Consejos de seguridad digital

Hoy en día Internet y los servicios disponibles a través de ella forman parte de nuestras vidas. Tanto a nivel laboral como personal utilizamos todo tipo de servicios digitales (servicios bancarios, redes sociales, correo electrónico, comercio electrónico...) en todo tipo de dispositivos (ordenadores, teléfonos, tabletas) y esto implica un montón de información y datos personales que circulan por la red, se almacenan en los dispositivos, se aportan a las compañías que nos ofrecen servicios... con los consiguientes riesgos de seguridad y para nuestra privacidad.

Este documento, más que una guía, es un conjunto de breves fichas con consejos y recomendaciones relacionados con nuestra seguridad en Internet que pretende promover un uso más seguro y responsable de los servicios digitales.

según si utilizas...

- CORREO
- NAVEGADOR
- BANCO
- MENSAJERÍA INSTANTÁNEA
- TRÁMITES ONLINE
- COMERCIOS
- PHISHING
- NUBE
- DISPOSITIVOS MÓVILES / APPS

FÍJATE EN...

- HTTPS?
- PIDE DATOS O CÓDIGOS?
- ¿REPUTACIÓN?
- ¿SOSPECHOSO? (PROMOS/-DESCUENTOS/ORO Y MORO)
- ¿SOSPECHOSO? (PROB. TÉCNICO O SEGURIDAD/CAMBIOS POLÍTICA/ CESE DE ACTIVIDAD...)
- ¿PASARELAS DE PAGO?
- ¿CONDICIONES DEL SERVICIO?
- ¿QUÉ INFO COMPARTES?
- ¿URL?
- ¿URGENCIA?
- ¿REMITENTE?
- ¿REPLY TO?
- ¿QUÉ DICE EL SALUDO?
- ¿ENLACES?
- ¿ERRORES GRAMATICALES?
- ¿DOMINIO?
- ¿ADJUNTOS?

... Y PROTÉGETE

- CERTIFICADO ELECTRÒNICO / CL@VE
- VERIFICACIÓN EN 2 PASOS
- ELIMINAR
- CÓDIGO O PATRÓN DE BLOQUEO
- BLOQUEO DE USUARI@S
- GESTOR DE CONTRASEÑAS ROBUSTAS
- CHAT/NAVEGACIÓN PRIVADOS
- REDES SEGURAS: WIFI CERRADO / DATOS PROPIOS / PROXY?
- COPIAS DE SEGURIDAD
- CERRAR SESIÓN
- CIFRADO
- CUENTAS DE USUARIO/A
- ANTIVIRUS
- CONFIGURAR PRIVACIDAD
- CONSULTAR A TU SERVIDOR
- CAMBIAR LA CLAVE DE ACCESO
- CONFIGURAR LÍMITES A LOS SERVICIOS
- CONSULTAR POR OTROS CANALES OFICIALES O DIRECTOS
- LIMPIAR HISTORIAL, DATOS, DESCARGAS, COOKIES, CACHÉ
- ACTUALIZAR SISTEMA OPERATIVO / SOFTWARE-APPS / ANTIVIRUS
- LEER AVISO LEGAL / POLÍTICA DE PRIVACIDAD / TRATAMIENTO DE DATOS
- NO RESPONDER / NO HACER CLIC / NO DESCARGAR NADA / NO FACILITAR DATOS / NO REENVIAR

ANTE LA DUDA, ANTES DE HACER NADA, BUSCA CANALES OFICIALES Y ¡CONSULTA!

Contraseñas

Las contraseñas dan acceso a tus servicios y por tanto a tu información personal, por lo que es importante protegerlas para evitar que nadie pueda comprometer tu privacidad o tu economía.

* RECURSOS

Keepass es un gestor de contraseñas de software libre y código abierto, de uso claro y sencillo.
https://keepass.info/

CONSEJOS

> Utiliza contraseñas **fuertes**. Que tengan como mínimo 8 caracteres, que contengan mayúsculas, minúsculas, números y caracteres especiales ($, &, #...)

> **NO utilices contraseñas fáciles de adivinar** como: "12345678", nombres de familiares, fechas de nacimiento, etc. -> mucha información rastreable en internet puede facilitar a otras personas adivinar tus contraseñas.

> **NO compartas** tus contraseñas. Las contraseñas deben ser personales e intransferibles

> **NO uses la misma contraseña** en varios servicios, aplicaciones o dispositivos. Si alguien lograse hacerse con tu contraseña, limitas el daño que te puede llegar a hacer.

> **Cambia las contraseñas** al menos una vez al año: por muy fuertes que sean se pueden ver comprometidas en algún momento.

Cómo crear una buena contraseña

Esas contraseñas tan largas, con números, caracteres especiales, etc, que nos facilitan en algunos servicios son muy seguras pero también muy difíciles de recordar. Así que acabamos apuntándolas en el típico post-it al lado de la pantalla, cosa que no es muy recomendable.

