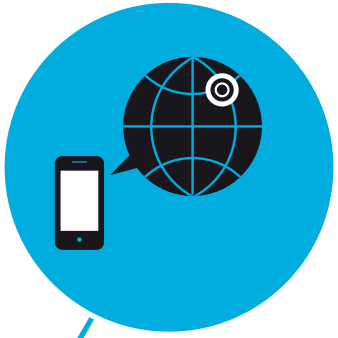
Recomendaciones
para un uso
SEGURO
*de los **dispositivos** y*
*de las **redes sociales***
*en el **Gobierno Vasco***

EUSKO JAURLARITZA
GOBIERNO VASCO

¿Tienes una respuesta segura a estas preguntas?

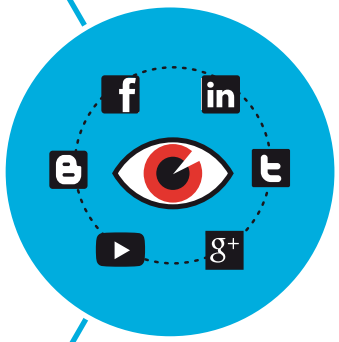
¿Sabes cuándo y por qué activar la geolocalización?



¿Utilizas bien tus contraseñas y tus certificados digitales?

¿En tu tiempo de ocio te preocupas por tu seguridad?

¿Sigues pautas de seguridad y privacidad en las redes sociales?



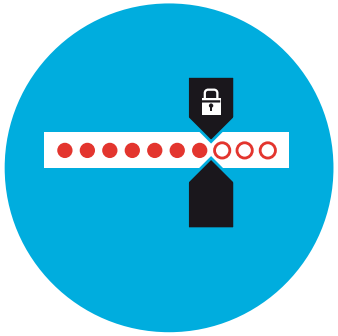
¿Envías información sensible con WhatsApp o cuando estás conectado a una WiFi pública?

¿Actualizas y proteges tus dispositivos móviles?

EUSKO JAURLARITZA
GOBIERNO VASCO

¿Utilizas bien tus contraseñas y tus certificados digitales?

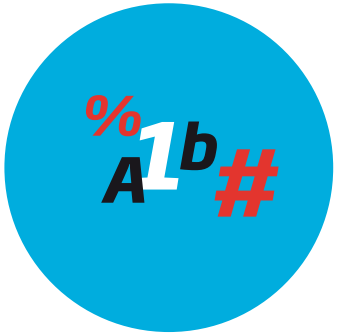
Requisitos para una contraseña segura:



Longitud mínima 8 caracteres.

No utilices 123456, 1q2w3e, 123QWEasd, password, tu nombre, palabras existentes en algún idioma o palabras fáciles de adivinar asociadas a tu persona (nombre de tu mascota, descendientes, etc.)

Una candidata a la vicepresidencia de EE.UU. utilizaba una cuenta de yahoo para comunicaciones oficiales con una contraseña débil, que fue vulnerada por un estudiante (septiembre 2008).



Usa números, letras (en mayúsculas y minúsculas) y símbolos ($, @, &, #, etc.)

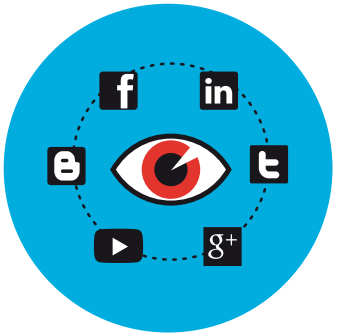
Usa una frase que sólo tú conozcas.

EUSKO JAURLARITZA
GOBIERNO VASCO

¿Utilizas bien tus contraseñas y tus certificados digitales?

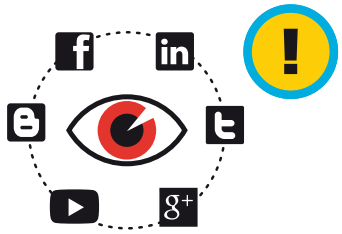
Buen uso de las contraseñas:

Siempre que introduces una contraseña tu navegador o las aplicaciones de tu dispositivo móvil te preguntan si deseas almacenarla. A veces la comodidad puede generar inseguridad si tu dispositivo está en manos ajenas.



Actúa con cautela al introducir tu contraseña cuando accedas a sitios web desde ordenadores ajenos.

