

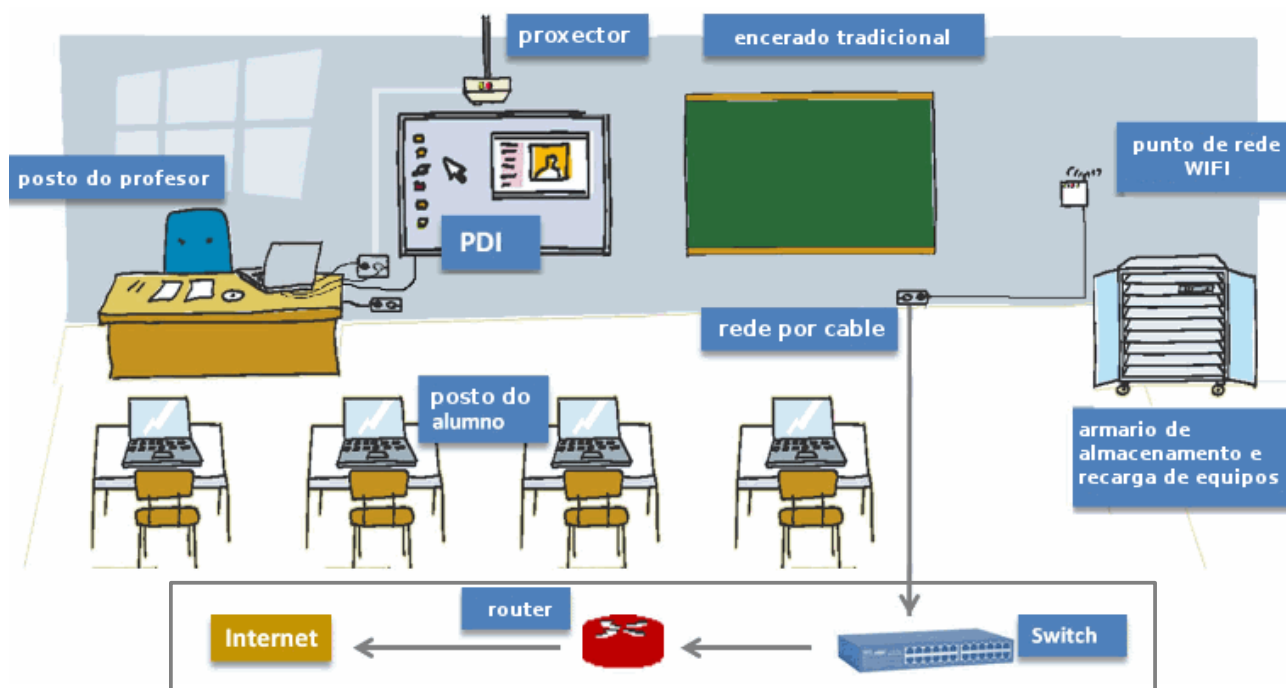
A aula TIC e a aula Abalar

Pódese considerar a aula TIC como o primeiro paso para a integración das Tecnoloxías da Información e a Comunicación nas aulas, pasando da "aula de informática" á "informática nas aulas".

Consideraremos unha aula TIC aquela que conte co seguinte equipamento mínimo: un PC, sexa portátil ou de sobremesa, cos periféricos precisos: rato, teclado, altosfalantes e impresora. Os equipos portátiles adoitan levar integrada, tamén, unha cámara web. A este equipamento pódese engadir, de ser o caso, un proxector e unha pantalla. Nos casos de aulas Abalar atoparemos outros elementos, como son un proxector de curta distancia, un EDI ou PDI (Encerado ou Pizarra dixital Interactiva), o portátil do profesor, os netbooks do alumnado e o armario de carga.

Ademáis, as aulas TIC dispoñen tamén de conectividade para tódolos equipos presentes na aula. No caso das aulas Abalar, dispónse de conectividade WIFI e mais conectividade por cable.

