradas indiscretas y accesos no permitidos.

Destruir documentación obsoleta

Si hubiera documentación que ya no sea necesaria, destruirla o depositarla en los espacios habilitados para que esto ocurra de manera controlada y segura.

Guardar bajo llave los dispositivos de almacenamiento externo

Aquellos dispositivos de almacenamiento externo susceptibles de contener datos sensibles deben mantenerse bajo llave, y así evitar que alguien pudiera llevárselos sin permiso.

Denegar el acceso a personas desconocidas

No permitir el acceso a los dispositivos a personas desconocidas o ajenas al equipo de trabajo, sin solicitar permiso expreso a quienes gestionan la seguridad.

Estar atentos a la documentación

No olvidar documentación en espacios ajenos (oficinas de colegas, transporte público, cafetería,) o en los sistemas de reproducción como la fotocopiadora, impresora o escáner.

Salvaguardar la información

No dejar contraseñas o datos personales a la vista, pegadas en post-it, en libretas o agendas que queden al alcance de otras personas.

Proteger información de la empresa

Para evitar pérdidas o extravío de información, se debe evitar extraer información de la empresa en cualquier tipo de almacenamiento o soporte (papel, digital o correo electrónico).

Evitar carteles con contraseñas

Evitar poner **carteles con redes y contraseñas**, salvo que sean para el uso de invitados. En este caso, las redes deben ser independientes.

No exponer datos personales

No se deben dejar nunca **datos personales expuestos** en espacios públicos, salvo que sea un requisito normativo.

Recuerda...

El espacio de trabajo ha de estar lo más organizado posible. Tener a la vista datos laborales puede generar una importante brecha de seguridad, especialmente en aquellos casos en los que se trabaja de cara al público.

2.3 Accesos, permisos y gestión de credenciales

El acceso a los espacios, tanto físicos como digitales, es una de las áreas sobre las que más se debe reforzar la seguridad.

Los accesos físicos deben ser revisados de forma periódica, ya que los protocolos deben cumplirse siempre si se quiere garantizar la seguridad necesaria en el acceso a los espacios de trabajo.

Los entornos digitales deben tener también un buen sistema de verificación, es decir deben tener un proceso mediante el cual **cualquier persona se identifica con sus credenciales dentro de un sistema**, normalmente a través de un **nombre de usuario o usuaria y una contraseña.**

¿Sabías que...?

El objetivo fundamental de una verificación o autenticación es que se compruebe que el usuario o la usuaria es quien dice ser.

Objetivos de los controles de acceso

Así como debemos comprobar quienes somos y verificar nuestra identidad, existen otros objetivos por los que se controla el acceso a los diversos espacios. Aquí destacamos los siguientes:

1. Identificar y seguir los accesos realizados, de forma que sea posible monitorear todo el proceso estableciendo controles internos.
2. Hacer un seguimiento y documentar todos los accesos que se realizan.
3. Establecer una ordenación de permisos clara para toda la organización, estableciendo diferentes escalas de privilegios según el cargo o las funciones que existen dentro de la empresa.

En el caso de que la autenticación se realice por contraseña, es fundamental que **dicho nombre de usuario o usuaria y dicha contraseña sean conocidos exclusivamente por la persona interesada.**

Si se produce cualquier problema de seguridad, la responsabilidad caerá primero sobre la persona con las credenciales con las que se haya producido dicha intromisión o robo de datos.

Existen otras formas de verificación o autenticación, como la documental (se realiza mediante DNI o permiso de conducir) y la biométrica (que implica la posibilidad de usar huellas digitales o escaneo facial).

Una vez que se ha realizado la **autenticación** se desarrolla **el control de acceso**. Esta acción consiste en decidir si la persona tiene permiso para poder acceder o no.

Normalmente, en el control de acceso es donde se darán **diferentes tipos de permisos para distintos entornos digitales**. De esta forma, cada persona puede tener privilegios distintos, por lo que podrá acceder a determinados datos y no podrá acceder a otros.

En la ONG "Un mundo mejor" han logrado mejorar su seguridad controlando el acceso a todos los dispositivos que utilizan las personas que trabajan y están revisando también la opción de incluir control de acceso en sus espacios físicos.

