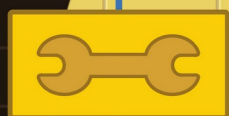


RESUMO DE CONTIDOS

EducACCIÓN dixital

Educación Dixital |
3º ESO

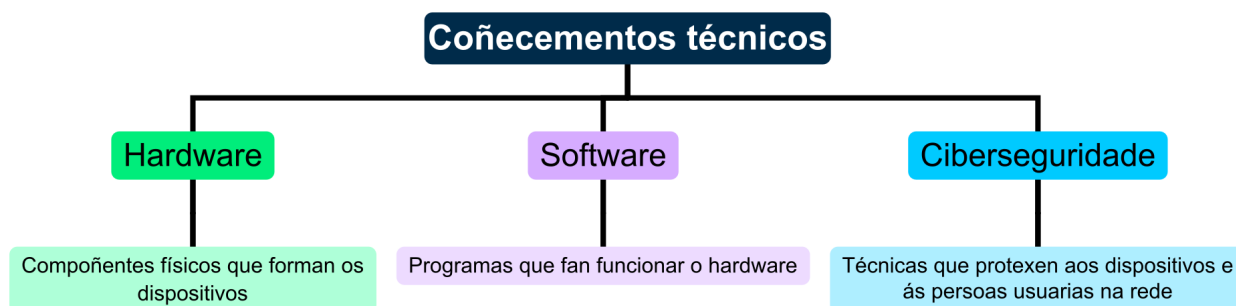


Índice

EducACCIÓN dixital.....	2
1. Centro de adestramento dixital.....	2
1.1 Hardware.....	2
Hardware interno.....	2
Hardware periférico.....	3
1.2 Software.....	4
Software de sistema.....	4
Software de aplicación.....	5
Software de desenvolvemento.....	5
1.3 Poñendo barreiras. Ciberseguridade.....	6
Ciberestafas.....	6
Ciberacoso.....	7
Malware.....	9
A privacidade na Rede.....	11
Atribución dos recursos incorporados ao documento.....	14

EducACCIÓN dixital

1. Centro de adestramento dixital



1.1 Hardware

O hardware é a **parte física dun dispositivo informático**. Está presente en todos os dispositivos: tabletas, teléfonos intelixentes, consolas de videoxogos, etc, que aínda que son moi distintos entre si, comparten os **mesmos compoñentes hardware básicos adaptados ao tamaño** e función de cada dispositivo.

Hardware interno

Son os compoñentes que se atopan **no interior do equipo** informático e que son esenciais para o seu funcionamento.

- **Placa base:** é o compoñente principal do ordenador. É unha placa de circuío impreso á que se conectan os demais compoñentes internos do ordenador.
- **Microprocesador:** tamén chamado **CPU** (*Central Processing Unit*), é o compoñente principal dun ordenador, encargado de procesar toda a información e executar as instrucións dos programas.
- **Memoria RAM:** a *Random Access Memory*, en galego Memoria de Acceso Aleatorio é o compoñente do ordenador onde se garda **temporalmente** a información que o procesador está a usar nese momento para executar instrucións.
- **Disco duro:** é o compoñente do ordenador encargado de almacenar de forma **permanente** a información: sistema operativo, programas e ficheiros. A diferenza da RAM, **a información non se perde** ao apagar o ordenador. A súa **capacidade** mídese en GB ou TB (terabytes).

- **HDD:** garda a información en pratos metálicos xiratorios mentres un brazo mecánico con un cabezal lector/escritor se despraza sobre os pratos, que xiran a gran velocidade, para ler ou escribir datos.
- **SSD:** almacena a información en **chips de memoria flash**. É moito máis rápido, silencioso, lixeiro e resistente aos golpes que o HDD.
- **Tarxeta gráfica:** a **GPU** (*Graphics Processing Unit*) é a encargada de **procesar e xerar as imaxes que se amosan na pantalla**. Pode estar **integrada** na placa base ou ser unha tarxeta independente conectada a ela (**dedicada**).
- **Tarxeta de rede:** permite a conexión a unha rede local ou a Internet. Existen dous tipos principais: a tarxeta de rede por cable (*Ethernet*) e a tarxeta de rede se fíos ou *WI-FI*.
- **Fonte de alimentación:** a **PSU** (*Power Supply Unit*) converte a corrente eléctrica da rede en enerxía utilizable polo ordenador. Nos dispositivos portátiles está presente en forma de adaptador externo.
- **Sistema de refrixeración:** conxunto de **compoñentes encargados de manter a temperatura dos demais elementos do ordenador** dentro duns límites seguros.