Esquema dunha aula TIC



Elementos dunha aula Abalar

Tódolos elementos que podemos ver a continuación, están presentes en calquera aula Abalar



portátil profesor



netbook alumno



videoproxector



EDI



armario de carga



interior armario de carga



caixa de conexións



interior caixa



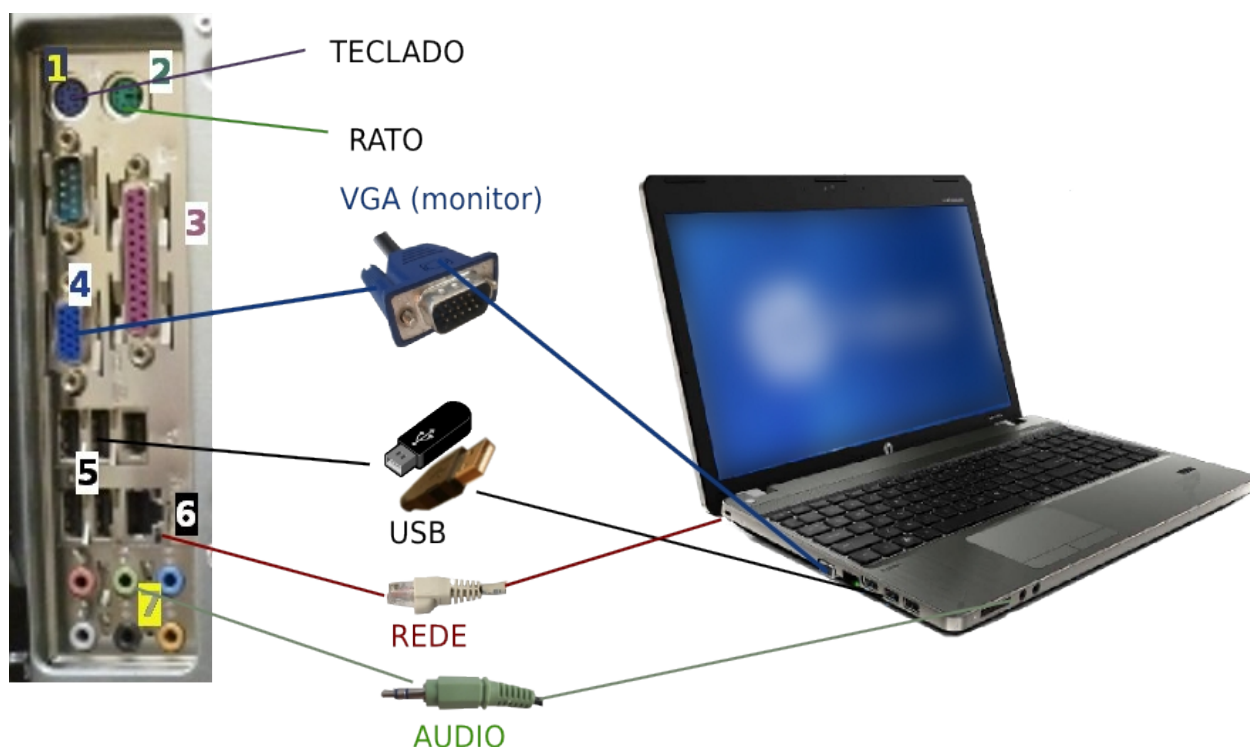
Punto de acceso WIFI



Conexións á rede por cable

Conexión dos periféricos

- Todos os ordenadores levan as conexións na parte traseira, sexan de formato torre (vertical) ou formato plano (horizontal). Cada unha destas conexións só pode acoller un dispositivo, de xeito que non se pode conectar, por exemplo, o monitor no conector da impresora.
- A continuación vemos a placa de conexións dun PC de sobremesa.