Ejemplo: robo de credenciales de Dunkin' Donuts

Los ataques a grandes y pequeñas empresas son cada vez más frecuentes. Uno de los ataques más famosos fue el robo de credenciales a la empresa Dunkin' Donuts que después, se utilizaría para acceder a las usuarias y los usuarios de su programa de fidelización DDPerks.

Este robo se debió a una fisura en la brecha de datos de una de las empresas proveedoras de la compañía.

Quienes realizaron este ataque también utilizaron los datos para acceder e iniciar sesión en otras plataformas de la marca que tenían las mismas credenciales.

Este caso supuso un problema de credibilidad, seguridad y reputación para la marca, que se vio afectada económicamente.

3. TRABAJO SEGURO EN PLATAFORMAS DIGITALES

3.1 Espacios web compartidos

Cualquier fallo de seguridad implica una intromisión. Y esta intromisión, tanto si se realiza para ver documentos como si se lleva a cabo para acceder a carpetas digitales, suele propiciarse por descuidos de seguridad.

La información debe ser custodiada en todo momento tanto en los dispositivos externos como los que utilizamos en Internet. Mantener el orden y confidencialidad de aquellos documentos sensibles y emplear contraseñas sólidas ayudan asegurar la calidad de nuestras conexiones.

Carpetas y documentos

De la misma forma que se debe cuidar la entrada a los espacios de trabajo de personal no autorizado, también han de cuidarse los accesos que se dan a los documentos y a las carpetas en línea. Marta, por ejemplo, ha conocido la posibilidad de poner contraseña a sus documentos en línea, lo que ayuda a proteger un poco más la información.

Hay momentos en los que hace falta consultar información de otras áreas, pero esa información puede ser usada **solamente durante el tiempo necesario.** Por desgracia, en muchas ocasiones ese acceso a carpetas compartidas no siempre se llega a cerrar.

Con ello, se crean vías adicionales para la consulta de datos sensibles. Una de las acciones que se debe cuidar, por tanto, es la de mantener esos accesos **digitales solo durante el tiempo rigurosamente necesario.**

Las aplicaciones y programas también pueden ayudarnos a hacer este tipo de control sobre la información. Mira el siguiente ejemplo.

Compartir archivos temporalmente en Google Drive

Con una cuenta de pago de Google Suites se puede compartir un archivo en Drive y fijar una fecha de caducidad de acceso para establecer un plazo máximo en que la persona con la que se ha compartido podrá seguir utilizándolo. Ahora con una cuenta estándar de Google esta operación no es posible realizar.

Para quienes tienen este tipo de cuenta es necesario dirigirse al apartado "**Compartir**" del archivo compartido y presionar la flecha que aparece junto al nombre de la usuaria o el usuario. Allí aparecerá la opción "**Dar acceso**

temporal", desde la cual se podrá establecer la fecha en que caducará el acceso. Si la persona tenía un rol de edición, automáticamente perderá estos permisos, pero podrá continuar visualizando y comentando el archivo.

Recuerda...
Las carpetas y los documentos compartidos han de gestionarse con cuidado para evitar brechas de seguridad con los datos.

Discos duros en línea

Tener un disco duro permite compartir recursos fuera de la nube, manteniendo la seguridad de los datos siempre y cuando se tomen las medidas necesarias.

Emplear un disco duro es una opción muy extendida cuando se debe trabajar con documentos de gran volumen o material multimedia. Es importante destacar que existen discos duros externos en los que puedes almacenar tu información y trasladarla personalmente y otros que están almacenados en internet donde puedes gestionar los datos en línea.

Estas unidades virtuales funcionan de manera similar a los dispositivos físicos y no es necesario llevarlos contigo todo el tiempo. Puedes almacenar o descargar información desde cualquier ordenador y solo necesitas conexión a internet. El uso de este tipo de dispositivos te ayuda a eliminar el riesgo de pérdida y deterioro de grandes archivos.

