PROTEGE TU INFORMACIÓN

SEGURIDAD EN LA ERA DE LOS MEDIOS DIGITALES

CERT-PY

Centro de Respuestas ante Incidentes Cibernéticos

SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL
Construyendo el futuro hoy

Marzo 2016

Tabla de contenido

INTRODUCCIÓN 3

CONTROL DE ACCESO – CREDENCIALES 4

¿Qué es la autenticación? 4

Contraseñas robustas 5

Autenticación de Doble Factor 6

Google 8

Outlook 14

Facebook 18

Twitter 21

Dropbox 25

Wordpress 29

Gestores de contraseñas 31

CORREO ELECTRÓNICO 32

Spam 32

Phishing 33

Enlaces falsos ocultos 34

Remitentes falsos ocultos 35

INGENIERÍA SOCIAL 36

NAVEGACIÓN SEGURA 37

Mozilla Firefox 37

Google Chrome 41

Internet Explorer 43

Safari 44

Complementos de Seguridad 44

SEGURIDAD EN EQUIPOS 46

Actualización de Sistema Operativo y Software 47

Windows 47

Mac OS X 51

Android 53

Antivirus, Antimalware y Firewall 55

Firewall 55

Antivirus 57

Anti malware 58

PROTECCIÓN DE DATOS 59

Contraseña de inicio de sesión 59

Windows 59

Android 60

Encriptación de datos 61

Windows 61

Mac OS X 63

Aplicaciones de terceros 64

Backup 65

Windows 65

Servicios en la nube 67

Borrado remoto 67

Android 68

Mac OS X y iOS 70

Otras herramientas 70

CONCLUSIÓN 71

Introducción

Día a día el perfil de los usuarios de Internet y los usos que estos hacen de la red, está variando, alcanzándose unas notables tasas de penetración en determinados servicios.

El uso de las redes sociales para fines empresariales, el uso de correo electrónico para comunicaciones oficiales, el uso de servicios en la nube para trabajar con información sensible se ha disparado de una forma acelerada en estos últimos años.

El nivel de interconexión entre esos servicios y herramientas fue aumentando, por lo que se han difuminado los límites entre la vida personal, la vida social y el trabajo.

Es por ello que, más que nunca, se vuelve imprescindible reforzar la seguridad de nuestro entorno, de nuestra información. Cualquier punto de entrada es válido a la hora de que un atacante busque acceder a nuestra información.

Este taller busca concienciar acerca de la importancia de seguir buenas prácticas de seguridad así como mostrar las diversas herramientas y técnicas que el usuario tiene a su alcance para resguardar su información y la de los demás.

Control de Acceso – Credenciales

Para realizar la mayoría de las transacciones en Internet, tales como revisar nuestro correo, publicar información, editar un documento, enviar un mensaje a través de una red social, etc., necesitamos autenticarnos en las diversas plataformas.

¿Qué es la autenticación?

La autenticación es el acto o proceso para el establecimiento o confirmación de algo (o alguien) como real, verificando su identidad.

El método de autenticación más utilizado en las plataformas en internet es, por lejos, el sistema basado en usuario y contraseña.

Desde hace varios años que los ataques a los sistemas de autenticación se han popularizado drásticamente: se han vuelto más frecuentes, más sofisticados, más fáciles de realizar.

Hoy en día, un atacante con herramientas de nivel intermedio es capaz de procesar 350 mil millones de contraseñas por segundo.

	Números	Minúsculas	Minúsculas + números	Minúsculas + Mayúsculas + números
6 caracteres	<0,003 milisegundos	< 1 milisegundos	6 milisegundos	0,16 segundos
8 caracteres	0,3 milisegundos	0,6 segundos	8 segundos	10 minutos
10 caracteres	0,3 segundos	6,7 minutos	3 horas	1 mes
12 caracteres	3 segundos	3 días	5 meses	296 años

Cuadro 1.

Además, pueden ser combinados varios tipos de ataque que pueden comprometer todo tipo de contraseñas en tiempos cada vez menores.
Es por eso que deben tomarse una serie de medidas de seguridad adicionales de modo a reducir el riesgo de que un atacante logre obtener acceso a nuestras cuentas.

1. Utilice contraseñas robustas: longitud mínima de 10-12 caracteres; combinación de letras, números, caracteres, etc.; use “frases” de seguridad en vez de palabras; evite palabras de diccionario, etc. En la sección “Contraseñas robustas” se profundizará acerca de las técnicas que pueden ser utilizadas para determinar si una contraseña es segura o no.

2. No utilice la misma contraseña para todo. Los delincuentes informáticos roban las contraseñas de los sitios web que cuentan con muy poca seguridad y, a continuación, intentan usar esas contraseñas y nombres de usuario en entornos más seguros, como sitios web de bancos.

3. Cambie sus contraseñas con regularidad. Establezca un recordatorio automático para cambiar las contraseñas de sus sitios web de correo electrónico, banca y tarjetas de crédito cada tres meses aproximadamente.

4. Cuanto mayor sea la variedad de caracteres que contiene su contraseña, mejor. Use la totalidad del teclado, no solo las letras y los caracteres que usa o ve con mayor frecuencia.

5. No escribir ni reflejar la contraseña en un papel o documento donde quede constancia de la misma. Tampoco se deben guardar en documentos de texto dentro del propio ordenador o dispositivo (ej: no guardar las contraseñas de las tarjetas de débito/crédito en el móvil o las contraseñas de los correos en documentos de texto dentro del ordenador).

6. No enviar nunca la contraseña por correo electrónico o en un SMS. Tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo.

7. Nunca introducir una contraseña en un sitio o programa del cual no tengamos la certeza absoluta de que es legítimo. Existen diversos tipos de ataque, tales como los de ingeniería social (phishing u otras variantes) en los que la contraseña queda expuesta ante un atacante, por más robusta que sea. En la sección "Ingeniería social" se abordará con mayor detalle este tipo de ataques y como reconocerlos.

8. No escribir las contraseñas en ordenadores de los que se desconozca su nivel de seguridad y puedan estar monitorizados, o en ordenadores de uso público (bibliotecas, cibercafés, telecentros, etc.).

9. Cambiar las contraseñas por defecto proporcionadas por desarrolladores/fabricantes e incluso por los administradores de sistemas

10. No utilizar herramientas online para crear contraseñas ni para encriptarlas. Muchas de estas herramientas almacenan estas contraseñas de modo a ampliar su base de datos de contraseñas conocidas.

Contraseñas robustas

Antiguamente, la mayoría de los expertos de tecnología afirmaban que una contraseña robusta constaba de una combinación de al menos 8 caracteres.

Sin embargo, la creciente industria del "password cracking" ha obligado a rever esa definición, ya que hoy en día los 8 caracteres han dejado de ser suficientes, como se puede ver en el cuadro 1.

1. **Longitud:**

   La longitud de la contraseña es un aspecto clave para determinar su robustez. Sería difícil establecer un límite mínimo para ello, ya que día a día, con la mejora de las técnicas de cracking, esta longitud debe aumentar.

   Al día de hoy, la mayoría se inclina a afirmar que una contraseña de 12 caracteres pudiera ser considerada robusta, ante las técnicas de ataque simples/medias.

2. **Combinación de tipos de caracteres:**

   Es importante utilizar distintos tipos de caracteres: minúsculas, mayúsculas, números, caracteres especiales como: *#$%&=?¡ u otros que fueran permitidos.

3. **Frases:**

   Una buena práctica para robustecer la contraseña es la utilización de frases en vez de palabras

como contraseña, lo que ayuda a crear contraseñas más largas. La frase puede representar algo que tenga algún sentido para uno mismo pero que no fuera evidente para los demás. Lo ideal es que la misma no guarde relación con información personal (nombres, apodos, preferencias conocidas, etc.).

Es aconsejable transformar dicha frase para convertirla en una combinación de letras mayúsculas y minúsculas, números y/o símbolos.

4. **Evitar palabras de diccionario:**

   Cuando vamos a elegir una contraseña, es importante evitar elegir palabras o nombres conocidos, normalmente llamados “palabra de diccionario”. Al tratarse de palabras conocidas, altamente probable que la misma se encuentre en alguna lista de palabras que los atacantes usan para sus ataques; a estas listas se le conoce como “diccionario”. Existen diccionarios con miles de millones de palabras, que incluyen casi todas las palabras y nombres que se nos pudieran ocurrir, incluidas combinaciones frecuentemente utilizadas como: admin, 12345, qwerty, asdfg, password, etc.

Autenticación de Doble Factor

Debido a que han aumentado considerablemente las técnicas para romper o comprometer contraseñas, surgió el concepto de autenticación de doble factor.

Se trata de una medida de seguridad adicional que complementa la autenticación tradicional en los servicios. En otras palabras, además de requerir un nombre de usuario y contraseña, solicita el ingreso de un segundo factor de autenticación, como por ejemplo, un código de seguridad. Generalmente, este código se genera en un dispositivo del usuario como un teléfono celular o token. Luego, la persona debe ingresarlo para poder validarse en el sistema.