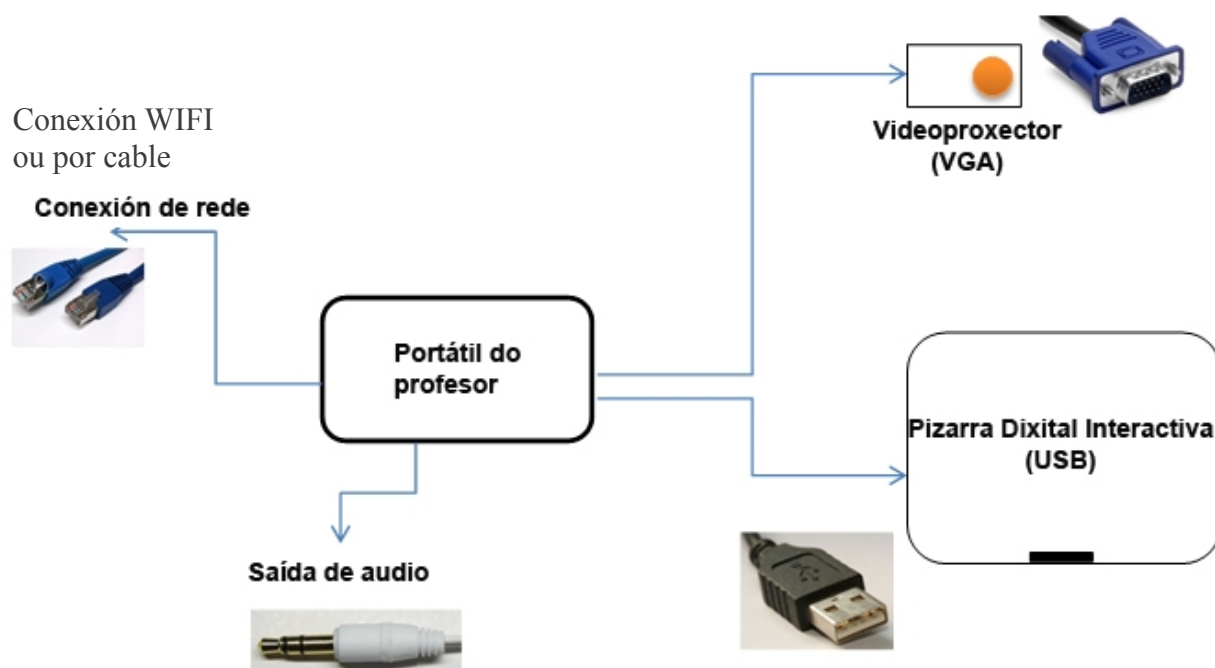


- Os portátiles adoitan ter as conexións nos laterais e na parte traseira. Na parte dianteira teñen, polo xeral, as conexións de audio (altosfalantes ou auriculares e microfone).
- Habitualmente, os portátiles teñen unha cámara web e un microfone integrados na parte superior do marco da pantalla.

Periféricos Abalar

Como dixemos con anterioridade, as aulas Abalar contan cun equipamento engadido e que precisa tamén de conexión ao portátil do profesor e á rede eléctrica.

En calquera caso, os tipos de entradas son os mesmos que xa vimos, e o esquema para deixar todo funcionando sería este.



Procedementos de seguridade

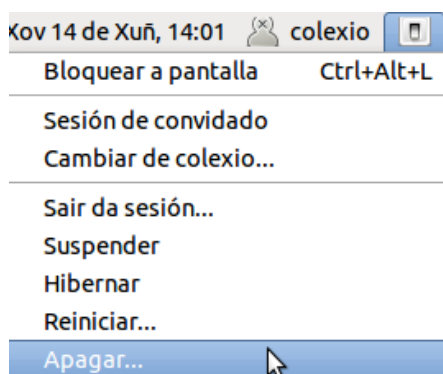
Apagar equipos

O apagado dun equipo débese facer utilizando sempre o menú de apagado con que contan todos os sistemas operativos, sexan Windows, Linux ou Mac; deste xeito asegurámonos de que todos os procesos finalizan correctamente e preservamos a integridade dos datos que contén o equipo.