Cuando utilizas un disco duro externo es muy importante tener en cuenta las medidas básicas de seguridad y proteger este dispositivo con las acciones que sean necesarias. A continuación, revisa alguna de ellas.

1. **Cifrado del disco**

Es muy recomendable que el disco duro esté cifrado. Cifrar el disco es un proceso muy sencillo que permite establecer una clave para acceder al contenido del disco, siendo imposible hacerlo sin ella.
Obviamente, hay que tener en cuenta todas las recomendaciones sobre las contraseñas, ya que es importante que cumpla con las diferentes medidas de seguridad.

2. **Actualización**

Se debe mantener actualizado el programa que da acceso al disco, ya que las actualizaciones siempre implementan mejoras de seguridad que son importantes para mantener a salvo los datos.

3. **Escaneado del disco**

Utilizar un programa para escanear el disco duro buscando problemas de seguridad es una acción importante para evitar que cualquier programa malicioso pueda comprometer la seguridad de los datos.

4. Desconexión

Durante el tiempo en que la conexión al disco duro no vaya a ser usada, es recomendable desactivar el acceso, particularmente si se está realizando a través de Internet. Obviamente, las intranets son más seguras para acceder a datos, pero en la actualidad suele ser bastante común que, para mejorar la operatividad, se puede acceder a estas informaciones utilizando Internet.

En este caso concreto, y aunque se cumpla con todos los protocolos de seguridad, es muy conveniente que eliminemos cualquier conexión no imprescindible para minimizar los riesgos.

Plataformas y espacios digitales

Los datos han de tener establecidos unos privilegios que reduzcan su acceso a un pequeño número de personas.

Es conveniente que, dentro de las plataformas y los espacios digitales, **se establezcan restricciones para diversas secciones de datos**. Esto no quiere decir que usuarios y usuarias no puedan acceder a ellos, pero sí que será necesario solicitar el privilegio a quien administra el sistema para conseguir un pase temporal. Este pase, que conviene monitorear si se trata de datos restringidos, **deberá caducar de forma programada**.

Recuerda...

Es importante que dentro de las plataformas de trabajo también se restrinja el movimiento de la información.

Es inevitable que, al trabajar con grandes sistemas de datos, se produzcan errores. Quienes lo gestionan son seres humanos y es normal que, en algún momento, se dejen datos en carpetas donde no deben estar. El problema es que esos errores pueden traer responsabilidades serias, de forma que, entendiendo que se pueden cometer, también debemos poner todo nuestro empeño en intentar que esto no ocurra.

Es necesario conocer y seguir los protocolos de trabajo establecidos por la empresa para las plataformas digitales y minimizar la posibilidad de cometer errores.

3.2 Seguridad al usar herramientas de gestión de tareas compartidas

Los tableros de colaboración y los tableros de tareas compartidas permiten gestionar las actividades diarias de una forma coordinada, por lo que están extendidos para trabajar en diversos proyectos de forma conjunta.

Las nuevas formas de trabajo implican que diferentes personas trabajen de manera coordinada y esto requiere registrar el progreso y finalización de las tareas en un espacio digital compartido. Existen múltiples plataformas que permiten la gestión de tareas a través de tableros colaborativos.

La cantidad de plataformas de este tipo cada vez es mayor y su uso puede dar fluidez y creatividad a los diferentes procesos de trabajo. Para usarlos con seguridad es **importante que cuides los datos que compartes** y que, después de la sesión de trabajo, los archives de forma segura o los elimines.

En el trabajo de Marta todos los días se organiza una reunión donde se presenta el tablero con las actividades y seguimientos de cada persona de su organización que trabaja en su proyecto. Estos tableros indican el estado de avance en que se encuentra cada miembro del equipo y qué le falta para completar su tarea.

Por supuesto, todo el proceso de trabajo debes realizarlo bajo contraseña y siempre teniendo en cuenta que, aunque tomemos todas las medidas necesarias, cualquier aplicación externa no debe contener datos sensibles (ni personales ni de la organización).

Herramientas colaborativas como Trello, SketchBoard, GroupBoard, Deskle, etc. ofrecen una gran funcionalidad, pero, al igual que con otras estructuras de trabajo, debemos revisar algunas cuestiones relacionadas con su uso para evitar fugas de información o filtraciones de datos restringidos.