Utiliza certificados electrónicos *(+ info.: www.izenpe.com)* ***o el DNIe para firmar o tramitar procedimientos que necesiten un reconocimiento seguro.***



¿Sigues pautas de seguridad y privacidad en las redes sociales?

Seguridad y privacidad en las redes sociales

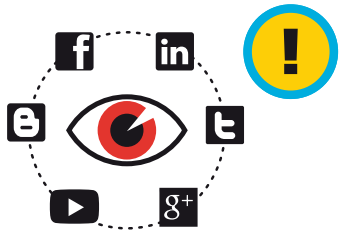
La mejor manera de asegurar tu privacidad en las redes sociales es accediendo a las siguientes páginas informativas, siempre actualizadas, de cada red social:

Un famoso consultor demostró a su hija la importancia de una buena configuración de privacidad mediante un juego: sin ser "amigo" de ella accedió a información personal que a ella no le habría gustado que él encontrara (enero 2013).

- ***Facebook***
- ***Twitter***
- ***Linkedin***
- ***Google Plus***

Utiliza las guías de El Gobierno en las redes (Irekia) siempre que tengas dudas sobre el buen uso de las redes sociales.

EUSKO JAURLARITZA
GOBIERNO VASCO



¿Sigues pautas de seguridad y privacidad en las redes sociales?

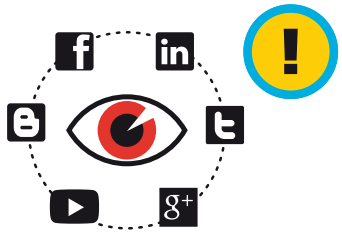
Seguridad y privacidad en Facebook

Consejos sobre tu cuenta

- Guía rápida (Irekia)
- Configuración
- Protección
- Búsqueda de amistades y función de sugerencias
- Bloqueo de personas usuarias
- Aparecer en los resultados de los motores de búsqueda
- Información compartida con aplicaciones
- Darte de baja de una aplicación

Video guías (AVPD)

- Opciones de privacidad I
- Opciones de privacidad II
- Crear y gestionar listas
- Controla el nuevo "timeline"



¿Sigues pautas de seguridad y privacidad en las redes sociales?

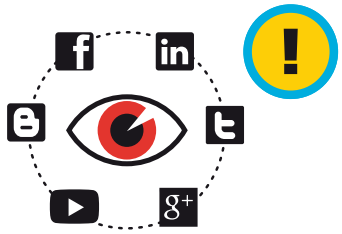
Seguridad y privacidad en Twitter

Consejos sobre tu cuenta

- Guía rápida (Irekia)
- Configuración
- Protección
- Borrado de tweets
- Borrado de la cuenta
- Informar sobre SPAM

Video guías (AVPD)

- Consejos generales sobre privacidad
- Opciones de privacidad
- Inconvenientes de la geolocalización

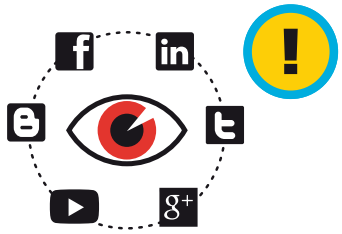


¿Sigues pautas de seguridad y privacidad en las redes sociales?

Seguridad y privacidad en LinkedIn

Consejos sobre tu cuenta

- Configuración
- Ayuda
- Centro de seguridad
- Protege tu identidad
- Protege tu cuenta
- Protege tu privacidad

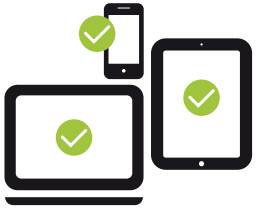


¿Sigues pautas de seguridad y privacidad en las redes sociales?

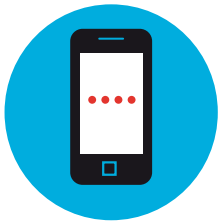
Seguridad y privacidad en Google Plus

Consejos sobre tu cuenta

- Guía rápida (Irekia)
- Configuración
- Privacidad de tu cuenta
- Seguridad
- Interactividad de terceros con tu perfil



¿Actualizas y proteges tus dispositivos móviles?



Utiliza siempre el PIN de tu tarjeta SIM en tu dispositivo móvil y modifícalo de manera preventiva periódicamente.