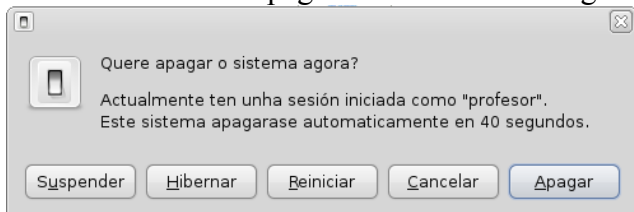
Ao finalizar este proceso interrómpese automaticamente a alimentación eléctrica.

No sistema operativo Linux instalado nos equipos Abalar o proceso é similar. A continuación vemos un exemplo.

1.- Facer clic na icona superior dereita da pantalla coa imaxe dun interruptor e no desplegable, clic en "Apagar".



2.- Clic no botón "Apagar" do cadro de diálogo seguinte.



Retirar unidades externas

Entendemos por unidades externas aqueles dispositivos de almacenaxe que se conectan ao PC por medio dun dos portos adicados a iso. Os máis comúns son os Pen Drives  que poden

almacenar varios Gigabytes (Gb) de datos como poden ser fotos, vídeos, música, etc. A capacidade destes aparellos varía, sendo o máis habitual capacidades de 2, 4, 8, 16 ou 32 Gb.

Estes dispositivos son recoñecidos, por norma xeral, polo noso ordenador en canto os conectamos ao mesmo.

O proceso máis seguio para retirar estes dispositivos unha vez rematado o traballo con eles é o que se indica a continuación.

- Antes de retirar o Pen Drive, debemos asegurarnos de cerrar as aplicacións que estaban gardando datos nel, como pode ser o procesador de textos, o reprodutor de música, etc. con isto evitaremos que apareza unha mensaxe dicindo que non se pode retirar.
- O último paso consiste en facer clic na flecha que aparece ao lado da icona que identifica ao Pen Drive. Cando esta icona desaparece, xa podemos retirar fisicamente o Pen Drive do noso equipo con total seguridade

Internet. Contas de usuario

Unha conta de usuario en internet ven definida por un nome de usuario e un contrasinal. O nome de usuario pode ser mesmo un endrezo de correo electrónico -caso de Google, hotmail ou Yahoo- e o contrasinal adoita ser elixida polo propio usuario.

Neste apartado da sesión imos tocar os puntos seguintes:

- Creación de contas. Nome de usuario e contrasinal.
- Elixir o contrasinal correcto.
- Acceso e peche de sesión en servizos da internet.

O Contrasinal

A elección do contrasinal de acceso é moi importante porque é o que, en boa medida, garante a confidencialidade dos nosos datos en Internet.

Moitos sitios web, como veremos no exemplo de creación dunha conta en Gmail, indícanos a "fortaleza" do contrasinal a medida que o imos escribindo. Canto máis forte, mellor.

Como regra xeral, un contrasinal seguro debe reunir os seguintes aspectos.

1. Ter una lonxitude mínima de seis caracteres; se son oito, mellor.
2. Combinar maiúsculas, minúsculas, signos e números.
3. NON incluír o nome de usuario nen nomes de familiares ou datas significativas.
4. Non deben ser palabras que se atopen nun diccionario.
5. Para o usuario tamén debe ser doado lembrala.



O acceso aos diversos servizos telemáticos que ofrece a Consellería de Cultura, Educación e Ordenación Universitaria realízase a través do dominio "@edu.xunta.es".

O noso enderezo de correo electrónico é moito máis que iso; é a porta de entrada a aplicacións como Xade, concurso de traslados, xestión de datos persoais, formación en Platega, consulta de actividades de formación en Fprofe, a rede social Redeiras, etc.