Para ello debes seguir las siguientes recomendaciones:

- **Restringir.**

La primera y la más importante es no tener en un tablero de tareas (ni grupal ni personal) **datos restringidos**. Pueden establecer enlaces a una plataforma (donde habrá que autenticarse), pero en ningún caso se debe hacer copia de datos, aunque eso facilite su consulta.

- **Proteger.**

Si se está trabajando con cualquier plataforma que use **tarjetas de información**, las acciones deberán estar en el interior de dichas tarjetas. Esta recomendación, además de favorecer la limpieza y la organización del tablero, también podría salvar la información y los procesos de trabajo de cualquiera que pueda ver dicho tablero sin tener autorización.

- **Archivar.**

En cuanto acabe un **proceso o una tarea se debe archivar**. Además de hacer efectivo el flujo de trabajo, esta acción eliminará del tablero información que ya no es necesaria.

¿Sabías que...?

Todas las acciones que se realizan en tableros compartidos, en programas de tareas conjuntas o en plataformas, deben cumplir el mismo principio: los datos deben ser usados con seguridad y durante el mínimo tiempo posible.

De esta forma, limitaremos al máximo los errores que puedan producirse cuando trabajamos con ellos.

3.3 Dispositivos con certificados digitales instalados

El uso del certificado digital está muy extendido, pero se deben tener en cuenta una serie de precauciones para poder hacer uso del mismo de forma segura.

Los certificados digitales son archivos que permiten la identificación personal en el mundo digital. Más sencillamente, es una clave autenticada por un servicio de seguridad pública que verifica tu identidad y asegura la autenticidad de quién firma.

Puedes visitar la página de la Real Casa de La Moneda y Timbre para conocer más sobre el certificado digital para personas físicas. Mira el enlace en el apartado de referencias bibliográficas.

Con este tipo de certificados es importante seguir las recomendaciones que se darán a continuación.

Autoridad que certifica
Lo primero que se ha de plantear es la necesidad de que el **certificado digital esté emitido por una Autoridad de Certificación que sea confiable.** Aunque esto se cumple en la mayor parte de las ocasiones, siempre conviene recordarlo.

Nunca compartir
No se deben compartir nunca los certificados digitales. Compartirlos puede ser enormemente peligroso, sobre todo cuando se utilizan en las empresas en las que, por comodidad, algunos ordenadores tienen varios instalados.

Clave del certificado
Un certificado digital siempre cuenta con una clave que no debe ser accesible para nadie excepto para su usuario o usuaria. La protección de dicha clave es lo que garantiza que el certificado pueda ser usado de forma segura, por lo que ha de ser gestionado adecuadamente en todo momento.

Por otro lado, es importante saber que existen **certificados digitales de seguridad (SSL)** para las páginas web. Este certificado permite cifrar los datos de las personas usuarias mientras navegan por dicha web, así como los datos del servidor donde se aloja la web, de manera que los datos que se intercambien estén protegidos.

Recuerda...

Si un ordenador cuenta con otros certificados, además del de su usuario o usuaria, dicha persona puede utilizarlos para firmar y acceder a todo tipo de documentos si le han cedido la clave.

Esto es bastante común cuando, por agilizar el proceso de firma, se facilita a alguien de administración con **acceso a los certificados**. Esta práctica debe ser abandonada,

por **la brecha de seguridad que puede suponer**. Es mucho más efectivo tener un flujo de trabajo ágil de petición de firmas que instalar en un ordenador los certificados de varias personas.

Una vez que una persona usuaria deja de usar el certificado, se debe revocar. Lo mismo se debe hacer en caso de pérdida de dicho certificado. De esta forma, se evitará un uso inadecuado del mismo.

Estas son algunas de las recomendaciones básicas de seguridad que deben tener en cuenta, haciendo hincapié en que **toda precaución es poca cuando se trata de proteger los certificados digitales** de cualquier organización.

3.4 Redes wifi y seguridad

El acceso a las redes wifi ha de realizarse siempre partiendo del hecho de que dicha red sea segura.