\+ Podemos construir una buena contraseña y mucho más fácil de recordar **a partir de una frase o título,** por ejemplo, con "Lo que el viento se llevó" podemos quedarnos con las iniciales: Lqevsl, le añadimos el número 9 y un carácter especial, el $, y podemos construir la contraseña "9Lqevsl$" que tiene los requisitos indispensables para ser una contraseña fuerte pero nos será más fácil de recordar.

\+ A menudo manejamos muchas contraseñas y acaba siendo complicado recordarlas todas, por eso existen los **gestores de contraseñas** * que son programas que permiten almacenar de forma segura tus claves de acceso a los diferentes servicios, y tú solo necesitas recordar una contraseña, la de acceso al gestor de contraseñas, que se conoce como **clave maestra** -> esta clave maestra sí que es importante que no la olvides, ya que es la llave para acceder a todas las demás.

Los sistemas de **verificación en dos pasos** (o de doble factor o doble autenticación) añaden un capa extra de seguridad: además de tu nombre de usuario y contraseña, deberás introducir un código que sólo tú conocerás.

-> Dependiendo del servicio, podrás obtener los códigos de seguridad usando diversos métodos, aunque el más habitual es el envío de un código por SMS

-> Si tienes identificados dispositivos de confianza no tendrás que introducir el código cada vez que quieras acceder a un determinado servicio pero, OJO, esta comodidad puede ponerte en riesgo en caso de robo o pérdida.

¡ATENCIÓN!

Los servicios bancarios utilizan sistemas de verificación en dos pasos y te envían un código por SMS.

NUNCA debes facilitar ese código a nadie, el banco jamás te llamará para solicitarte ningún código de verificación. Hay muchas estafas relacionadas con los servicios bancarios, ¡mucho ojo!

Servicios bancarios

Los servicios bancarios son objetivo de los ciberdelincuentes a través de **mensajes falsos** que suelen llegar por SMS y te informan de que:

> hay un dispositivo nuevo conectado a tu banca *online*,
> te asignan un gestor de un supuesto fraude,
> debes verificar un inicio de sesión
> debes rellenar un formulario para desbloquear tu cuenta,
> debes autorizar una operación,
> tu cuenta va a ser bloqueada,
> etc.

LA REGLA BÁSICA ES DESCONFIAR SIEMPRE DE ESTOS MENSAJES, sean correos electrónicos, SMS, llamadas telefónicas u otro tipo de comunicaciones.

Servicios bancarios

CONSEJOS

- Si recibes un mensaje de este tipo de un **banco del que no eres cliente**, haz caso omiso.
- **Desde tu banco nunca te llamarán para solicitarte datos**, ni contraseñas, ni números pin, ni códigos de verificación que hayas recibido en tu móvil.
- Si detectas un **comportamiento inusual** en tu BancaONLINE o BancaMÓVIL y por ejemplo te solicita que proporciones datos adicionales (teléfono móvil, tarjeta de crédito…) **revisa la dirección** a la que has accedido y verifica que tu dispositivo no tiene *malware*.
- Accede a la web de tu entidad bancaria o de tu banca online usando siempre la **dirección oficial**, nunca a través de enlaces que recibas por correo electrónico o por SMS.
- **Cuida tu teléfono móvil**, los dispositivos móviles pueden infectarse con *malware* que tome el control de tu teléfono y suplante tu identidad a la hora de acceder a la BancaMÓVIL. **Ten cuidado con los SMS** que llegan con enlaces, muchas veces acortados/abreviados (enmascaran así a dónde enlazan para que no sepas que son fraudulentos), o con los archivos que **descargas** o las **aplicaciones** que instalas.
- **Gestiona los límites de tu servicio de BancaONLINE y BancaMÓVIL** reduciéndolos para ajustarlos a tus necesidades reales y desactiva las tarjetas para protegerlas cuando no las utilices.
- **Comprueba siempre la operación** que estás firmando. Cuando tu banco te envía un SMS para firmar una operación, siempre te indica a qué operación corresponde y normalmente te recuerda que no compartas ese código con nadie.
- **Cambia periódicamente tu clave de acceso a BancaONLINE.**