Aínda que para o correo electrónico utilicemos contas distintas á que nos proporciona a Administración Educativa, esta é de suma importancia, polo que convén facer algunhas recomendacións:

1. O contrasinal é absolutamente persoal e intransferible, polo que ninguén, agás nós, debe coñecelo. O contrasinal non se di nin se "empresta".
2. Para que o contrasinal faga correctamente o seu traballo, debe reunir os requisitos xa comentados anteriormente e que repetimos:
 - Debe ter unha lonxitude de 6-8 caracteres, misturando letras, números e caracteres diferentes (signos como "=", "?", "%", "-", "_")
 - Nunca debe ser unha palabra que se poda atopar nun diccionario; estes contrasinais poden ser descubertos con facilidade.
 - Non debemos utilizar datas ou iniciais relacionadas con nós u co noso entorno máis próximo.
 - Se o navegador nos pregunta se queremos que lembre o contrasinal, **diremos que non**. Do contrario, calquera podería acceder á nosa conta só con saber o nome de usuario, o que é bastante común.
 - A conta de usuario corporativa debe ser utilizada unicamente para acceder a estes servizos, e evitaremos utilizala para darnos de alta noutras páxinas que precisen rexistro para acceder.
 - Ignoraremos sempre os correos e as mensaxes de orixe descoñecida que nos soliciten os nosos datos de usuario (aplícase como medida de seguridade para calquera conta).

Para utilizar a nosa conta deberemos introducir só o nome de usuario (o que vai á esquerda de @edu.xunta.es); escribir o contrasinal, tendo en conta que non vemos o que escribimos senón uns puntos; procedemento estándar que ten a finalidade de protexer o contrasinal de miradas alleas, e prememos "Entrar".

**XUNTA DE GALICIA**
CONSELLERÍA DE EDUCACIÓN
E ORDENACIÓN UNIVERSITARIA

Benvido ao servizo de correo da Consellería de
Educación e Ordenación Universitaria



Usuario

Contrasinal

Idioma Galego

Modo Dinámico

Nome de usuario sen
@edu.xunta.es

Contrasinal

Conta de usuario/a ?

Estase a identificar para acceder a un servizo web da Consellería de Educación e Ordenación Universitaria.

Por favor teclee o nome de usuario/a e o contrasinal da súa conta de correo de edu.xunta.es.

Lembre:

- Preste especial atención a se está usando maiúsculas ou minúsculas.
- Se erra varias veces no seu contrasinal, o seu usuario/a e contrasinal bloquearanse e non poderá acceder a ningún servizo web incluíndo o correo. Neste caso terá que desbloquealo accedendo ao seguinte enderezo [desbloquear usuario](#), ou contactando coa Unidade de Atención a Centros (vexa a información de Contacto no pé de páxina).

Nome de usuario/a

@edu.xunta.es

Contrasinal

Creación dunha conta de usuario

A continuación imos crear unha conta de usuario. Seguiremos o proceso paso por paso.

Utilizaremos GMail, de Google, porque é un caso típico de como unha conta de correo e un contrasinal facilítanos o acceso a unha chea de servizos.

Habitualmente deberemos cubrir un formulario no que se nos pedirán certos datos; algúns son obrigatorios e outros non.

Son datos obrigatorios:

- Nome de usuario. É o que aparecerá na nosa conta de correo electrónico, antes do símbolo @
- Contrasinal. Deberemos escribila dúas veces para que o sistema se cerciore de que é a que quermos. No caso de equivocarnos e que non coincidan, avisaranos.
- Nome e Apelidos.
- Data de nacemento
- Sexo

Outros campos non son obrigatorios, a excepción da cadradiño no que dis que aceptas a política e termos de uso de Google e o Captcha, que consiste nun recadro no que aparecen un par de palabras, deformadas e difíciles de ler, que permiten determinar que quen está facendo a solicitude é un ser humano, e non un programa informático ou outro ordenador cun sistema automatizado.

Despois de cubrir estes datos, pasas a dúas pantallas que, se queres, podes deixar tal como están e clicar en "Siguiente"; a conta de correo e de usuario dos servizos de Google está creada.