Hardware periférico

Defínense os periféricos como os dispositivos **conectados ao equipo** informático que permiten a entrada e saída de información

- **Rato:** periférico de **entrada** que permite mover o cursor pola pantalla e interactuar cos elementos do sistema operativo mediante *clícs* e desprazamentos.
- **Teclado:** periférico de **entrada** que permite introducir texto, números e comandos no ordenador mediante teclas.
- **Monitor:** periférico de **saída** que amosa visualmente a información procesada polo ordenador.
- **Almacenamento externo:** periférico de **mixto** que permite gardar información de forma permanente fóra do ordenador de xeito transportable. Os dispositivos máis comúns son o **pendrive** e o **disco duro externo**.

- **Micrófono:** periférico de **entrada** que capta o son e convérteo en sinal dixital para que o ordenador poida procesalo.
- **Cámara web:** periférico de **entrada** que captura imaxes e vídeo en tempo real para transmitilo a través do ordenador.
- **Altosfalantes e auriculares:** periféricos de **saída** que converten o sinal dixital do ordenador en son audible. Os auriculares, ademais reproducen o son do ordenador de forma individual e privada.
- **Impresora multitarefa:** periférico **mixto** que permite imprimir, escanear e fotocopiar documentos dende un único dispositivo.

Un aspecto importante en referencia aos periféricos é o **método de conexión** ao equipo principal:

- **Físicamente:** mediante **conectores USB-A, USB-C, HDMI, DisplayPort, Jack 3.5 mm, RJ-45**, etc, e os seus **portos** correspondentes.
- **Sen fíos:** mediante *Bluetooth* ou *WI-FI*.

1.2 Software

Software de sistema

O software do sistema é o conxunto de programas que fan posible que o ordenador funcione e que o hardware (a parte física) poida ser utilizado correctamente. **É o software principal do computador** e permite que os demais programas se executen correctamente. Os sistemas operativos máis coñecidos e comúns no teu entorno son **Linux, Windows, Android e iOS**.

O software do sistema actúa como **intermediario** entre o hardware (procesador, memoria, discos e dispositivos) e o software de aplicación (programas de deseño, procesadores de texto ou xogos). A maneira de controlar estas funcións é mediante a **creación de procesos**.

Un proceso é un programa que está funcionando nun momento determinado no ordenador. Por exemplo, cando abres un navegador, un reprodutor de música ou un editor de textos, cada un deles convértese nun proceso.

O sistema operativo encárgase de:

- **Crear procesos** cando se inicia un programa.
- **Repartir o tempo do procesador** entre os programas para que varios poidan funcionar ao mesmo tempo (multitarefa).

- **Controlar a memoria** que utiliza cada programa.
- **Permitir que os programas se comuniquen** entre eles cando é necesario.
- **Pechar os procesos** cando o programa remata ou cando aparece un erro.

Software de aplicación

Os programas de aplicación son o software que utiliza directamente a persoa usuaria para **realizar tarefas concretas** nun ordenador ou dispositivo.

Cada programa de aplicación ten unha función específica, pero existen moitos tipos diferentes, procesadores de texto, navegadores web, editores de imaxe ou vídeo, reprodutores multimedia, videoxogos, programas de deseño, etc.

Segundo as súas funcións **non todos necesitan o mesmo esforzo e recursos do ordenador**. Os principais recursos que usan son o procesador ou CPU, a memoria RAM, o almacenamento en disco e a tarxeta gráfica ou GPU. Así, un editor de vídeo ou un videoxogo usan moitos máis recursos do sistema que un procesador de textos.

Ás veces poden xurdir erros cando usamos un programa, como que vaia lento ou que se peche de repente.