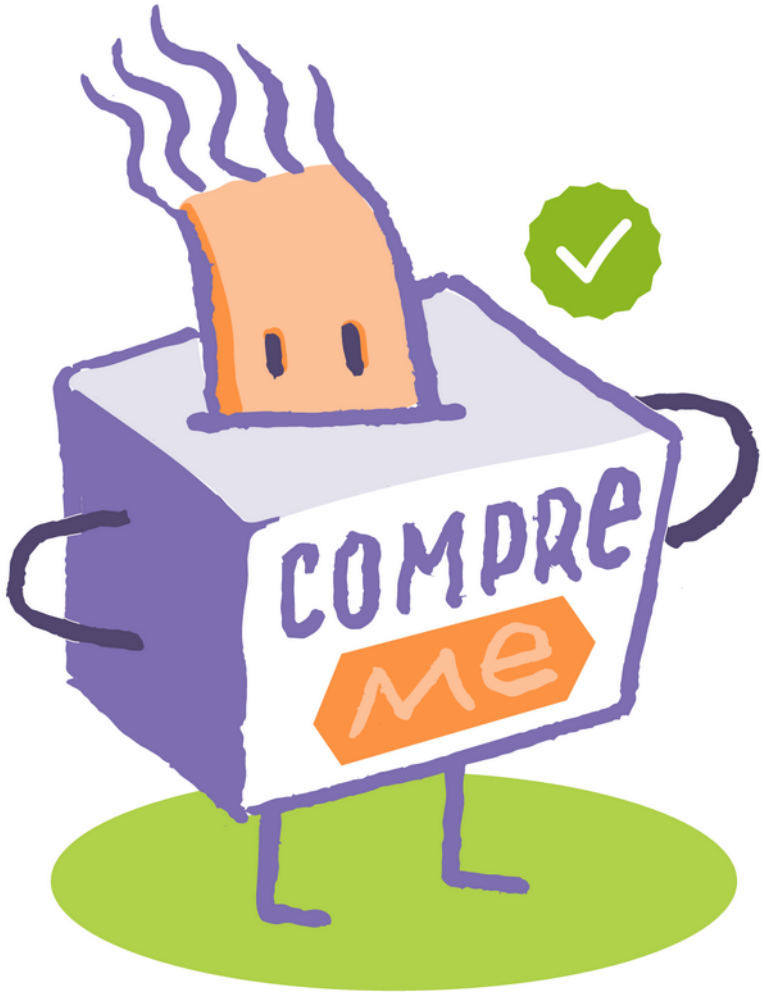
* RECURSOS

ClamAV es un **software antivirus** open source (de licencia GPL) para las plataformas Windows, GNU/Linux, BSD, Solaris, Mac OS X y otros sistemas operativos semejantes a Unix.
https://www.clamav.net/

Servicios comerciales

Las compras *online* están a la orden del día y los ciberdelincuentes son cada vez más sofisticados a la hora de suplantar la identidad de las empresas y comercios donde compramos para así acceder a nuestra información.

Una de las formas más habituales son las estafas de '*phishing*' por correo electrónico: se hacen pasar por empresas o comercios de confianza alertando de algún problema e indicando que con urgencia debes hacer clic en un enlace. Atención, a veces pueden enviarte también un SMS o incluso hacerte una llamada telefónica.



GUÍAS PANGEA

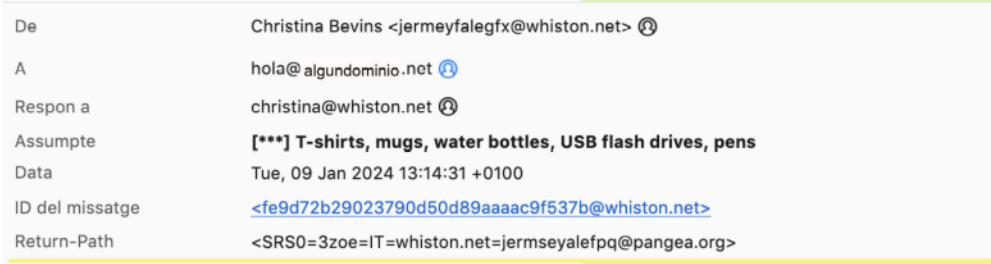
Servicios comerciales

CONSEJOS

> Ante mensajes urgentes y alarmistas **desconfía siempre**.

> **Nunca hagas clic** en ninguno de los enlaces que te facilitan.

→ **Verifica siempre los enlaces:** si pasas el ratón por encima podrás ver dónde enlazan realmente (en la esquina inferior izquierda del navegador te aparecerá), y seguramente descubrirás que apunta a un dominio que no es el oficial del comercio.



De	Christina Bevins <jermeyfalegfx@whiston.net>
A	hola@algundominio.net
Respon a	christina@whiston.net
Assumpte	**[***] T-shirts, mugs, water bottles, USB flash drives, pens**
Data	Tue, 09 Jan 2024 13:14:31 +0100
ID del missatge	<fe9d72b29023790d50d89aaaac9f537b@whiston.net>
Return-Path	<SRS0=3zoe=IT=whiston.net=jermseyalefpq@pangea.org>

> **Verifica los remitentes** ante un correo electrónico sospechoso: en la cabecera del mensaje puedes revisar desde qué dirección se te envió y también el "Reply to" que es a donde escribirías si contestases. Puedes, si no lo ves claro, intentar hacer una búsqueda del dominio desde el que te escriben.