Un sistema de doble autenticación es aquel que utiliza dos de los tres factores de autenticación que existen para validar al usuario. Estos factores pueden ser:

- Algo que el usuario sabe (conocimiento), como una contraseña.
- Algo que el usuario tiene (posesión), como un teléfono o token que le permite recibir un código de seguridad.
- Algo que el usuario es (inherencia), o sea, una característica intrínseca del ser humano como huellas dactilares, iris, etc.

Por lo general, los sistemas de doble autenticación suelen utilizar los factores conocimiento (nombre de usuario y contraseña) y posesión (teléfono o token para recibir código de seguridad

Con este modelo de autenticación, si un atacante ha logrado obtener el usuario y contraseña de alguna manera, aún así no podrá iniciar sesión debido a que no tendrá forma de obtener el código de seguridad ya que no posee el dispositivo del usuario.

La mayoría de los servicios como Google, Twitter, Outlook, Dropbox, etc. ofrecen esta característica de forma opcional para que cada usuario pueda activarlo. Es importante destacar que este tipo de protección no viene configurada por defecto, por lo tanto, el usuario deberá modificar algunos parámetros para activarla.

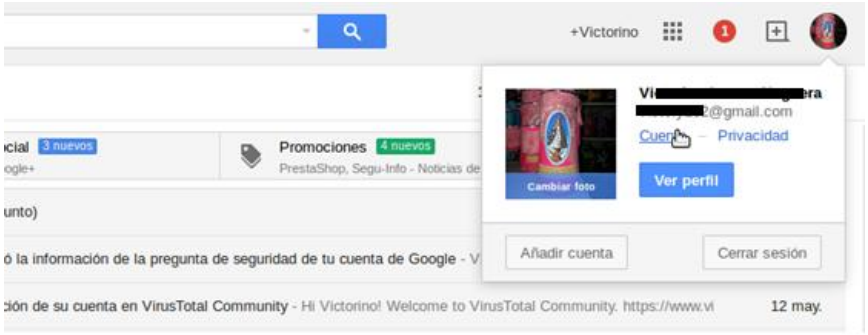
Si además, administramos un sitio web o blog basado en CMS como Wordpress, Joomla u otros CMS populares, existen plugins que pueden ser integrados fácilmente para brindar una capa adicional a nuestro sitio web.

A continuación mostramos como activarla en las plataformas más utilizadas.

Google:

1. Iniciamos sesión ingresando a https://accounts.google.com

2. En la esquina superior derecha, hacemos click sobre nuestra imagen de perfil y seleccionamos “Cuenta”.



3. Vamos hasta la sección Acceso y veremos que hay una opción “Verificación de dos pasos”, que nos dirá si está activada o desactivada. En caso de que esté desactivada, hacer click sobre la opción.

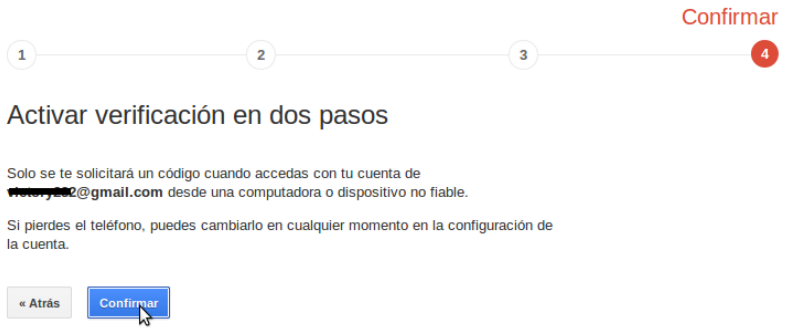
4. En la siguiente pantalla, selecciona “Iniciar configuración”, lo que nos abrirá el asistente de configuración.

5. En el primer paso, completar el número de teléfono con el cual deseamos vincular la cuenta, y elegir si queremos recibir el código a través de un SMS o llamada de voz.

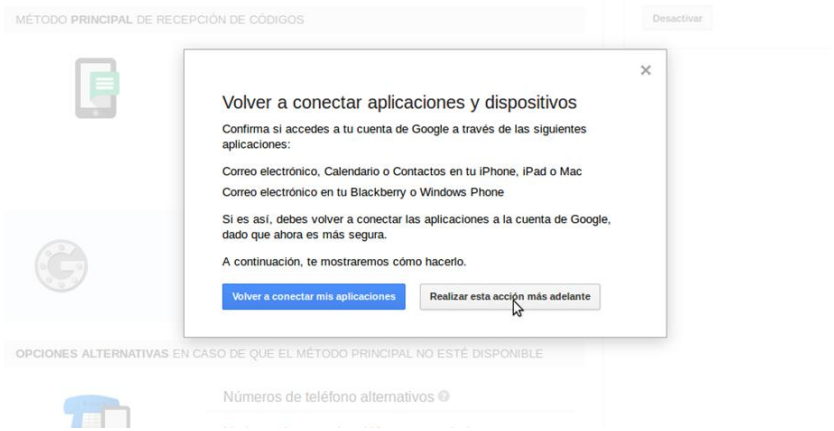
6. A continuación recibiremos un SMS (o una llamada) con un código de 6 dígitos, el cual debemos ingresar en la pantalla.

7. A continuación, se puede elegir si el navegador actual en el que estamos configurando la autenticación será un navegador de confianza o no. Al marcar un navegador como “confiable”, no nos solicitará un código cuando iniciemos sesión en éste. No es recomendable marcar un navegador como “confiable” en caso de que el equipo sea compartido con otras personas.

8. En el último paso hacemos click sobre “Confirmar”, con lo que se ha activado la autenticación de doble factor.



Obs.: Como hemos activado la autenticación de doble factor por primera vez, Google nos desautenticará de sus servicios como Gmail, Calendario, Google+ o Contactos. Nos preguntará si deseamos volver a conectarlas. Podemos elegir “Volver a conectar mis aplicaciones” y seguir las instrucciones, o “Realizar esta acción más adelante”.

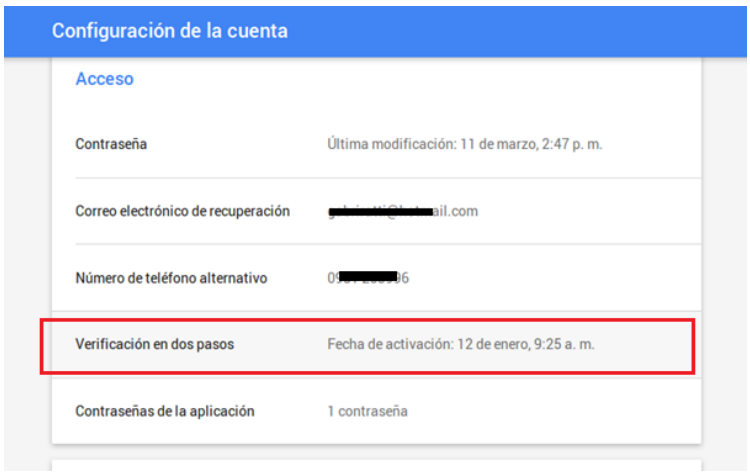


Opcional:

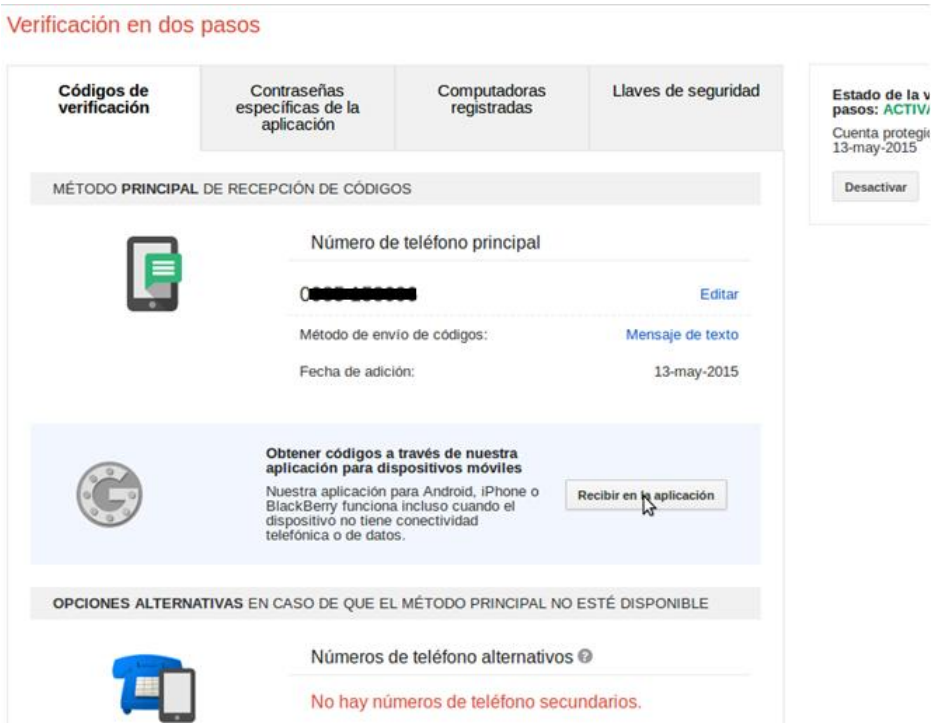
La autenticación de doble factor de Google requiere el envío de un SMS o una llamada, por lo que si no estamos conectados a una red telefónica, la autenticación no será posible. Es por eso que Google además ofrece otro método de recibir el código, a través de una aplicación para el teléfono, Google Authenticator. Este método funcionará incluso cuando no tengamos conectividad telefónica o de datos.