Para solucionar problemas cos programas e aplicacións pódese pechar e abrir de novo o programa que ten o erro, gardar o traballo con frecuencia, manter os programas actualizados ou, no último caso, reiniciar o ordenador.

Software de desenvolvemento

O software de desenvolvemento son as contornas e as linguaxes de programación, os conxuntos de regras e símbolos que permiten ás persoas escribir instrucións que o ordenador pode entender e executar.

O **software de desenvolvemento permite facer diferentes tarefas**, dependendo do tipo de ferramenta, seguro que coñeces aplicacións para programar como Scratch, Makecode ou Mblock, estes son solo o comezo. Existen moitos máis no mercado. Os informáticos profesionais usan **contornos de desenvolvemento integrados (IDE)** para facer programas comerciais.

Algúns de estes programas precisan moitos recursos do ordenador. Por exemplo, compilar un xogo grande ou usar un IDE con moitas funcións require moita CPU, memoria RAM e almacenamento, mentres que escribir código simple usa poucos recursos do sistema.

Traballar con software de desenvolvemento pode xerar problemas, algúns similares aos que ten o software de aplicación.

- **Erro de execución:** o programa falla mentres se executa ao intentar, por exemplo, dividir entre cero.
- **Rendemento lento:** o código está pouco optimizado ou fai tarefas complexas que diminúen a velocidade do programa.

Para evitar estes problemas, é habitual depurar o código (buscar e corraxir erros), probar pequenas partes antes de executalo completo e optimizalo para que use os recursos do ordenador de forma eficiente.

1.3 Poñendo barreiras. Ciberseguridade

Ciberestafas

As ciberestafas son aqueles enganos feitos empregando medios dixitais para conseguir datos persoais, acceso a contas ou diñeiro. Existen varios tipos.

Ciberestafas por mensaxería

Teñen como obxectivo manipular á persoa usuaria para que facilite información persoal ou realice accións que comprometan a súa seguridade dixital. Estas mensaxes aparentan ser fiables, pois adoitan suplantar a identidade de persoas ou entidades coñecidas. Porén, a súa finalidade é ben distinta.

Tipos:

- **Phishing:** a vítima recibe un correo electrónico falso no que a persoa delincente se fai pasar unha empresa ou algún servizo descoñecido coa finalidade de conseguir datos persoais, contrasinais ou información bancaria.
- **Smishing:** a vítima recibe a estafa a través dunha mensaxe SMS ou dunha aplicación de mensaxería instantánea (WhatsApp, Telegram...), na que se solicita información persoal ou se inclúe unha ligazón fraudulenta.
- **Vishing:** a vítima recibe a estafa a través dunha chamada telefónica na que se solicitan datos persoais, bancarios ou credenciais de acceso. Nalgúns casos tamén se lle indica que realice determinadas accións, como facer unha transferencia bancaria ou acceder a unha ligazón fraudulenta.
- **QR-shing:** a vítima recibe a estafa a través dun código QR que, unha vez escaneado, redirixe a unha web fraudulenta ou descarga contido malicioso. Estes códigos adoitan camuflarse en carteis informativos ou superpoñerse sobre os códigos lexítimos, por exemplo, en cartas de menú de restaurantes.

Perfís falsos e roubo de contas

Teñen por obxectivo acceder á información persoal ou tomar o control de contas mediante técnicas de enxeñaría social e manipulación da identidade. Unha das técnicas empregadas é a **suplantación de identidade**, onde a persoa atacante se fai pasar por outra persoa ou entidade real coa finalidade de gañar a confianza da vítima. Isto pode facer que a vítima desvele datos persoais, coma contrasinais, derivando nun **roubo de**

contas, que tamén pode ser derivado de algunha das ciberestafas explicadas anteriormente. Deste xeito a vítima convértese nun "**usuario marioneta**". Tipos:

- **Suplantación de identidade**
- **Romance scam:** a persoa delincente crea un perfil falso na rede coa finalidade de establecer unha relación afectiva coa vítima, empregando a técnica do *cattfishing*. Tras gañar a súa confianza e o control emocional, solicítalle diñeiro, alegando unha situación financeira complicada e urxente, como por exemplo unha enfermidade grave.
- **SIM swapping ou duplicado da tarxeta SIM:** ten lugar cando a persoa atacante se fai co control da tarxeta SIM da vítima. Para iso, suplanta a identidade da persoa propietaria da tarxeta ante a súa operadora móbil. Unha vez feito o cambio, a persoa ciberdelincente pode interceptar as chamadas e SMS, incluídos os códigos de autenticación en dous factores (2FA), o que permite o acceso e control das contas vencelladas a este número, tales como as contas bancarias. O primeiro indicio deste problema é que a vítima queda sen cobertura e deixa de recibir notificacións no móbil.