> **Nunca facilites información**, ni por correo, ni por teléfono, ni por ningún otro canal de mensajería.

→ El **comercio legítimo nunca te pedirá que proporciones información** personal ni datos de tarjetas bancarias por teléfono.

> Antes de hacer nada, ve por tu cuenta a la web o app del comercio, **entra en tu espacio online** y verifica la información de tu perfil, el estado de tus pedidos...

> Si tienes dudas o detectas algún problema en tu cuenta o tus pedidos **contacta con el servicio de atención al cliente del comercio por el canal oficial.**

> Si no eres cliente de ese comercio, haz caso omiso al mensaje.

Todos los comercios y empresas en sus páginas web tienen la información de contacto, el servicio de atención al cliente, las direcciones de correo oficiales desde las que te escriben... **Ve siempre directamente a la fuente oficial**, esta es una recomendación útil en cualquier caso o situación.

Phishing

Versión abreviada de nuestra guía sobre Phishing

Entre los riesgos con los que nos podemos encontrar cuando hacemos uso de Internet está el *phishing*, una técnica usada por ciberdelincuentes para obtener información personal y bancaria de la gente usuaria suplantando a una entidad legítima como puede ser un banco, una red social, una entidad pública, etc.

Phishing

CONSEJOS

- **Sé precavido/a** ante los correos que aparentan ser de entidades bancarias o servicios conocidos con mensajes del tipo:
  - · Problemas de carácter técnico de la entidad.
  - · Problemas de seguridad en la cuenta del usuario.
  - · Recomendaciones de seguridad para evitar fraudes.
  - · Cambios en la política de seguridad de la entidad.
  - · Promoción de nuevos productos.
  - · Vales descuento, premios o regalos.
  - · Inminente cese o desactivación del servicio.
- Sospecha si hay **errores gramaticales** en el texto.
- Si recibes **comunicaciones anónimas** dirigidas a "Estimado cliente", "Notificación a usuario" o "Querido amigo", ponte alerta.
- Si el mensaje te obliga a **tomar una decisión en unas pocas horas**, es mala señal. Contrasta la veracidad del aviso directamente con el servicio a través de los canales oficiales.
- Revisa que el texto del **enlace** coincida con la dirección a la que apunta.
- Un servicio con cierto prestigio utilizará sus propios dominios para las direcciones de correo corporativas. Si recibes la comunicación desde un **buzón de correo tipo @gmail.com o @hotmail.com,** no es buena señal.

¿Qué debes hacer si detectas un caso de *phishing*?

- **No contestes** en ningún caso a estos correos. Si tienes dudas pregunta directamente a la empresa o servicio que representa o ponte en contacto con nosotros para hacernos llegar tu consulta.
- **No accedas a los enlaces** facilitados en el mensaje **ni descargues** ningún documento adjunto.
- **Elimínalo** y, si lo deseas, **alerta a tus contactos** sobre este fraude.

Más información

Encontrarás información más extensa en nuestras guías sobre ***spam*** y ***phishing***.

Dispositivos móviles

Hoy en día los dispositivos móviles son parte indispensable de nuestra vida. Con ellos no solo hacemos llamadas sino que enviamos mensajes, navegamos por Internet, gestionamos nuestras cuentas bancarias, hacemos compras *online*, gestionamos nuestra agenda de contactos o nuestro calendario de actividades y un largo etcétera, por eso contienen cantidad de información y datos personales importantes que necesitamos proteger.

Dispositivos móviles

CONSEJOS

> **Cuidado con las apps** que instalas en tus dispositivos móviles, si instalases una app con código malicioso te arriesgas a que roben tu información personal, o que puedan suplantarte para acceder a tus servicios de correo o a tus cuentas bancarias.

→ descarga las apps sólo de los **sitios oficiales o con reputación garantizada**

→ revisa previamente las **valoraciones y comentarios** de la app que han dejado otras personas usuarias para decidir si es conveniente instalarla o no

→ puedes instalar un **antivirus** que te ayude a detectar las apps maliciosas y a proteger tu dispositivo

> Utiliza solo **redes wifi de confianza** que sepas que son seguras. Si utilizas redes wifi públicas o abiertas ten cuidado, pueden no ser seguras (puede que no cifren la información que se transmite, que tengan funcionalidades limitadas o bloqueadas, no sabes qué otros usuarios pueden estar conectados a la misma red...)

→ Si usas redes **wifi públicas**, ya sea en aeropuertos, bibliotecas, etc, como medida de precaución:

- **no envíes datos personales**
- **no uses tus servicios bancarios**
- **no hagas compras online**

> Utiliza un método de **bloqueo de la pantalla** (código numérico o patrón).

> **Cifra la información** que guardes en tu dispositivo móvil.

> Utiliza **herramientas de seguridad** para localizar tu dispositivo, para bloquearlo o eliminar la información almacenada en él, en caso de pérdida o robo.