Para que este método funcione, es necesario que la hora del dispositivo móvil esté correctamente sincronizada, por lo que antes de iniciar debemos verificar esto.

1. Para configurarlo, debemos iniciar sesión, entrar a la configuración de la cuenta y hacer click sobre “Verificación de dos pasos”, la cual ahora indicará que fue activada en la fecha en la que lo hicimos.



2. Dentro de la pestaña “Códigos de Verificación”, en la sección “Método principal de recepción de códigos” hacemos click sobre “Recibir en la aplicación”

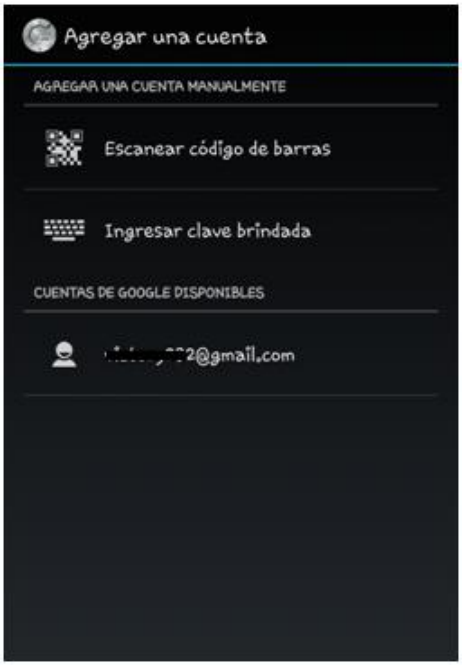


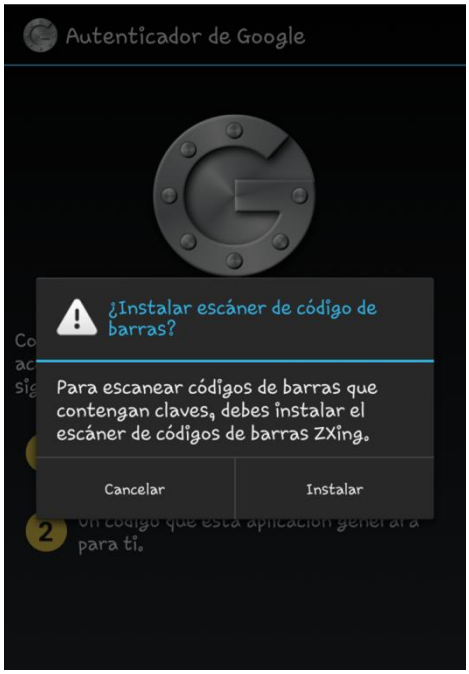
3. A continuación, debemos elegir la opción de acuerdo al sistema operativo que tengamos en nuestro teléfono móvil o en el dispositivo en el cual deseamos recibir el código de verificación. A modo demostrativo, en este manual hemos elegido “Android”. El proceso puede variar ligeramente de acuerdo al sistema operativo y al modelo del teléfono utilizado.

4. Nos aparecerá una guía de configuración con las instrucciones que debemos seguir, paso por paso.

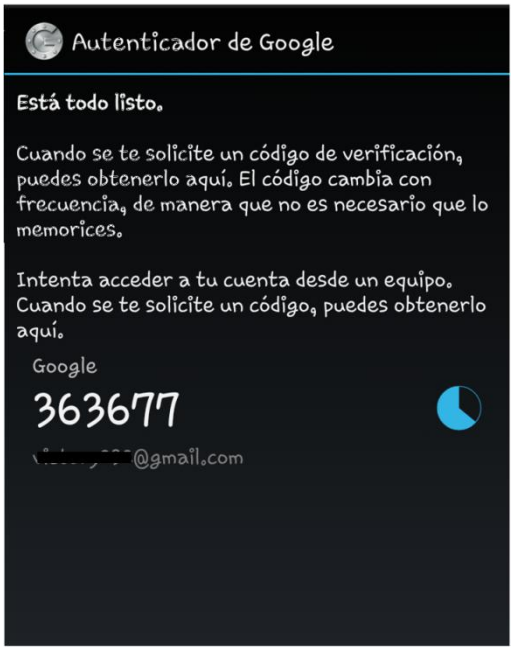
5. Primero debemos instalar la aplicación Authenticator de Google en nuestro teléfono, desde el Google Play Store. Una vez instalada, abrimos la aplicación.

6. En la aplicación, hacemos click en “Comenzar la instalación” y seleccionamos “Escanear código de barras”. Dependiendo del modelo del teléfono, nos podrá pedir que instalemos un lector de códigos adicional, Zxing. En otros modelos, funcionará con el lector de códigos nativos del teléfono.





7. En la aplicación Authenticator seleccionamos “Escanear código” y escaneamos el código QR que aparece en la pantalla del navegador en el que estamos realizando la configuración. Una vez que la aplicación haya reconocido correctamente el código, aparecerá un código de 6 dígitos en la aplicación de nuestro teléfono. Debemos introducir este código en el navegador.



Obs.: Los códigos generados en esta aplicación son dinámicos y tienen un tiempo de vida de 30 segundos, es decir, este código será válido únicamente durante 30 segundos. Transcurrido ese tiempo, el código ya no será válido, por lo que si lo ingresamos para autenticarnos nos dará un error. Siempre debemos asegurarnos de introducir el código antes de que transcurra su tiempo de vida.

Métodos alternativos:

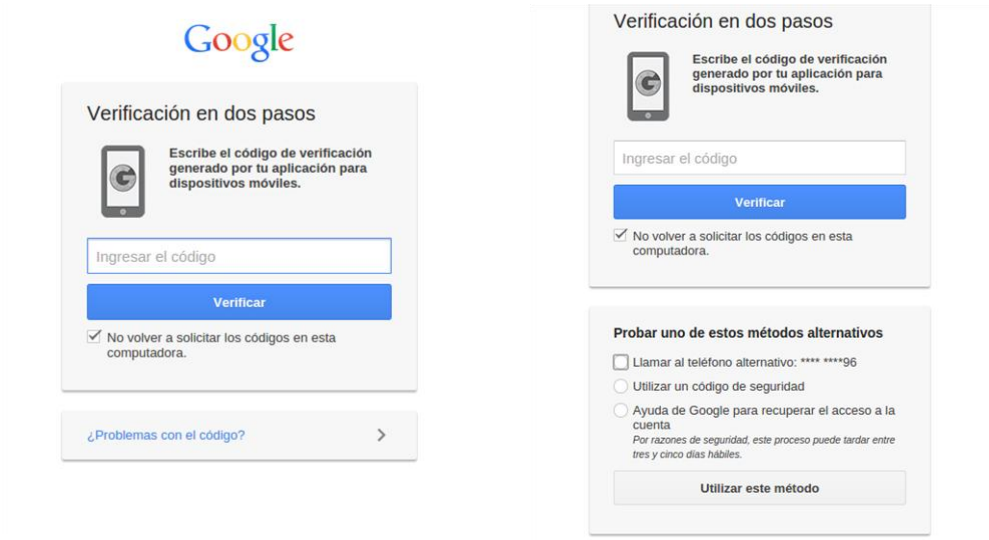
Google permite elegir métodos alternativos de autenticación para los casos en que no tengamos acceso al teléfono que habíamos configurado, por ejemplo en el caso de extravío, daños u otros imprevistos.

En la sección de configuración de la autenticación de dos pasos, en la pestaña “Códigos de verificación”, en “Opciones alternativas” podemos elegir:

1. Números de teléfono alternativos: podemos elegir recibir los códigos a través de un mensaje SMS o una llamada.

2. Códigos de Seguridad: podemos generar 10 códigos de seguridad, cada uno de los cuales será válido por una única vez. Estos códigos pueden ser impresos y/o guardados en un archivo.

Los métodos alternativos se utilizarán solamente cuando, al tratar de iniciar sesión y no poder acceder al método principal, voluntariamente elegimos usarlo. Para ello, ingresamos nuestra contraseña, y cuando nos pida el código de verificación, seleccionamos “Problemas con el código”. Se desplegará un menú donde podemos seleccionar el método alternativo que deseamos usar.