Ciberestafas a través de premios, ofertas e gangas

Todas elas teñen como finalidade atraer á vítima a través de reclamos moi rechamante, para o cal acostuman empregar, en moitos casos, a suplantación da identidade de empresas e marcas coñecidas. Estas campañas tenden a difundirse por medios de correos electrónicos, redes sociais, anuncios en páxinas web que aparentemente son lexítimas ou videoxogos en liña.

Tipos: premios inexistentes, gangas e ofertas falsas, sstafas a través de xogos en liña.

Ciberacoso

É unha forma de acoso ou intimidación que se realiza empregando tecnoloxías dixitais, tales coma redes sociais, aplicacións de mensaxería, plataformas de xogo, entre outras. Caracterízase por ser un comportamento repetido no tempo e ter como finalidade atemorizar, molestar ou humillar a outra persoa.

Acoso ou intimidación directa

Prodúcese en diferentes canles dixitais como redes sociais, servizos de mensaxería instantánea ou, mesmo, videoxogos en liña. As persoas que acosan buscan prexudicar, ameazar ou exercer un control sobre a vítima. Un dos máis habituais é o **ciberbullying**.

Tipos:

- **Ciberbullying:** é o acoso entre iguais a través de medios dixitais de xeito continuo no tempo. Pode incluír insultos, burlas, ameazas ou publicación de material ofensivo sobre a vítima co fin de humillar. Xeralmente, este termo resérvase para o ciberacoso que ten lugar entre menores.
- **Ciberstalking:** é unha forma de acoso baseada no seguimento e persecución continuada dunha persoa empregando medios telemáticos. A persoa acosadora monitoriza a actividade da vítima en diferentes plataformas e redes sociais. Incluso pode chegar a contactar de maneira insistente ou invadir os seus espazos dixitais co fin de vixiar, controlar ou xerar medo na vítima. Este comportamento caracterízase pola súa continuidade no tempo e a sensación de ameaza que provoca. Nalgúns casos, pode ir acompañado doutros delitos ou riscos, como o envío de mensaxes ameazantes, o acceso non autorizado ás contas da vítima para a obtención de información persoal ou situacións que deriven en casos de *sextorsión*, *grooming* ou *doxing*.
- **Hate ou discurso de odio na Rede:** refírese á difusión de contido a través de medios dixitais que promove o odio, a violencia ou a discriminación contra unha persoa ou grupo baseándose en certas características como a relixión, sexo, orientación sexual, nacionalidade, etnia, diversidade funcional ou determinadas condicións persoais. O *hate* pode producirse a través de comentarios, publicacións, mensaxes, imaxes ou vídeos que atacan a dignidade da vítima e fomentan a súa exclusión social.

Chantaxe sexual

Na contorna dixital existen prácticas a través das que as persoas ciberacosadoras buscan manipular á vítima para obter contidos de carácter sexual, diñeiro ou beneficios persoais, aproveitándose da súa vulnerabilidade. Nestas chantaxes emprégase material de carácter sexual para exercer presión e control sobre a vítima.

Este tipo de situacións adoita producirse a través de redes sociais, aplicacións de mensaxería instantánea ou videoxogos en liña, mediante as que a persoa acosadora contacta coa vítima e gaña a súa confianza.

Tipos:

- **Sextorsión:** é unha forma de violencia sexual e extorsión na que a persoa acosadora ameaza á vítima con difundir contidos íntimos se non cumpre coas súas esixencias, que adoitan ser o envío de máis material íntimo ou a realización de pagos.