> Haz **copias de seguridad** en un soporte externo de la información guardada en tu dispositivo móvil.

* RECURSOS

Los móviles con sistema operativo Android ya incorporan la función de cifrado desde las últimas versiones del S.O.
Si quieres aprender cómo cifrar la información de tu móvil puedes consultar las guías sobre configuración de móviles del INCIBE.
https://www.incibe.es/ciudadania/formacion/guias/guia-para-configurar-dispositivos-moviles

Seguridad en las aplicaciones de mensajería instantánea

WhatsApp, Telegram y el resto de aplicaciones de mensajería instantánea incorporan muchas funcionalidades: enviar/recibir mensajes de texto, vídeos, fotos… y como tal, están expuestas a los mismos riesgos asociados a otros servicios de Internet como el correo electrónico y las redes sociales: spam, bulos, timos, estafas, *malware*, etc, están en el orden del día. Tener una idea de qué tipo de engaños suelen utilizar los ciberdelincuentes nos puede ayudar a no caer en sus trampas.

Mensajería instantánea

* RECURSOS

Las listas Robinson son varios directorios creados con la finalidad de ayudar a particulares a librarse del acoso publicitario a través de llamadas telefónicas, SMS, correos electrónicos, por correo postal o fax,...

La más difundida en España fue creada por la Federación de Comercio Electrónico y Marketing Directo FECEMD en 1993 y actualmente está gestionada por la Asociación Española de Economía Digital.
https://www.listarobinson.es/

CONSEJOS

> Hay que estar alerta. **Cuidado si recibes...**
  - Mensajes de contactos desconocidos. → Si no le conoces, mejor **no le agregues**.
  - Enlaces a páginas web. → **No hagas clic** si no sabes a que página te redirige, mucho menos si se trata de un enlace acortado.
  - Bulos y mensajes en cadena. → **No los reenvíes**. Contrasta la información y asegúrate que es veraz.
  - Cuidado si el mensaje es alarmista, utilizan el miedo para que hagas lo que quieren → **Busca información** del posible problema por canales oficiales.
  - Si el mensaje solicita información privada (datos personales, bancarios...) → **No contestes**.
  - Si el mensaje promete premios/cupones/sorteos simplemente por rellenar una encuesta, descargar una aplicación, facilitar tu número de teléfono, etc. → De entrada **desconfía**

> Si no quieres que una información sobre ti se haga pública, mejor **no la difundas a través de un chat**, no sabes lo que tus contactos podrían hacer con ella.

> Foto de perfil → Sé **consciente** de que tu foto es un dato más que alguien (o incluso la IA) puede usar fraudulentamente.

> Bloqueo de usuarios → Decide **con quién** quieres mantener comunicación y con quién no.

> Información de estado → No utilices tu estado para facilitar **información privada** sobre ti.

> Asegúrate de que el intercambio de mensajes esté **cifrado**. Así, aunque alguien los intercepte, no podrá comprenderlos.

> Haz uso de la opción de **chat privado** y/o secreto y evita que personas ajenas a la conversación puedan espiarla.

> Realiza **copias de seguridad** si no quieres perder los mensajes de chat.

> Para evitar casos de suplantación de identidad en caso de pérdida o robo, **establece una contraseña de bloqueo** en tu teléfono inteligente, así impedirás que lo utilicen sin tu consentimiento.

Seguridad en el navegador

Cuando navegamos por Internet toda la actividad que vamos realizando con el navegador se va registrando y queda guardada en nuestro PC o dispositivo, de forma que se puede seguir paso a paso, con el riesgo para nuestra privacidad y seguridad que esto puede suponer.

Piensa que toda nuestra actividad en Internet está expuesta a cualquiera que tenga acceso al navegador que hemos utilizado, también estamos dando pistas acerca de nuestro comportamiento y preferencias en la Red.

Es importante saber qué información almacenan los navegadores y cómo podemos gestionarla adecuadamente, para aplicar las medidas de protección que nos ofrecen los navegadores, sobretodo si utilizamos un dispositivo público o compartido. Una de las opciones más importantes que ofrecen es un modo de navegación privada.

La navegación privada

La navegación privada evita que otras personas sepan las páginas que hemos visitado, los productos que hemos comprado, la publicidad que nos ha interesado, etc... ya que **elimina automática e inmediatamente nuestra información de navegación**, como contraseñas, *cookies* e historial. Actualmente todos los navegadores web ofrecen opciones de navegación privada.

Por ejemplo si utilizas Firefox su navegación privada evitará que se guarden:

- **las páginas visitadas**. No se agregarán ni al Historial ni a la lista de la barra de direcciones.
- las **entradas de formulario** y de la barra de búsqueda. Nada de lo que escribas en los cuadros de texto de las páginas web o en la barra de búsqueda quedará guardado en los datos de la función de autocompletado formulario.
- las entradas de la **Lista de descargas**.
- las ***cookies***. Las *cookies* se almacenan de forma temporal en la memoria, de forma separada a las ventanas normales, y al final de la sesión se eliminan (una vez que se cierre la última ventana privada).
- los archivos de la **caché web**.