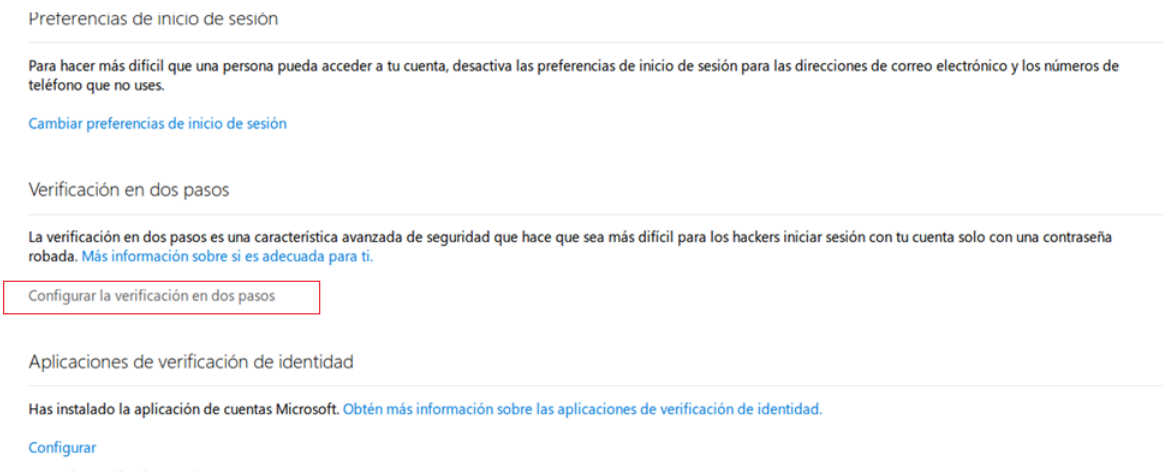
Outlook:

1. Iniciamos sesión ingresando en https://login.live.com/ o en https://outlook.com.

2. Ingresamos a la pestaña “Seguridad y Privacidad” y elegimos “Administrar seguridad avanzada”

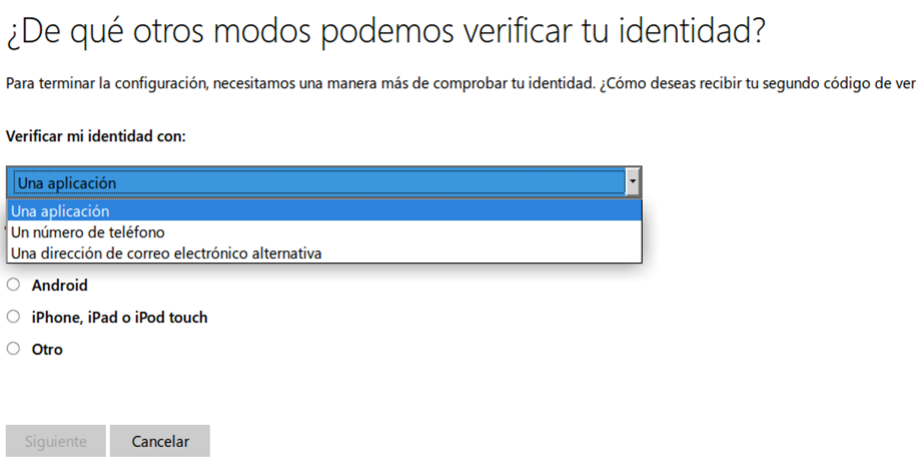
Obs.: En caso de que hayamos iniciado sesión desde Outlook, vamos a la esquina superior derecha seleccionamos nuestro perfil y entramos a “Configuración de cuenta”.

3. A continuación, en la sección “Verificación de dos pasos”, seleccionamos “Configurar la verificación de dos pasos”.



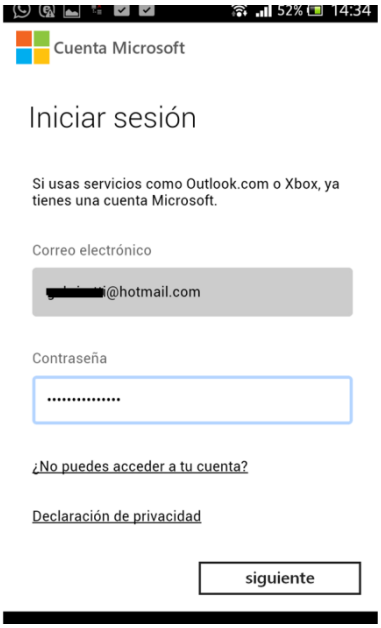
4. Debemos seleccionar el método que queremos utilizar para recibir el código; puede ser a través de:

   - la aplicación para dispositivos móviles
   - un SMS o una llamada a un número telefónico ó
   - un correo a una dirección de correo alternativa.



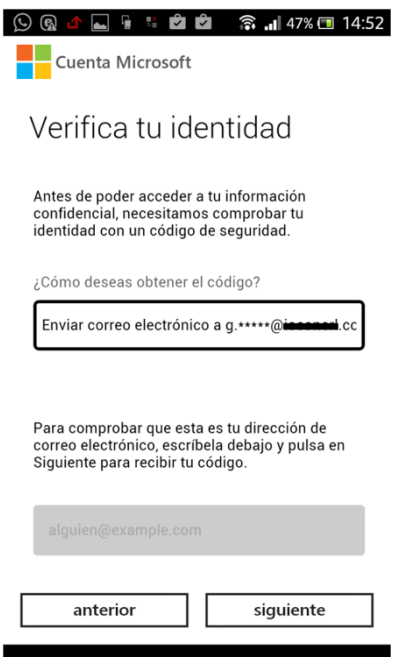
Luego de elegir el método, nos aparecerán instrucciones que deben ser seguidas. A modo de demostración, se elegirá la opción “Una aplicación”, en un dispositivo “Android”. El proceso puede variar ligeramente dependiendo del tipo de dispositivo.

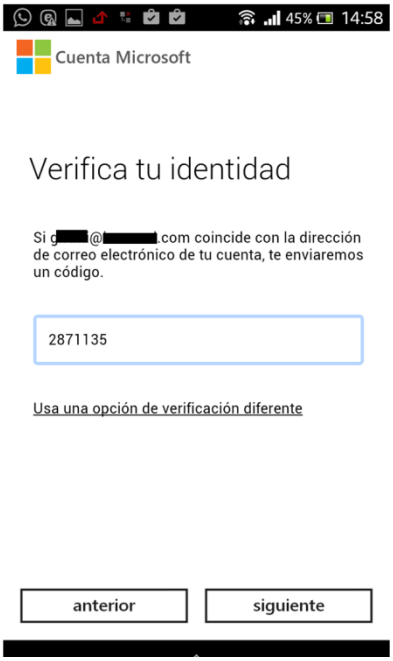
5. En el teléfono, instalamos la aplicación “Cuenta Microsoft” desde el Play Store. Luego de instalar la abrimos y seleccionamos “Configurar ahora”.



6. Completamos la información solicitada (nombre de la cuenta y contraseña) y seleccionamos “Siguiente”.

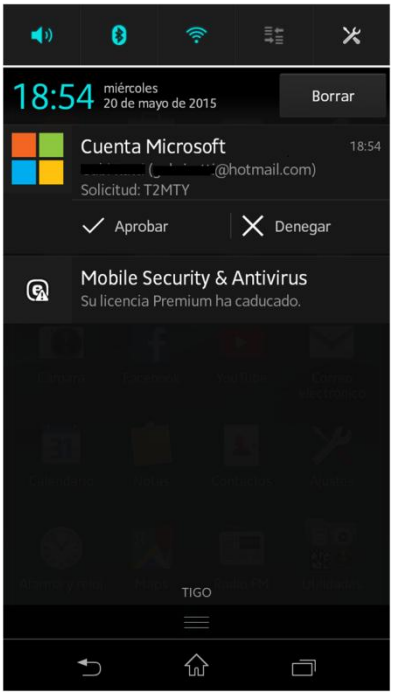
7. A continuación nos pedirá verificar nuestra identidad, enviando un código de seguridad a nuestra información de verificación que tenemos vinculada ya con anterioridad a nuestra cuenta: un SMS a nuestro número de teléfono o un correo a un correo alternativo. Seguimos las instrucciones, ingresando el código recibido, con lo cual habremos finalizado de configurar la aplicación.

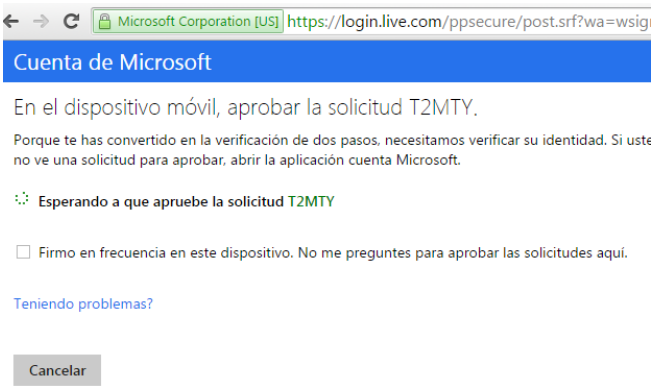




8. En el navegador donde habíamos iniciado la configuración de la autenticación de doble factor, seleccionamos “Siguiente”, con lo cual ha quedado activa la autenticación de doble factor.