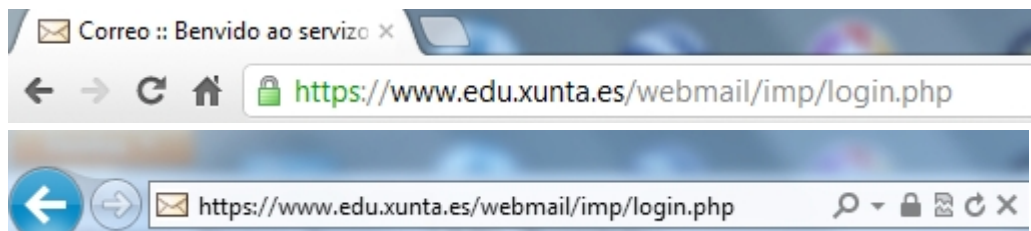


Acceso seguro

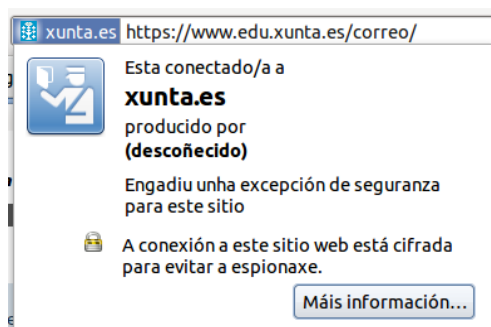
A popularización dos accesos de banda ampla a Internet facilitou tamén a aparición de servizos web que permiten realizar múltiples operacións a través da web. Sirvan de exemplo as contas de correo web, o proceso do concurso de traslados, a xestión de centros a través de Xade, a posibilidade de comprar por internet, ou consultar as contas bancarias, entre outros moitos. Todo isto xenera un inxente tráfico de datos, e moitos deles moi apetecibles para os amigos do alleo, como as claves de acceso ao banco ou os números das tarxetas de crédito, por exemplo.

Que podemos facer para previr que nos rouben datos importantes?

1. Verificar que accedemos a unha páxina segura. O navegador web informaranos mediante un signo de un candado ou similar, e sobre todo, porque na barra de direccións veremos que ésta comeza por **https://** en vez de **http://**



No caso de Mozilla Firefox, un dos navegadores máis utilizados, a información de seguridade aparece cando facemos clic no botón que está xusto ao lado de https:// e que pode ser **gris**, se a páxina non facilita ningún tipo de información, **azul** se da información básica ou **verde** se da información completa.



2. Utilizar os teclados virtuais se están disponibles no sitio que visitamos, desta maneira podemos evitar que programas espia capturen (rexistren) as teclas que prememos.
3. Na medida do posible non seguir ligazóns para acceder a estes sitios e teclear a dirección.
4. Non enviar nunca, en ningún formulario, o nome de usuario e o contrasinal. Nin o noso banco, nin a Xunta, nin Facenda, ningunha entidade seria nos vai pedir nunca o nome de usuario e o contrasinal.

Peché de sesión

Cando rematamos de interactuar nun sitio web, é importante pechar a sesión; NON vale simplemente con pechar a ventá do navegador, **é preciso que fagamos clic na icona ou na ligazón que fai efectivo o peche da nosa sesión** de usuario.

O dito anteriormente non ten excesiva importancia se estamos a utilizar o noso ordenador na casa, pero resulta vital cando usamos un equipo que é compartido por moitas persoas (ordenador da sala de profesores, da aula de informática, nun cibercafé, etc.) Se non cerramos explicitamente a sesión, a persoa que utilice o ordenador xusto despois que nós, pode atoparse cos nosos datos, correos ou a información que tiveramos en pantalla no momento de deixar o aparello.

No mesmo caso dos equipos compartidos, **debemos rexeitar sempre a suxerencia de gardar o contrasinal** que nos fai o navegador; é cómodo se temos un ordenador en exclusiva, pero no caso contrario, hai que pensar que calquera podería entón acceder ás contas protexidas con dito contrasinal.

Exemplos de botóns de peche de sesión.

1. Correo da Consellería de Educación.



2. Botón de peche de sesión en Xade.



3. Ligazón de peche de sesión en Gmail.