La navegación privada de Firefox también incluye el bloqueo de contenido, que evita que los rastreadores ocultos recopilen tus datos en sitios web y ralenticen tu experiencia de navegación.

Más información sobre la navegación privada en **Firefox.**
https://www.mozilla.org/es-ES/firefox/features/private-browsing/

https://support.mozilla.org/es/kb/navegacion-privada-Firefox-no-guardar-historial-navegacion

Navegador

CONSEJOS

Independientemente del navegador que utilices, puedes minimizar los riesgos a los que te expones cuando navegas por Internet si:

- Mantienes el **navegador actualizado** a la última versión.
- Eliges **complementos y plugins de confianza**. Descárgalos solo de sitios conocidos y con buena reputación como son las páginas oficiales de los navegadores.
- Puedes instalar un **verificador de páginas web**, suelen tenerlos casi todos los antivirus.
- Revisas las opciones de **configuración del navegador** y habilitas las que ayudan a proteger tu privacidad y seguridad.
- **Borras el historial de navegación** de vez en cuando.
- **Eliminas las cookies** de vez en cuando.
- Utilizas un **gestor de contraseñas** (que no sea el propio navegador) para almacenar tus claves de acceso.
- **Cierras siempre la sesión** cuando salgas de una página en la que te hayas autenticado con usuario y contraseña. Con esta acción evitas que si una persona utiliza tu ordenador o tu dispositivo móvil pueda acceder a tu información personal usando la sesión que has dejado abierta.

Trámites *online* vía web

Cada vez hay más y más trámites que se pueden o se deben hacer *online*, sobretodo con la administración publica, podemos desde presentar la declaración de la renta hasta pedir cita con el médico entre muchas otras cosas más, y se necesitan un mínimo de conocimientos de ciertos aspectos de seguridad para evitar errores o ser víctimas de algún fraude.

Trámites *online*

CONSEJOS

> Accede a la web para hacer el trámite online desde la **dirección oficial.**
> Fíjate que la URL empiece por **https y que aparezca el candado en la barra de direcciones**. Haciendo clic en el candado podrás comprobar que la dirección a la que accedes sea la correcta y podrás ver el certificado de seguridad de la web (que sea de una autoridad certificadora oficial, que no esté caducado…).
> En general para realizar un trámite online debes abrir una sesión en la web, así que cuando acabes el trámite debes **cerrar la sesión** para evitar problemas.
> Debes **mantener en secreto tus contraseñas** de acceso a los servicios donde vayas a realizar trámites online. No compartirlas y no facilitarlas a nadie.
> Ante cualquier duda o anomalía que detectes, **contacta con el servicio de atención** de donde haces el trámite, ya sea el banco, una administración pública, un comercio…
> Muchos trámites pueden o deben realizarse usando un **certificado electrónico o una Cl@ve** permanente.
  · Un certificado electrónico es un documento electrónico expedido por una Autoridad de Certificación e identifica a una persona (física o jurídica) con un par de claves.
  · Los certificados sirven para validar y certificar que una firma electrónica se corresponde con una persona o entidad concreta. Contiene la información necesaria para firmar electrónicamente e identificar a su propietario con sus datos: nombre, NIF, algoritmo y claves de firma, fecha de expiración y organismo que lo expide.
  · Si no lo tienes aún, obtener uno te facilitará el acceso y la realización de muchos trámites.
> En el caso de compras online recuerda comprobar algunos aspectos antes de hacer la compra.
  · Asegúrate que estás en la **web oficial** del comercio.
  · **Revisa los métodos de pago, condiciones de envío, política de devoluciones, etc.**
  · **Revisa el precio final**, que coincida con el precio del articulo mostrado.
  · **Consulta las opiniones** de otros compradores y la reputación del comercio.