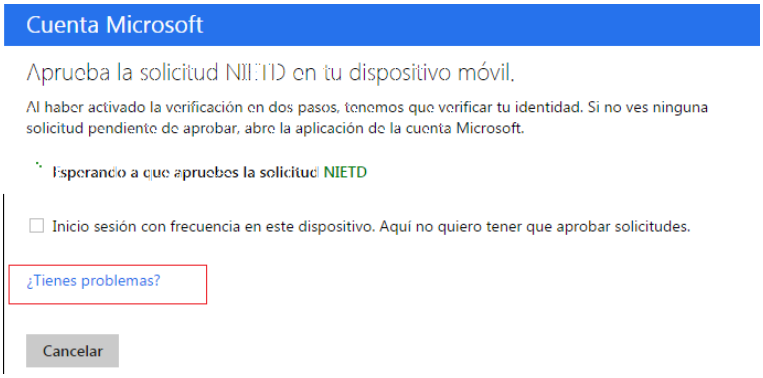
Cada vez que ingresemos nuestro usuario y contraseña, en el dispositivo móvil que hemos configurado nos aparecerá una notificación de inicio de sesión, la cual debemos aprobar. Luego, en unos segundos, el navegador o la aplicación desde donde estamos intentando acceder nos redirigirá a nuestro correo.



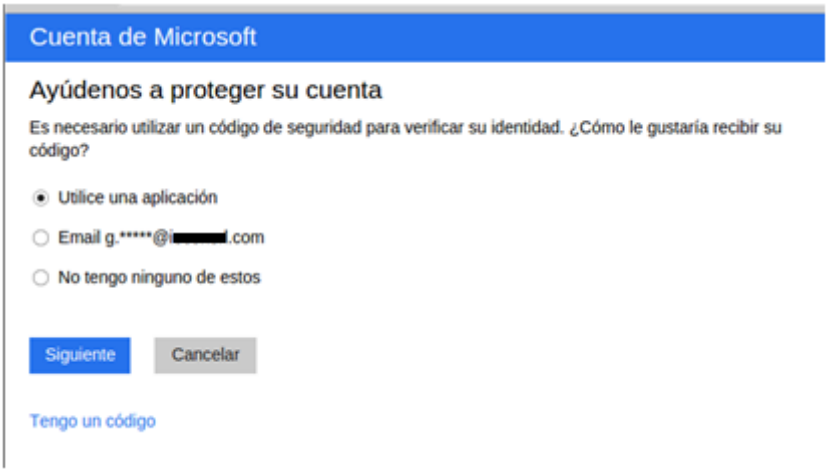


Obs.: Es importante configurar correctamente la información de recuperación de la cuenta, tales como números de teléfono alternativos, cuentas de correo alternativas y/o códigos de recuperación. Esto es de suma importancia para poder acceder a nuestra cuenta cuando no podamos utilizar el método de autenticación primario (en el caso de robo del dispositivo móvil, falta de conectividad a redes telefónicas o datos u otros inconvenientes).

En caso de no poder acceder a través del método de autenticación primario, luego de ingresar nuestro usuario y contraseña, cuando nos pide el código de verificación, seleccionamos “Tienes problemas?” o “Si no puedes usar una aplicación en este momento, obtén un código de otra manera” (el mensaje puede variar dependiendo del tipo de dispositivo).

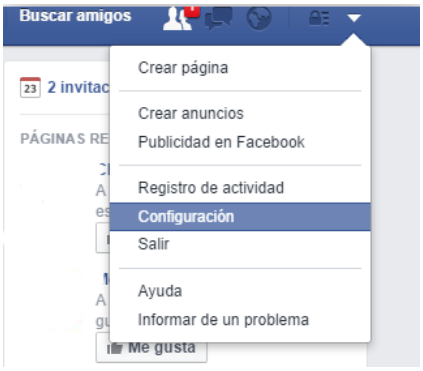


A continuación podemos seleccionar un método alternativo para recibir un código de verificación.



Facebook:

1. Luego de iniciar sesión, vamos al menú de la esquina superior derecha y seleccionamos “Configuración”.



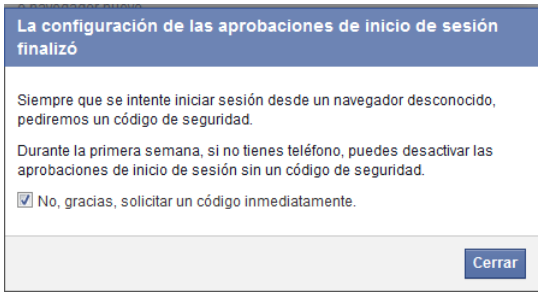
2. En la sección “Seguridad”, seleccionamos “Aprobación de inicio de sección”. Tildamos la opción “Solicitar un código de seguridad para acceder a mi cuenta desde navegadores desconocidos”. Seguimos las instrucciones en pantalla.

3. Ingresamos el número de teléfono que deseamos vincular.

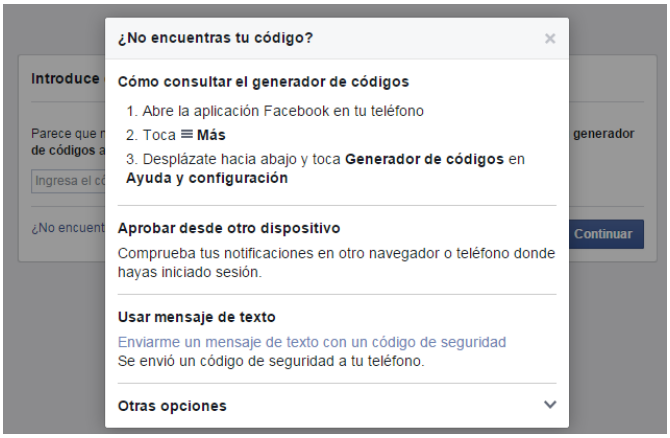
4. Recibiremos un mensaje de texto con el código de verificación, el cual debemos ingresar en el campo indicado.

5. Nos solicitará nuestra contraseña antes de continuar.

6. Durante la primera semana posterior a la activación de la autenticación de doble factor, Facebook nos da la posibilidad de iniciar sesión sin código de verificación. Sin embargo, si deseamos activarla de forma inmediata, tildamos la opción “No, gracias, solicitar un código inmediatamente”. Con esto, la autenticación de doble factor quedará activa.



7. En caso de que, cuando se requiera el código de verificación tuviéramos problemas para recibirlo, seleccionamos “¿No encuentras tu código?” y elegimos una opción.



Opcional:

Facebook ofrece métodos alternativos para obtener los códigos de verificación. Para revisar las opciones disponibles entramos a “Configuración” > “Seguridad” > “Aprobación de inicio de sesión”.

Se puede elegir configurar la aplicación de Facebook en el móvil como generador de códigos. Este método funciona cuando no tenemos conectividad a la red telefónica o de datos.

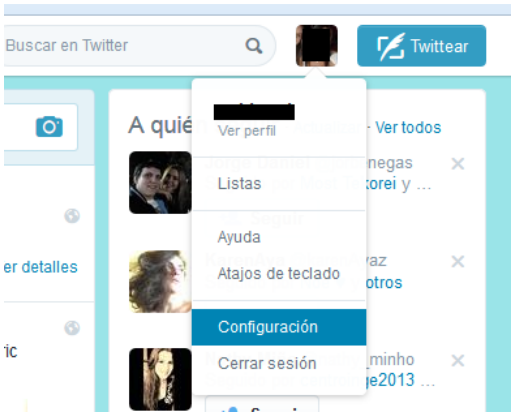
Si esta opción está activa, los códigos no llegarán a través de mensajes de texto.

También se puede obtener 10 códigos para utilizarlos cuando no tengamos acceso al teléfono vinculado, como en casos de robo, extravío, daño, etc. Estos códigos servirán una sola vez. Podemos volver a generarlos en el panel de Configuración. Se recomienda imprimir estos códigos y/o guardarlos en un archivo en un lugar seguro.

Obs.: Es importante revisar y completar las configuraciones de seguridad y privacidad disponibles, tales como “Dónde iniciaste sesión”, “Tus navegadores y aplicaciones”, “Alertas de inicio de sesión”, etc. Esto aumentará la efectividad de las medidas de seguridad tales como la autenticación de doble factor.