En moitas ocasións, o material íntimo obtívose inicialmente a través do **sexting**, é dicir, unha práctica que consiste no envío voluntario de contidos íntimos. Porén, este material pode ser empregado posteriormente sen consentimento e derivar nun caso de *sextorsión*.

- **Grooming**: é un proceso no que unha persoa adulta contacta cun menor a través de medios telemáticos co obxectivo de gañar a súa confianza, manipulalo e establecer unha relación de proximidade. Ao longo deste proceso busca obter información persoal ou contidos íntimos que son utilizados para exercer chantaxe sexual ou incluso tentar acordar encontros presenciais.

Difusión de información privada

Na contorna dixital existen prácticas nas que se difunden datos, imaxes ou conversas privadas sen o consentimento da vítima, o que supón unha violación da súa privacidade. Estas situacións poden ter lugar en redes sociais, aplicacións de mensaxería ou outras plataformas, onde a información pode compartirse rapidamente e chegar a un gran número de persoas, aumentando o impacto do dano.

- **Doxing**: consiste en revelar información persoal dunha persoa na Rede sen o seu consentimento, incluíndo datos identificativos ou sensibles (dirección, teléfono...). A persoa acosadora busca expoñer á vítima, intimidala ou exercer presión sobre ela.
- **Outing**: definido dun xeito estrito, é a revelación pública da orientación sexual dunha persoa sen o seu consentimento coa finalidade de humillar. Porén, dun xeito máis amplo, este termo tamén se emprega para a revelación de segredos ou conversacións privadas. Constitúe unha violación da intimidade.

Malware

O *malware* é todo aquel programa deseñado para infiltrarse nun sistema informático sen o consentimento da persoa usuaria e executar accións maliciosas como causar danos, roubar información, bloquear ficheiros, alterar o funcionamento ou controlar o dispositivo con fins ilícitos.

Malware que causa dano e se propaga

Entre o *malware* con capacidade de propagación e infección destacan:

- **Virus**: é un tipo de *malware* que precisa inserirse nun ficheiro ou programa para propagarse. Polo tanto, non funciona de xeito autónomo, sendo preciso que a persoa usuaria abra, execute ou active o programa ou o contido do ficheiro

infectado. Poden modificar, corromper ou alterar o comportamento dos arquivos infectados, así como do propio equipo.

- **Verme informático:** é un tipo de *malware* capaz de reproducirse e propagarse por si mesmo. A diferenza dos virus, non precisan inserirse nun ficheiro nin que a persoa usuaria o execute, pois é quen de espallarse de xeito autónomo a través de redes ou sistemas conectados. Poden explorar vulnerabilidades do sistema operativo, do software ou da Rede e ser quen de abrir portas traseiras ou desactivar protección.

Malware que espía

Dentro do grupo de *malware* centrado na espionaxe destacan:

- **Spyware:** é un tipo de *malware* creado para espíar a actividade da persoa usuaria sen que esta se decate e, por suposto, sen o seu consentimento. O seu principal obxectivo é recompilar información persoal, como hábitos de navegación, credenciais de acceso ou datos sensibles. Pode rexistrar a actividade do dispositivo, monitorizar o uso de aplicacións ou enviar información a terceiras persoas, comprometendo gravemente a privacidade da persoa usuaria.

Adoita instalarse de xeito oculto xunto con outros programas ou mediante descargas enganosas. Pode funcionar en segundo plano, de xeito oculto, durante longos períodos de tempo.

- **Keylogger:** é un tipo de *malware* especializado en rexistrar as teclas que se premen nun dispositivo. Pode obter información sensible sen que a persoa usuaria o perciba co obxectivo de enviarlla á persoa cibercriminal. Céntrase en conseguir credenciais de acceso, contrasinais ou datos bancarios introducidos a través do teclado. Pode funcionar de maneira oculta no sistema, almacenando a información rexistrada ou enviándoa a terceiras persoas, comprometendo a seguridade e privacidade da persoa usuaria.

Malware que controla e secuestra

Entre o *malware* que se caracteriza por controlar ou secuestrar o funcionamento do equipo cabe sinalar:

- **Troiano:** é un tipo de *malware* que se presenta como software aparentemente lexítimo para enganar á persoa usuaria. Unha vez executado, pode abrir accesos non autorizados, descargar outros compoñentes maliciosos ou permitir o control remoto do dispositivo. Adoita chegar camuflado en instaladores, programas pirateados ou anexos e non ten a capacidade de replicarse por si mesmo.