Trámites *online*

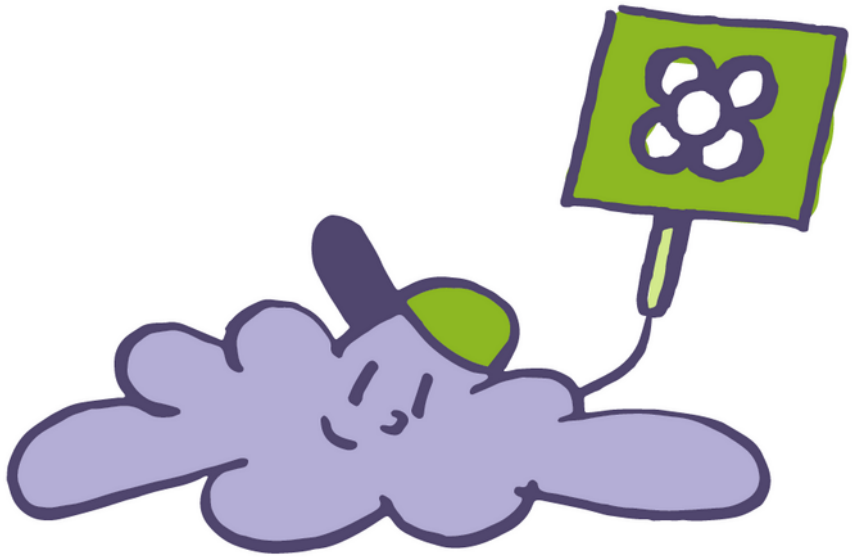
> No te olvides de tener bien **protegidos tus dispositivos.**
  - Asegúrate de que tu dispositivo tenga la **capacidad de hacer el trámite** que necesitas (sistema operativo adecuado, aplicaciones necesarias...).
  - **Instala un antivirus y mantenlo actualizado** para que detecte las últimas amenazas que circulan por la red, siempre que sea necesario.
  - **Mantén actualizado el sistema operativo** de tu equipo y tus programas, como por ejemplo el navegador, y correctamente configurados.
  - Si más de una persona usa el dispositivo, crea **cuentas de usuario** para cada una.

> Tampoco **descuides la conexión** que utilizas.
  - Para realizar trámites online **evita usar redes wifi públicas**. No sabes cómo están configuradas, ni quién puede tener acceso a ellas.
  - Conéctate mejor con el 3G/4G del móvil o desde tu wifi de casa o de un lugar de confianza.
  - Ya sea en tu casa o en un lugar de confianza, comprueba que la red wifi está **correctamente configurada** para evitar que desconocidos se conecten a ella.

> Siempre **desconfía** si un sitio web te solicita información personal pero no te informan acerca de quién es el responsable que va a tratar tus datos personales, de la finalidad para la que se van a destinar y de la forma en la que puedes ejercer tus derechos.
  - Todos los sitios web deben incluir en algún lugar el **aviso legal y la política de privacidad**, en los que debe estar indicado la persona o entidad responsable de la web y del tratamiento de los datos que te solicitan.
  - También debe aparecer un mínimo de **información del responsable del servicio** (Denominación social, CIF, domicilio social (dirección postal), información mercantil, etc.)
  - Deben indicarte claramente **cómo puedes ejercer tus derechos** con relación a tus datos personales.

Seguridad en los servicios en la nube

Los servicios de almacenamiento en la nube te permiten acceder a tus ficheros desde cualquier lugar y dispositivo (PC, smartphone, tableta...), crear carpetas para organizar la información, compartir archivos, sincronizar automáticamente una carpeta en tu dispositivo como copia de seguridad *online* de la información, etc. Pero no todo son ventajas, pueden haber inconvenientes sobretodo si no se toman las medidas de seguridad y privacidad adecuadas.



ALGUNAS VENTAJAS DE LOS SERVICIOS EN LA NUBE

→ Tu información siempre estará accesible desde cualquier lugar con conexión a Internet.
→ No perderás la información si te roban o pierdes tu móvil o tableta, ya que se almacena en los servidores del servicio de nube que hacen funciones de copias de seguridad.
→ Te permiten compartir información fácilmente con quien quieras.
→ Podrás sincronizar tus dispositivos con la "nube" para acceder a ella desde todos ellos.
→ En algunos servicios en la nube podrás acceder a funciones de edición de documentos online.
→ Puedes tener acceso a otros servicios online como: calendario, contactos, galería de imágenes, formularios…

Servicios en la nube

CONSEJOS

Al escoger un servicio en la nube

> Al elegir un servicio de almacenamiento o aplicaciones en la nube busca el que mejor **se adapte a tus necesidades.**
> Nunca dejes de **leer los términos y condiciones de uso** antes de aceptarlos
> Te recomendamos que elijas **un servicio en la nube de proximidad, de confianza,** en el que sepas dónde se guardan tus datos, qué legislación los protege y regula, con quién se comparten, dónde viajan…

Al usar un servicio en la nube

> Asegúrate que el acceso sea bajo **HTTPS**.
> Configura correctamente las **opciones de privacidad y seguridad** del servicio.
> Si es necesario para más seguridad, **cifra tus datos** más confidenciales antes de subirlos al servicio de la nube.
> Utiliza una **contraseña robusta** de acceso y no la compartas. (ver ficha de contraseña !)
> Siempre es una buena práctica hacer **copias de seguridad** en soportes alternativos.
> Si compartes ficheros, asegúrate de que el **destinatario** es realmente quien deseas.