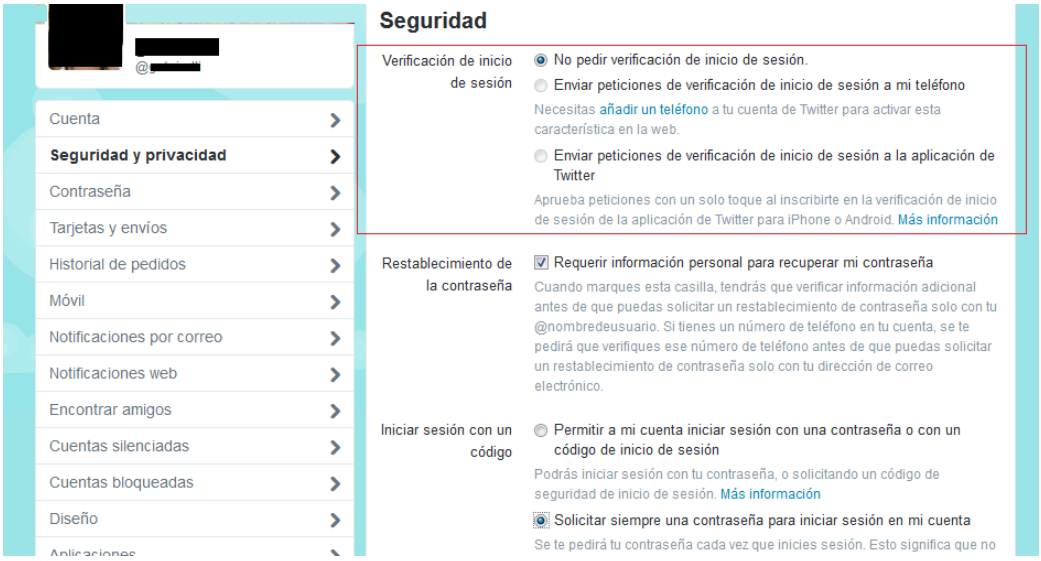
Twitter:

1. Iniciamos sesión y en la esquina superior derecha entramos a la Configuración de nuestra cuenta.



2. En la sección “Seguridad y Privacidad”, en la opción de “Verificación de inicio de sesión” tenemos dos posibles métodos que podemos elegir para recibir los códigos de verificación:

   - A través de un mensaje de texto en un teléfono
   - A través de la aplicación de Twitter



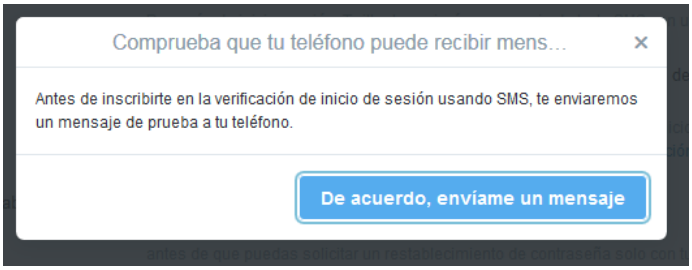
   A modo de demostración, elegiremos el método “Enviar petición de verificación de inicio de sesión a mi teléfono”.

3. Hacemos click en el enlace “añadir un teléfono” e ingresamos el número de teléfono que deseamos vincular.

4. Recibiremos un código de confirmación que debemos ingresar antes de continuar.

5. Recién ahora podemos activar la verificación de inicio de sesión en el teléfono. Regresamos a la sección de Seguridad y privacidad y seleccionamos la opción.

6. Nos pedirá una comprobación de que el teléfono vinculado puede recibir mensajes, para lo cual debemos seleccionar "De acuerdo, envíame un mensaje". En caso de recibir un mensaje, lo confirmamos en la siguiente pantalla eligiendo "SI".



7. Antes de finalizar nos solicitará nuevamente nuestra contraseña, con lo que la autenticación de doble factor quedará activa.

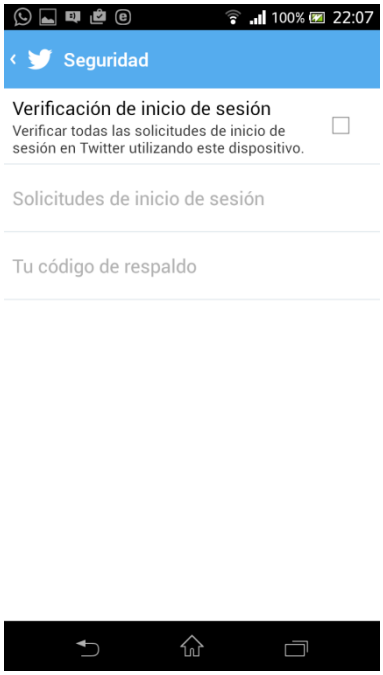
Opcional:

Twitter ofrece un segundo método de autenticación en el cual las solicitudes de inicios de sesión deben ser autorizadas a través de la aplicación de Twitter de un dispositivo móvil determinado. A modo de mostración, mostramos la configuración en un dispositivo Android. En otros sistemas operativos el proceso puede ser ligeramente diferente.

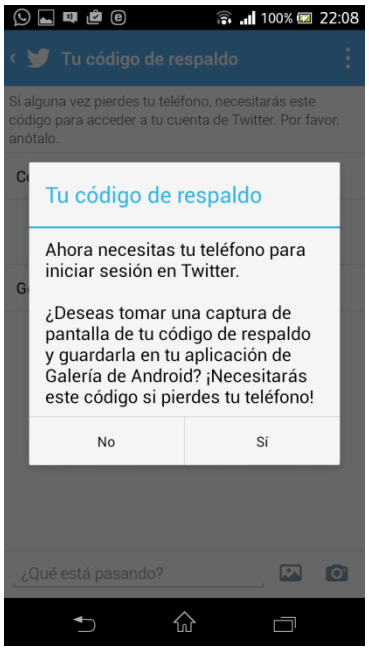
1. Iniciamos sesión en la aplicación de Twitter para Android con nuestro usuario y contraseña. En caso de haber activada la verificación de inicio de sesión a través de un teléfono, debemos introducir además el código de verificación que nos llegará a través de SMS.

2. En la aplicación, hacemos click sobre los tres puntos en la esquina superior derecha, seleccionamos "Configuración" y elegimos el usuario de la cuenta que deseamos configurar.

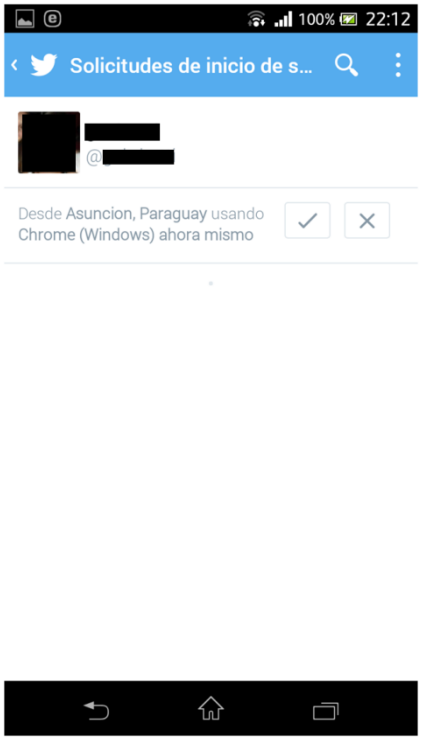
3. Entramos en la sección "Seguridad" y tildamos la opción "Verificación de inicio de sesión". Nos advertirá que necesitaremos iniciar sesión con el dispositivo actual.

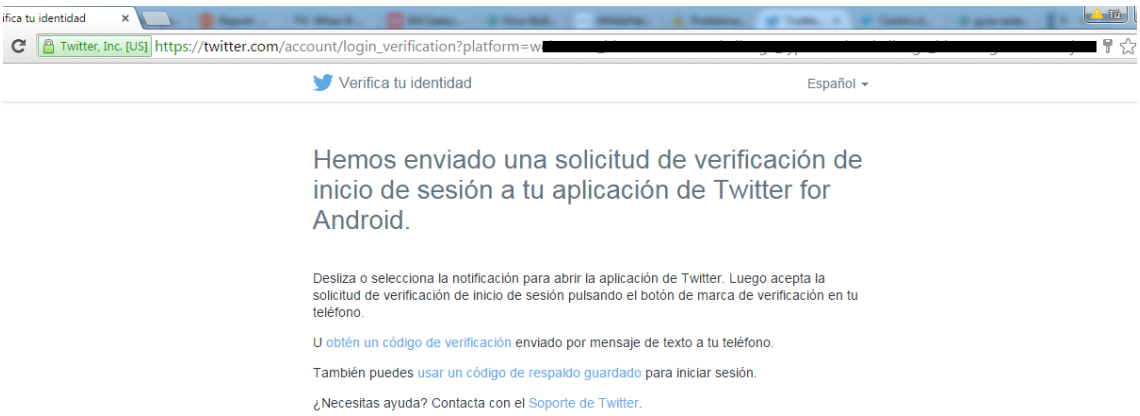


4. A continuación se nos solicitará que hagamos una captura de pantalla y/o que guardemos el código de respaldo en caso de que no tengamos acceso al dispositivo, como en caso de robo, extravío, daño u otros imprevistos. Seleccionamos “Si” para resguardar el código de respaldo.



Cuando deseamos iniciar una sesión en otro dispositivo o a través de un navegador, luego de ingresar el usuario y contraseña, recibiremos una notificación en la aplicación que hemos configurado. Debemos aprobar dicha solicitud de modo a que se pueda completar el inicio de sesión desde el otro dispositivo o navegador, que será redirigido luego de la aprobación.