Activa la opción de bloqueo automático. (p. ej. patrón deslizar el dedo/PIN/ Contraseña/bloqueo biométrico).

Cifra tus datos sensibles.

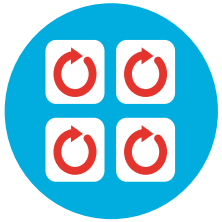
No dejes la pantalla encendida cuando no lo utilices: bloquea siempre el dispositivo móvil. Además de aportar seguridad ahorrarás batería.

Apaga el dispositivo cuando finalices tu trabajo. Iniciar y cerrar sesión en las pausas.

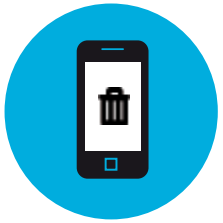
No compartas con terceras personas tu información personal, ni la publiques ni la envíes por correo o mensajería instantánea.

Configura adecuadamente las conexiones inalámbricas para que sólo estén activadas cuando se vayan a utilizar.

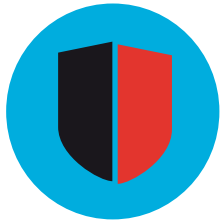
¿Actualizas y proteges tus dispositivos móviles?



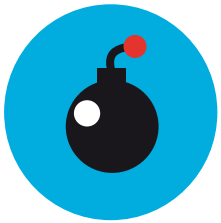
Anota el número IMEI de tu dispositivo ante posibles pérdidas (marca *#06#).



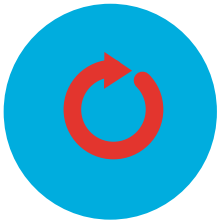
Cuando se da de baja un terminal en el Gobierno, toda la información es borrada por parte del operador, sin posible recuperación.



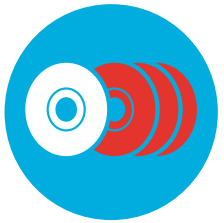
Utiliza programas de seguridad: antivirus, etc. (Siempre de proveedores confiables).



Mantente alerta ante mensajes colgados en redes sociales o distribuidos de forma masiva con enlaces o ficheros adjuntos, pueden incorporar links con SPAM o malware.



Mantén actualizados tus programas, aplicaciones y sistemas operativos. Solemos recibir avisos para actualizarlos (se solicita confirmación).



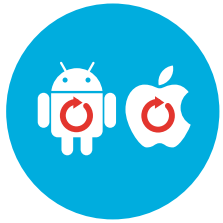
Realiza Copias de Seguridad regularmente, existen muchas formas de automatizar este proceso.

EUSKO JAURLARITZA
GOBIERNO VASCO

¿Actualizas y proteges tus dispositivos móviles?

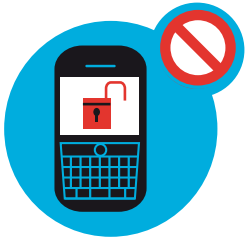
Cuidado con los SMS, correos electrónicos y links de remitentes desconocidos.

No instales aplicaciones de fuentes de dudosa procedencia (sólo de repositorios oficiales, p. ej. Apple Store, Google Play...)



Actualiza automáticamente el Sistema Operativo a la última versión (Android, iOS...)

La instalación de aplicaciones en los dispositivos, en muchas ocasiones, suele autorizar el acceso a datos privados, si lo haces asegúrate de conocer qué permisos concedes.



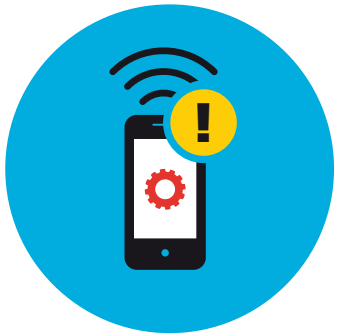
Respeta la garantía del terminal. No lo desbloquees.

Ejecuta automáticamente actualizaciones de las aplicaciones instaladas.

¿Envías información sensible con WhatsApp o cuando estás conectado a una WiFi pública?

Nunca transfieras información sensible con conexiones WiFi públicas.

Ten siempre en cuenta que la transmisión vía conexiones WiFi abiertas es pública y, por lo tanto, no es segura.