- **Botnet:** é unha rede de dispositivos que foron previamente comprometidos e que quedaron baixo o control remoto dunha persoa atacante para executar accións coordinadas, como o envío masivo de *spam*, ataques distribuídos ou envío doutro *malware*. Pode pasar desapercibida durante bastante tempo, xa que o equipo segue funcionando mentres participa en actividades maliciosas en segundo plano.
- **Ransomware:** é un tipo de *malware* que cifra os ficheiros do dispositivo ou bloquea o acceso ao dispositivo coa finalidade de pedir un rescate económico. O seu impacto adoita ser inmediato e moi visible, especialmente cando afecta documentos.
- **Cryptojacking:** consiste no uso non autorizado dun dispositivo para minar criptomoedas aproveitando a súa capacidade de procesamento. A diferenza doutras ameazas, non sempre busca roubar información nin bloquear o equipo, senón manterse o maior tempo posible consumindo recursos sen ser detectado.
- **Adware:** mostra publicidade intrusiva, introduce redireccións ou altera a navegación para xerar ingresos por clics ou número de visualizacións. Adoita instalarse xunto con programas aparentemente lexítimos, extensións dubidosas ou paquetes gratuítos modificados.
- **Rootkits:** están deseñados para ocultar a presenza doutro *malware* e manter acceso privilexiado ao sistema ás persoas ciberdelinquentes sen seren detectadas. A súa perigosidade radica na capacidade de actuar a niveis moi profundos do sistema, alterando a visión que as ferramentas de seguridade teñen do equipo comprometido.

A privacidade na Rede

Actualmente, boa parte da vida das persoas desenvólvese na Rede. A diario, empregamos aplicacións para comunicarnos, acceder a servizos, buscar información ou compartir momentos en redes sociais. Sen case decatarnos, imos deixando unha pegada con cada acción que realizamos. Esa pegada pode parecer inofensiva, pero non sempre o é. Ás veces, pequenas decisións como o que se comparte, a privacidade ou como protexer correctamente as contas poden ter máis importancia da que pensamos.

Identidade dixital e pegada dixital

Cada acción que realizas na Rede contribúe á construción da túa identidade dixital, tanto a nivel explícito como implícito. Isto non se limita exclusivamente ao que decides publicar, por exemplo nas redes sociais, senón que tamén inclúe toda a información que se xera durante o uso de servizos dixitais: patróns de navegación, consultas, metadatos de localización, interaccións ou mesmo os tempos de uso.

Deste xeito, vas xerando unha pegada dixital que combina dúas dimensións complementarias:

Pegada dixital activa: conxunto de datos que unha persoa usuaria comparte de xeito consciente e voluntario da Rede. Inclúe publicacións en redes sociais, correos electrónicos, comentarios en foros, compras na Rede ou formularios que se envían.

Pegada dixital pasiva: conxunto de datos recompilados automaticamente sen que a persoa usuaria sexa consciente mentres navega pola Rede. Inclúe información como o historial de navegación, as cookies, a dirección IP, o tipo de dispositivo empregado na navegación, a frecuencia de visitas, a localización xeográfica ou o comportamento en plataformas de comercio electrónico, entre outras.

Esta acumulación de datos permite a construción de perfís dixitais altamente precisos. Non só reflicten os teus intereses, senón tamén hábitos, rutinas e patróns de comportamento. Desde unha perspectiva de ciberseguridade, isto supón unha superficie de exposición relevante, posto que canta máis información está dispoñible, máis viable resulta a realización de ataques dirixidos.

Enxeñería social: a exposición de información persoal na Rede incrementa de forma significativa a eficacia das técnicas de enxeñaría social. Cando unha persoa atacante dispón de datos reais sobre ti, pode construír mensaxes fraudulentas máis cribles e adaptadas ao teu contexto, reducindo a desconfianza da vítima e aumentando a probabilidade de éxito do ataque.