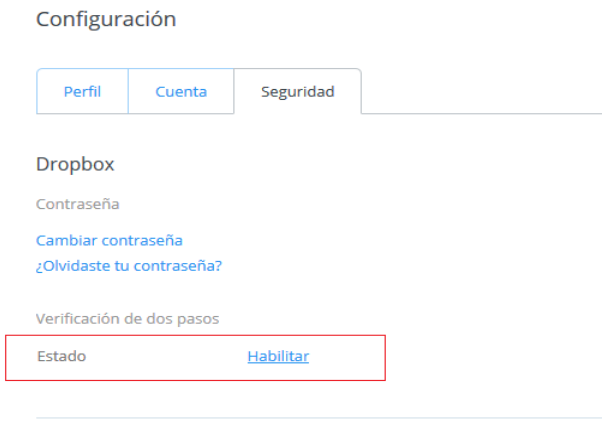


Obs.: Al activar este método, éste pasará a ser el método de verificación principal, por lo que ya no recibiremos mensajes de texto con códigos de verificación. Todas las solicitudes de aprobación de inicio de sesión se recibirán en la aplicación del dispositivo vinculado.

Dropbox:

1. Iniciamos sesión con nuestra cuenta y en la esquina superior derecha seleccionamos “Configuración”.

2. Seleccionamos la pestaña “Seguridad”, y en la opción Verificación de dos pasos, elegimos “Habilitar”.

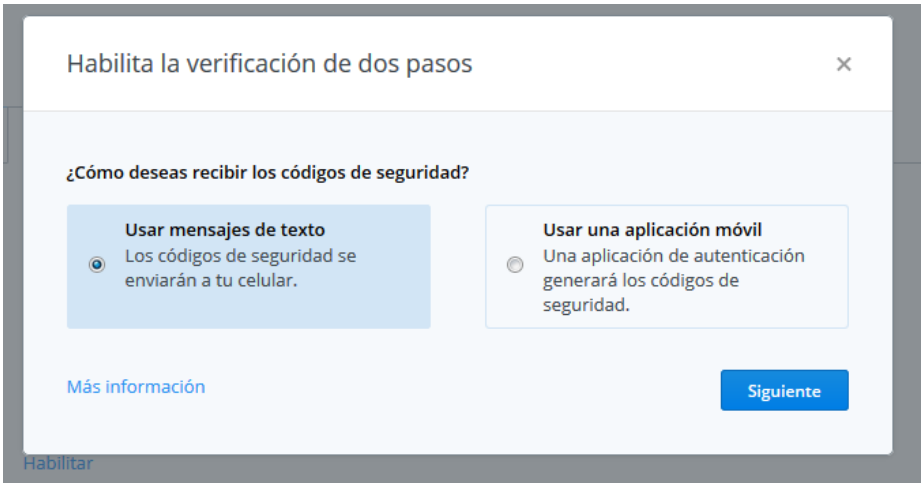


3. Se abrirá un asistente de configuraciones cuyas instrucciones debemos seguir.

4. Introducimos nuestra contraseña para continuar.

5. Dropbox ofrece dos métodos para recibir los códigos de verificación:

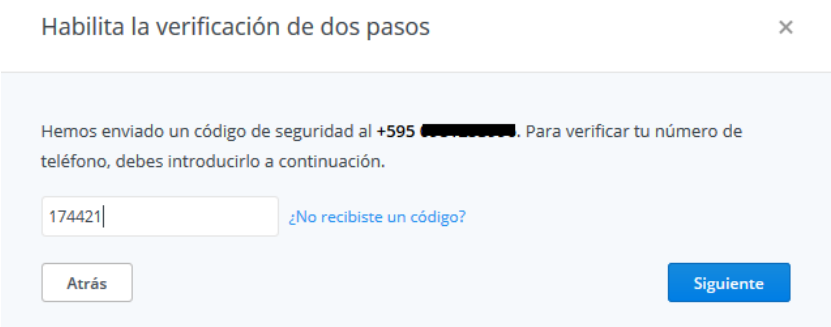
    - A través de un mensaje de texto a un número de teléfono
    - A través de una aplicación de autenticación.



    A modo de demostración elegiremos el primer método.

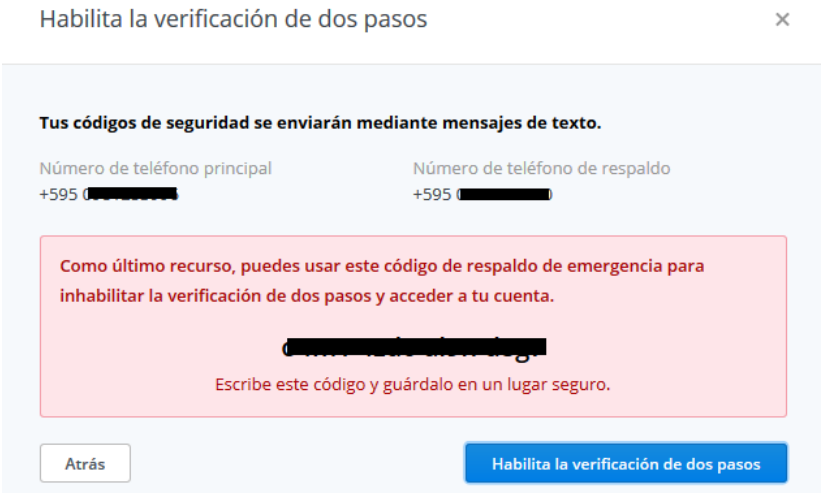
6. Introducimos el número de teléfono que deseamos vincular.

7. A continuación recibiremos un mensaje de texto con el código de verificación, que debemos introducir antes de continuar.



8. Si deseamos, podemos introducir un número de teléfono alternativo en el que podemos recibir el código en caso de que no tengamos acceso al número que vinculamos.

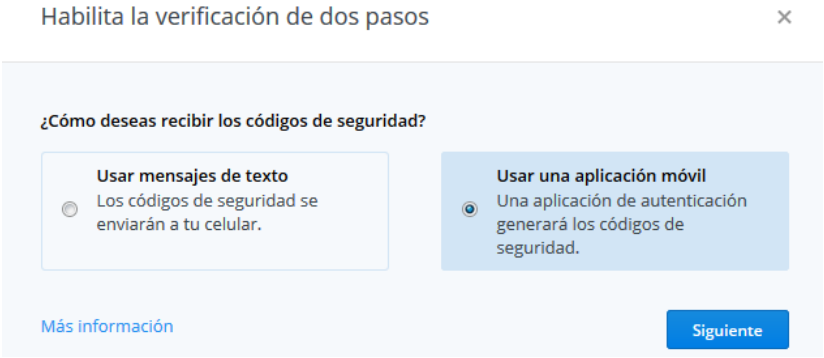
9. Dropbox generará un código de respaldo único que podrá ser utilizado para acceder a la cuenta en caso de que no podamos recibir el código de verificación en ninguno de los números vinculados. Dicho código debe ser guardado en un lugar seguro. Con esto quedará habilitada la autenticación de doble factor.



Opcional:

El método de mensaje de texto a un número celular funcionará únicamente si tenemos conectividad a la red telefónica o de datos. El segundo método, con el cual recibimos el código a través de una aplicación, no requiere que esté disponible ninguna conectividad.

1. En la configuración de la autenticación de doble factor, elegimos el segundo método “Usar una aplicación móvil”.



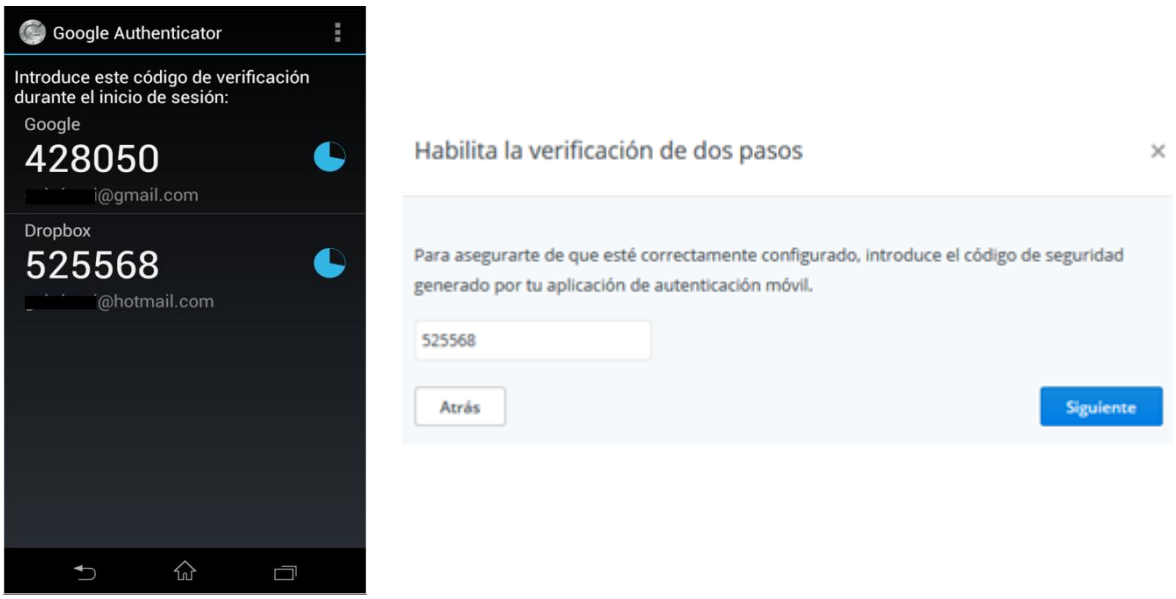
2. Podemos elegir entre varias aplicaciones de autenticación, tales como Authenticator de Google, Duo Mobile, Amazon AWS MFA, etc. A modo de demostración, utilizaremos Authenticator de Google (disponible para iOS, Android y Blackberry desde los app store).