Los teléfonos móviles del personal del Gobierno Vasco utilizarán los servicios de transporte ofrecidos por la tarjeta SIM, no se debe cambiar la configuración de los mismos.

Dos personas expertas en seguridad del blog "Seguridad Ofensiva" demuestran de forma práctica que WhatsApp no es seguro y que debería blindarse (noviembre 2013).

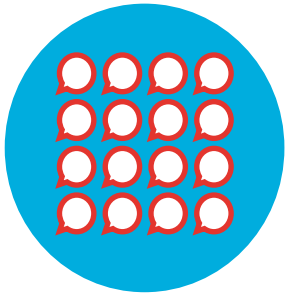
EUSKO JAURLARITZA
GOBIERNO VASCO

¿Envías información sensible con WhatsApp o cuando estás conectado a una WiFi pública?

Riesgos de WhatsApp

Suplantación de identidad.

Envío de mensajes "Phishing".



Envío masivo de mensajes.

Denegación de servicio.

Enumeración de personas usuarias.

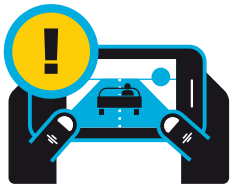
Extracción de claves.

Extracción de conversaciones.

No se recomienda usar esta herramienta para fines laborales, ni tampoco la inclusión de la misma en dispositivos de la administración.

EUSKO JAURLARITZA
GOBIERNO VASCO

¿En tu tiempo de ocio te preocupas por tu seguridad?



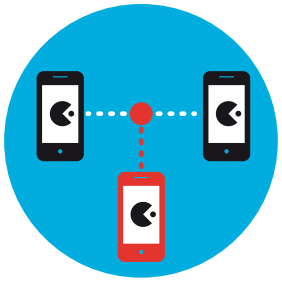
Consejos de seguridad

No te dejes engañar por la ciberdelincuencia.

Cuidado con tu cuenta: evita dar datos personales a personas desconocidas.

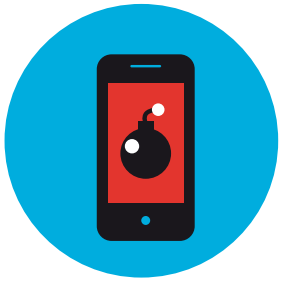
Una aplicación de un juego social instalada en el móvil de un alto cargo utilizó de forma automática su cuenta de twitter para lanzar mensajes publicitarios con el consiguiente eco en toda la prensa (julio 2012).

Riesgos de los juegos sociales



Interceptación de datos cuando te comunicas con otras personas.

Suplantación de identidad.



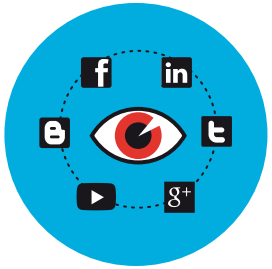
Envío de software malicioso.

¿Sabes cuándo y por qué activar la geolocalización?

Lee con detenimiento y comprende las cláusulas de privacidad de los servicios de geolocalización y las redes geosociales.

Ten cuidado con las imágenes y/o videos que publiques o en los que te etiqueten, ya que pueden servir para dar pistas sobre el lugar en el que te encuentras.

Desconfía, como norma general, de toda persona que no sea conocida.



Configura correctamente los vínculos que publiquen tu ubicación y restringe al máximo la información que ofreces de forma pública.

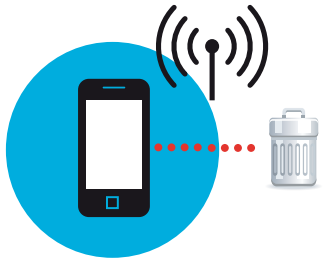
Configura el grupo de personas usuarias que podrán ver la información de geolocalización generada por las aplicaciones o redes geosociales.

Ante la pérdida o robo de tu dispositivo móvil

Ponte en contacto con el Servicio de Atención a Usuario (SAU) en el ***400*** *o* **+34 945 016 400** *si lo haces desde fuera de la red interna.*

Activa aplicaciones de rastreo o búsqueda del mismo.

Cambia, a la mayor brevedad posible, las contraseñas de acceso a los servicios que tuvieses instalados en él.



Borra remotamente los datos (si tenemos la certeza de que no lo vamos a recuperar).