Reflexiona

Teniendo en cuenta lo común que resulta conectarse a redes wifi en espacios como restaurantes, cafeterías o centros comerciales, quienes practican ciberdelincuencia han buscado diversas maneras de hacerse pasar por proveedores de una red wifi gratuita y poder acceder a los dispositivos de sus víctimas. Por ejemplo, alguien puede estar en un restaurante y generar con su portátil una red que se llame “Red wifi restaurante” y las personas que están de paso pueden acceder a este tipo de Red.

Esto no quiere decir que no sea posible conectarnos a estas redes, pero debes **buscar siempre las máximas garantías de seguridad**. Por ejemplo, una red de una institución pública siempre puede ser más confiable que una red de una cafetería.

Utilizar redes ajenas siempre implica un riesgo, especialmente si se consultan cuestiones personales o, aún más, si se está trabajando con datos laborales, ya que los **correos electrónicos, mensajes y cualquier tipo de datos que se introduzcan podrían estar siendo monitorizados.** Por ello, no se deben utilizar bajo ninguna circunstancia redes abiertas o públicas para hacer gestiones de contenido sensible, como **acceder a la banca online o consultar el correo corporativo.**

Configuración de red

En Windows, a través del menú Centro de redes y recursos compartidos se pueden realizar configuraciones que ayudan a proteger la seguridad. La red de tipo 'Pública' es aquella que se debe seleccionar siempre que se utilicen redes públicas cuya seguridad no se pueda comprobar. 'Privada', en cambio, es la que se puede utilizar en redes de total confianza, como la de casa o el trabajo.

De este modo, el ordenador estará protegido de peligros externos.

En la medida de lo posible no utilices redes públicas abiertas o aplicaciones donde se puedan comprometer datos especialmente interesantes para ciberdelincuentes, tales como claves de acceso a la banca online o claves de usuario de plataformas empresariales, entre otras.

Consejos y recomendaciones para hacer uso de las redes wifi

Se deben seguir unas recomendaciones básicas para hacer uso de las redes wifi con seguridad.

Utilizar las redes wifi de forma segura es posible hacerlo siguiendo algunas de las siguientes recomendaciones.

Usa sitios webs seguros
Al utilizar una red wifi abierta, para minimizar los riesgos, conviene conectar principalmente con sitios web seguros (https).

Usa VPN
Es conveniente evitar la conexión a cualquier red abierta. En caso de que se deba hacerlo, a menudo es posible utilizar una VPN, que es una red virtual privada. Este tipo de conexiones en el ámbito laboral las debe proporcionar y configurar la propia organización. En el uso personal, existen soluciones de seguridad VPN integradas con los principales antivirus del mercado, los cuales son fáciles de configurar en ordenadores y dispositivos móviles.

Cambia contraseñas
En las redes wifi personales es muy recomendable cambiar tanto el nombre como la contraseña que se ofrecen por defecto por parte de quien provee el servicio. Estas redes se detectan con facilidad y resulta más sencillo acceder a ellas que si se establecen un nombre y una contraseña propia. Eso sí, es conveniente que esa contraseña cumpla con las condiciones de seguridad.

Elimina la red del dispositivo
Tras la conexión a cualquier red abierta conviene eliminar la red de la memoria del dispositivo. Esto evitará que el teléfono o el ordenador puedan volver a conectarse de forma automática a dicha red.

4. CIERRE

4.1 Resumen

¿Qué le ha ocurrido a nuestra protagonista?