Seguridad en el correo

Es relativamente fácil que alguien pueda conseguir tu dirección de correo electrónico porque:

- puede aparecer publicada en algún blog, foro, etc.;
- por el reenvío de correos electrónicos en cadena;
- por el envío de correos electrónicos con múltiples direcciones sin usar el campo de BCC (Copia Oculta) para protegerlas;
- por haber participado en páginas con falsos concursos, promociones, premios... que obligan a introducir datos;
- por acción de un virus;
- y muchas otras posibilidades.

Si a esto le sumamos el uso de una contraseña poco segura para acceder al buzón, se incrementan mucho las posibilidades de que alguien pueda conseguir tener acceso a tu buzón y pueda leer, modificar y borrar correos privados, enviar correos electrónicos en tu nombre, cambiar las opciones de privacidad y seguridad asociadas al correo...

Correo

CONSEJOS

El correo electrónico es una fantástica herramienta con muchas posibilidades y siguiendo algunas sencillas recomendaciones podemos hacer un uso más seguro de ella.

- Utiliza una **contraseña robusta**
- Que sea una contraseña **exclusiva**, no la utilices para acceder a ningún otro servicio.
- **Evita facilitar información** que pueda comprometer tu privacidad en los correos electrónicos.
- Puedes utilizar **cifrado** con una clave que solo conozca el destinatario del correo electrónico y tú. (consulta nuestra guía Seguridad en el correo para más información)
- Cuidado con los correos de usuarios desconocidos, podrían contener ficheros con *malware* o virus, enlaces a páginas maliciosas o que suplantan la identidad de alguna entidad, etc. Sé precavido **antes de abrirlos o haz clic en los enlaces, revísalos bien**. (consulta nuestra guía sobre Phishing para más información)
- Si el mensaje te resulta sospechoso, aunque el remitente sea conocido, **consulta directamente a esa persona** para confirmar que no han falseado su dirección de correo electrónico.
- Realiza **copias de seguridad** para no perder información de valor en caso de problemas con el servidor de correo.

Bibliografía

Aquí os dejamos algunas guías de ayuda que hemos preparado anteriormente en Pangea que pueden complementar la información.

Correo electrónico, Buenas prácticas

https://laweb.pangea.org/wp-content/uploads/2023/02/guia_correo2_ca.pdf

Phishing

https://laweb.pangea.org/wp-content/uploads/2023/02/guia_phishing_ca.pdf

Correo seguro

https://laweb.pangea.org/wp-content/uploads/2022/05/guia-correu-segur-ca.pdf

Enigmail y OpenPGP para Thunderbird (Linux) – Correo electrónico seguro

https://laweb.pangea.org/es/area-de-usuariosas/enigmail-y-openpgp-para-thunderbird-linux-correo-electronico-seguro/

Enigmail y OpenPGP para Thunderbird (Windows) – Correo electrónico seguro

https://laweb.pangea.org/es/area-de-usuariosas/enigmail-y-openpgp-para-thunderbird-windows-correo-electronico-seguro/

INCIBE

El Instituto Nacional de Ciberseguridad de España (INCIBE), dispone de muchos materiales y guías de ayuda muy interesantes, os dejamos algunas de ellas aquí enlazadas.

Guía de navegadores web

https://www.incibe.es/ciudadania/formacion/guias/guia-de-navegadores-web

Guía de privacidad y seguridad en Internet

https://www.incibe.es/ciudadania/formacion/guias/guia-de-privacidad-y-seguridad-en-internet

Guía para compra segura en Internet

https://www.incibe.es/ciudadania/formacion/guias/guia-para-compra-segura-en-internet

Guía para aprender a identificar fraudes online

https://www.incibe.es/ciudadania/formacion/guias/guia-para-aprender-identificar-fraudes-online

Guía para configurar dispositivos móviles

https://www.incibe.es/ciudadania/formacion/guias/guia-para-configurar-dispositivos-moviles

Guía de ciberataques

https://www.incibe.es/ciudadania/formacion/guias/guia-de-ciberataques

Guía para configurar el router wifi

https://www.incibe.es/ciudadania/formacion/guias/guia-para-configurar-el-router-wifi

Guía para gestionar tu seguridad y privacidad con Google

https://www.incibe.es/ciudadania/formacion/guias/guia-para-gestionar-tu-seguridad-y-privacidad-con-google

Guía de ciberseguridad. La ciberseguridad al alcance de todos

https://www.incibe.es/ciudadania/formacion/guias/guia-de-ciberseguridad-la-ciberseguridad-al-alcance-de-todos

Cómo crear una copia de seguridad

https://www.incibe.es/ciudadania/formacion/guias/como-crear-una-copia-de-seguridad

www.pangea.org
Plaça Eusebi Güell 6-7
Edifici Vertex, planta 0
08034 Barcelona
Tel: +34 934015664
Correo: suport@pangea.org

CON EL SOPORTE DE:

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

Pangea.org

< *INTERNET*
ÈTIC I SOLIDARI >