Ante cualquier posible fraude, suplantación de identidad, o robo del dispositivo

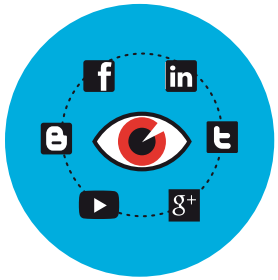
DENUNCIA en la Ertzaintza o Policía

delitosinformaticos@ertzaintza.net

EUSKO JAURLARITZA
GOBIERNO VASCO

Los diez consejos básicos de seguridad

Define bien tus contraseñas y utilízalas de manera segura.



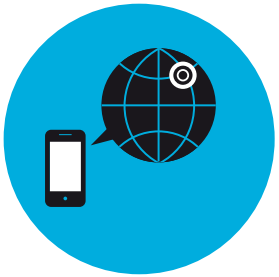
Vigila y asegura tu privacidad en las redes sociales.

Mantén actualizados los Sistemas Operativos y aplicaciones, y protégete con Software de Seguridad.

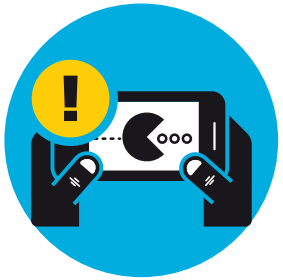
Mantente alerta cuando recibas enlaces o ficheros adjuntos.

Nunca envíes información sensible a través de WhatsApp.

Conéctate mediante los servicios que proporciona tu dispositivo y no utilices una WiFi Pública para enviar información sensible.

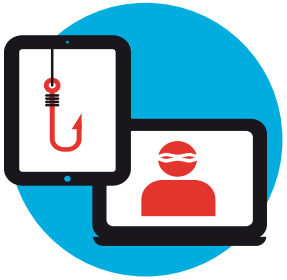


Activa o desactiva la geolocalización en función de las necesidades que tengas.



Utiliza tus dispositivos móviles con responsabilidad en tu tiempo de ocio.

No aportes información que sirva para deducir el lugar en el que te encuentras en un momento dado.



Ante cualquier posible fraude, suplantación de identidad o robo del dispositivo denuncia ante la Ertzaintza o Policía.

Glosario de términos:

Apple Store: Portal de aplicaciones de Apple (iOS)

AVPD: Agencia Vasca de Protección de Datos (www.avpd.euskadi.net)

Geolocalización: También denominada georreferenciación, hace referencia al conocimiento de la propia ubicación geográfica de modo automático e implica el posicionamiento que define la localización de un objeto en un sistema de coordenadas determinado.

Google Play: Antes denominada "*Android Market*", es una tienda de productos "*software*" en línea para dispositivos con sistema operativo Android

IMEI: Siglas en inglés de "*International Mobile Equipment Identity*", Identidad Internacional de Equipo Móvil; es un código que identifica de una forma unívoca el dispositivo móvil físico que realiza la conexión a la red, y posibilita, en caso de robo o sustracción del mismo, su bloqueo.

Irekia: Portal del Gobierno Abierto en Euskadi (www.irekia.euskadi.net)

Phishing: Del inglés "*fishing*" «pesca». Hace alusión al acto de «pescar» personas usuarias mediante señuelos para obtener información secreta sobre ellos. También se dice que es la contracción de "*password harvesting fishing*" (cosecha y pesca de contraseñas).

PIN: Siglas en inglés de "*Personal Identification Number*", Número de Identificación Personal; generalmente de 4 dígitos, que permite acceder o bloquear el dispositivo móvil.

Redes geosociales: Redes sociales que incluyen interacción entre sus miembros basada en el lugar en el cual estos se encuentran.

SIM: Tarjeta de pequeño tamaño que contiene un "*chip*" inteligente desmontable que almacena toda la información sobre el servicio del suscriptor usada para identificarse ante la red, de forma que sea posible cambiar la línea de un terminal a otro simplemente cambiando la tarjeta.

WiFi: Tecnología de comunicación inalámbrica mediante ondas, basada en el estándar IEEE 802.11, que se utiliza para el acceso a Internet sin cables.

Nota: Todas las marcas mencionadas son propiedad de sus respectivos dueños: Google, Facebook, LinkedIn, Twitter, WhatsApp, etc

1ª edición, diciembre 2013

EUSKO JAURLARITZA
GOBIERNO VASCO