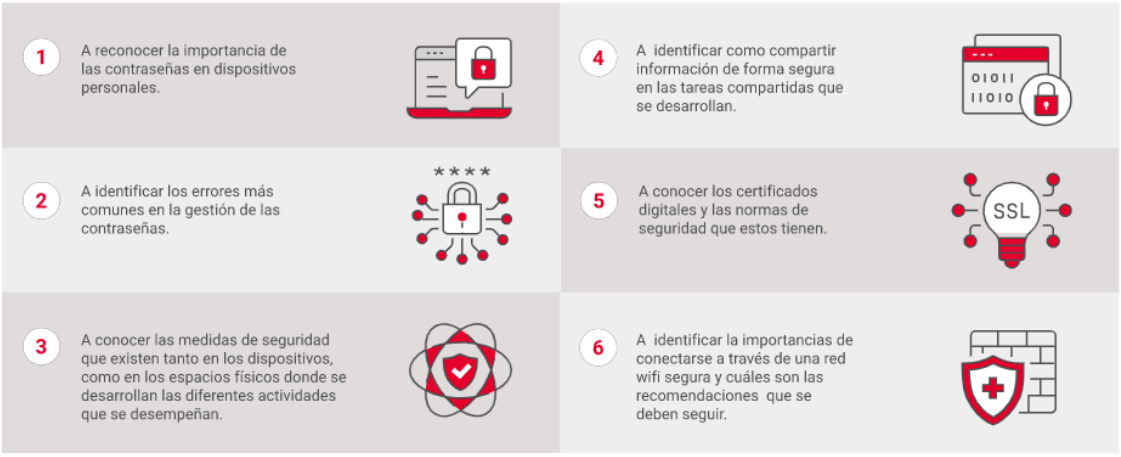
A lo largo de esta unidad didáctica, Marta ha podido aprender que no solo ella es la responsable de proteger la información de las personas que atiende. La ONG "Un mundo mejor" también es parte de este proceso de mejorar la seguridad informática

de las personas con quien trabaja. Además, han logrado consensuar hábitos y políticas seguras en el manejo de claves en los dispositivos de trabajo.

Marta en resumen ha podido aprender a:

- Identificar formas de proteger dispositivos y contenidos digitales, diferenciando riesgos y amenazas en estos entornos.
- Conocer algunas medidas de seguridad y protección, identificando maneras de asegurar la fiabilidad y la privacidad de la información que manejan.
- Saber cómo compartir información personal identificativa sin exponerse a uno mismo ni a terceros a riesgos.
- Conocer las políticas de privacidad sobre cómo se trata la información personal que se utiliza en servicios digitales.

¿Y qué has aprendido a hacer?



Ya has podido apreciar la importancia de asegurar tu información con claves fuertes, utilizar espacios seguros de trabajo tanto en la Red como en los lugares físicos, hacer uso de certificaciones digitales para realizar operaciones importantes y evitar el uso de redes públicas.

En la siguiente unidad tendrás la oportunidad de reconocer e identificar las principales amenazas de la ciberdelincuencia y conocer las medidas de seguridad que se pueden aplicar. Además, podrás ver a Marta como avanza en su formación y tener más herramientas para proteger la información que alberga su trabajo.

Te invito a continuar con la formación.

4.2 Referencias bibliográficas

A continuación, puedes ver la relación de recursos (artículos, estudios, investigaciones, páginas web...) que se han consultado y citado para elaborar el contenido de esta Unidad Didáctica:

- Amaro, M. C. (2020). La seguridad de los datos personales y la obligación de notificar las brechas de seguridad. Revista de Derecho, Empresa y Sociedad (REDS), (16), 151-162.
- Cuerpo Nacional de Policía. (s.f). Qué son los certificados electrónicos. Recuperado de: <https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_430> [12/02/2022].
- Fábrica Nacional de La Moneda y Timbre. Real Casa de la Moneda. Sede electrónica. Certificado Digital. Recuperado de: <https://www.sede.fnmt.gob.es/certificados/persona-fisica> [08/03/2022].
- Oficina de seguridad del internauta (OSI). (s.f). Protégete al usar WiFi públicas. Protégete. Recuperado de: <https://www.osi.es/es/wifi-publica> [12/02/2022].
- Oficina de seguridad del internauta (OSI). (s.f). En Internet cuida tu privacidad. Salvaguarda la información. Recuperado de: <https://www.osi.es/es/tu-informacion-personal> [12/02/2022].
- Porcelli, A. M. (2019). La Protección de los Datos Personales en el Entorno Digital. Los Estándares de Protección de Datos en los Países Iberoamericanos. REVISTA QUAESTIO IURIS, 12(2), 465-497.