Suplantación de identidade: certa información como fotografías, nomes de usuario ou datos biográficos, entre outros, poden ser reutilizados para crear perfís falsos, facerse pasar por ti e gañar a confianza doutras persoas. Ademais, moitos servizos empregan datos persoais ou preguntas de verificación nos procesos de recuperación de contas. Se esa información está pública, facilítanse os accesos indebidos ou recuperacións fraudulentas.

Persistencia: unha vez que a información se publica na Rede, pode ser indexada por motores de busca, almacenada en cachés, arquivada por plataformas, replicada por terceiras persoas ou reutilizada fóra do contexto orixinal, introducindo un compoñente de persistencia que dificulta o control posterior sobre os datos. A eliminación dun contido non garante a súa desaparición. Pode ter sido descargado, capturado, reenviado ou procesado por sistemas automatizados. Isto implica que a difusión inicial dun dato pode xerar efectos duradeiros no tempo e nun ámbito distinto ao previsto inicialmente.

Redes sociais: nelas esta dinámica intensifícase. Cada publicación, “gústame”, comentario, etiqueta, historia ou interacción contribúe a aumentar a túa pegada dixital. Isto non depende só do que compartes, senón tamén das opcións de visibilidade, da

información asociada ao teu perfil e da actividade xerada pola túa rede de contactos. Ademais do acceso por parte doutras persoas, estas plataformas poden empregar os datos recollidos para procesos de perfilado, segmentación e personalización algorítmica. Alén diso, unha configuración de privacidade inadecuada pode ampliar a exposición pública da túa información.

Privacidade na Rede

A privacidade na Rede non depende só do que decides compartir, senón tamén de como se recollen, tratan e expoñen os teus datos no ámbito dixital. Cada servizo que utilizas establece condicións de acceso, permisos e configuracións que determinan quen pode ver a túa información e con que finalidade pode ser empregada.

Algúns aspectos clave para xestionar correctamente a túa privacidade, reducir a túa pegada dixital e manter un maior control sobre a túa información persoal son: a visibilidade, a recollida e tratamento de datos e os permisos que outorgas.

Contrasinais e protección da privacidade

A protección da túa privacidade tamén depende da seguridade coas que blindas o acceso ás túas contas e dispositivos. Un control de acceso deficiente facilita accesos non autorizados, exposición de datos persoais ou a suplantación de identidade. Por iso, resulta fundamental empregar mecanismos de autenticación robustos e aplicar medidas técnicas que reduzan o risco de intrusión como:

- **Xestores de contrasinais:** os contrasinais deben ser robustos para cumprir correctamente coa súa finalidade. Nesta función, pode ser útil o emprego de xestores de contrasinais. Estes xestores permiten crear, almacenar e xestionar credenciais seguras sen necesidade de memorizalas todas. Permiten empregar claves únicas e complexas en cada conta, reducindo a reutilización e mellorando o control das credenciais.
- **Autenticación multifactor (MFA):** engade unha segunda capa de seguridade ao proceso de acceso. Ademais do contrasinal, solicita unha segunda proba de identidade, como un código temporal, unha aplicación autenticadora, unha chave física ou un sistema biométrico. Isto reduce de forma significativa o risco de acceso indebido, mesmo cando o contrasinal foi comprometido.
- **Accesos:** a protección do acceso require tamén supervisión. Por unha banda é necesario protexer o acceso aos dispositivos mediante un mecanismo seguro, como un código PIN ou patrón. Ademais, é recomendable revisar sesións activas, dispositivos conectados e alertas de inicio de sesión sospeitoso. Ademais: pecha sesión en dispositivos compartidos ou públicos, activa as alertas de acceso cando a

plataforma o permita e rexeita sesións descoñecidas e cambia as credenciais ante calquera indicio de que a túa conta estea comprometida.

Atribución dos recursos incorporados ao documento

Recursos incorporados por orde de aparición e páxina:

Páxina 2: [Elaboración propia \(Proxecto cREAgal\)](#). *Coñecementos técnicos dos dispositivos dixitais*. [Licenza CC BY NC SA](#).



“Resumo de contidos: EducACCIÓN dixital”, do proxecto *cREAgal*, publícase coa [Licenza Creative Commons Atribución Non-comercial Compartir igual 4.0](#)