3. Una vez instalada la aplicación Authenticator de Google, la abrimos y hacemos click sobre los tres puntos verticales en la esquina superior derecha y elegimos “Configurar cuenta”.

4. Para añadir la cuenta, seleccionamos “Escanear código de barras”. Luego de que el código QR sea reconocido, la cuenta quedará añadida a la aplicación y se empezarán a generar los códigos.

Obs.: alternativamente, se puede seleccionar la opción de introducir una clave proporcionada, para lo cual debemos hacer click sobre el enlace de “especifica manualmente tu clave secreta”, que se encuentra en el asistente de configuración de Dropbox. Obtendremos una clave que es la que debemos introducir en la aplicación del teléfono.

5. A continuación ingresamos el código de 6 dígitos generado para la cuenta de Dropbox en la aplicación, atendiendo de introducirlo antes de que expire su tiempo de vida.



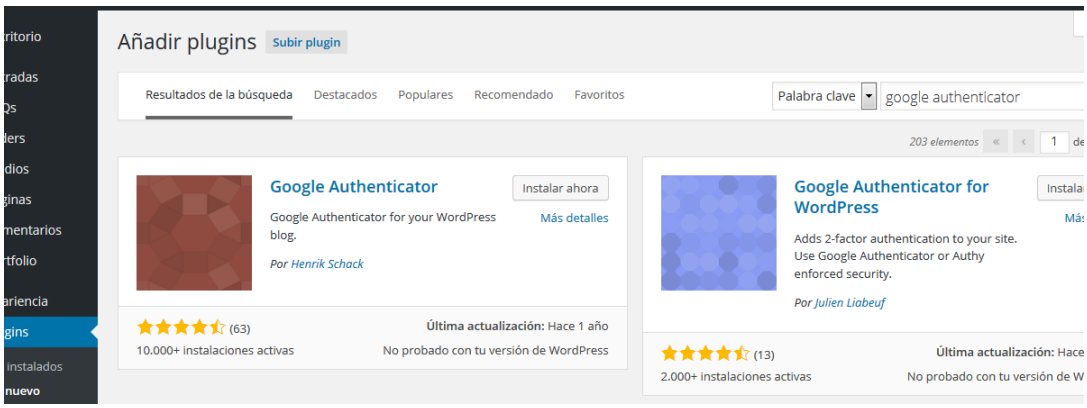
6. Se nos solicita un número de teléfono de respaldo, como método alternativo para recibir el código de verificación si es que no tenemos acceso a la aplicación. Se genera además un código de respaldo de emergencia el cual debe ser guardado en un lugar seguro, en caso de que los demás métodos fallaran o no estuvieran disponibles. Con esto, la autenticación de doble factor quedará habilitada.

Wordpress:

Existen múltiples plugins para Wordpress que integran la autenticación de doble factor al sitio web. Muchos de estos plugins se basan en el esquema de autenticación de Google, a través de su aplicación Google Authenticator. Veremos cómo implementar uno de estos plugins a Wordpress.

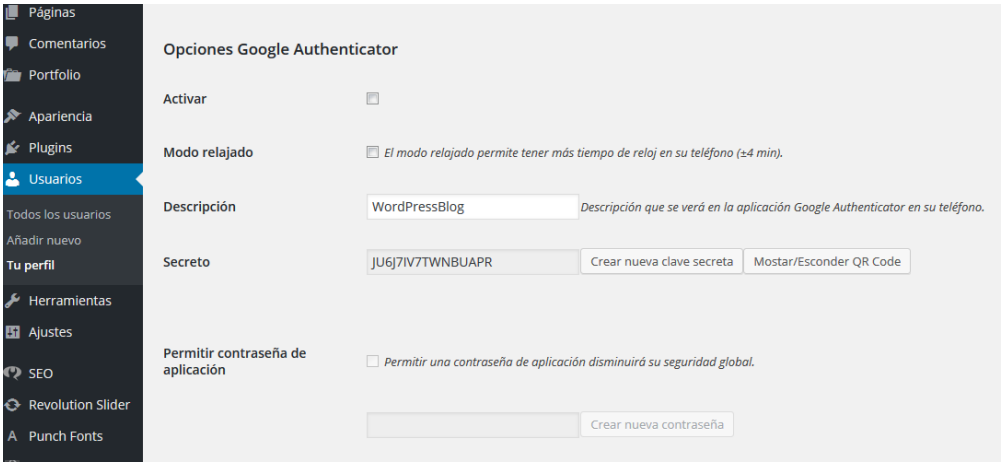
1. Iniciamos sesión como Administrador en nuestro sitio web.

2. Vamos a la pestaña Plugins y elegimos “Añadir nuevo”. Buscando “Google Authenticator”, vemos que aparecen varios plugins. A modo de demostración elegiremos “Google Authenticator” de Henrik Schack. Seleccionamos “Instalar ahora” y lo activamos.



Obs.: El plugin podría ser descargado de https://wordpress.org/plugins/google-authenticator/ e instalado de forma manual.

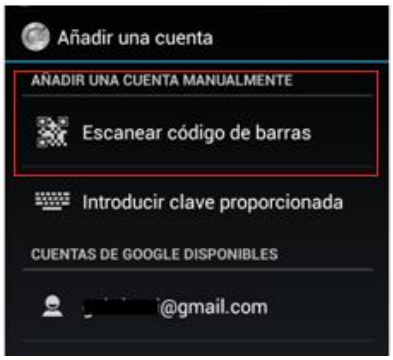
3. Para configurarlo, una vez instalado y activado el plugin, vamos al perfil del usuario en el que aparecerán unas opciones extras.



4. Tildamos la opción “Activar”.
5. En caso de que lo deseemos, tildamos la opción “Modo relajado”, el cual aumentará el tiempo de vida del código generado por la aplicación. Si no lo tildamos, el tiempo de vida por defecto es de 30 segundos.
6. Editamos la descripción que veremos en la aplicación.
7. Para configurar la cuenta en la aplicación Authenticator de Google (instalada previamente en el teléfono móvil, ver instrucciones en la sección “Autenticación de doble factor – Google”), podemos

optar por introducir la clave secreta de forma manual o a través de un código QR. En caso de que deseemos utilizar el código QR, seleccionamos “Mostrar/Esconder QR Code”.

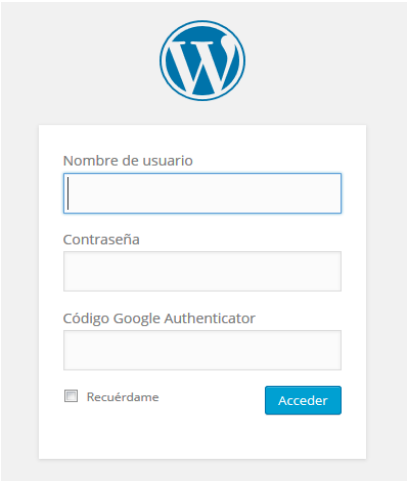
8. Para añadir la cuenta, abrimos la aplicación Authenticator en nuestro dispositivo móvil y seleccionamos “Escanear código de barras”. Luego de que el código QR sea reconocido, la cuenta quedará añadida a la aplicación y se empezarán a generar los códigos.



Obs.: alternativamente, se puede seleccionar la opción “Introducir clave proporcionada”, para lo cual debemos copiar manualmente la clave “Secret” generada en Wordpress.

9. Para finalizar, seleccionamos “Actualizar perfil” en nuestro sitio de Wordpress, con lo que quedará activada la autenticación de doble factor para dicho usuario. La configuración debe realizarse para cada usuario.

Cuando deseamos iniciar sesión en nuestro sitio, nos aparecerá un campo adicional en el cual nos solicitará el código de verificación generado en la aplicación Authenticator.



Gestores de contraseñas

Entre las recomendaciones para proteger las contraseñas, se ha mencionado la importancia de elegir contraseñas largas, diferentes para cada servicio y cambiarlas regularmente. Sin embargo, esto dificulta enormemente recordar todas estas contraseñas, por lo que nos dificulta nuestra vida cotidiana.

Por estas razones se han desarrollado soluciones como los gestores de contraseñas. Son programas que se utilizan para almacenar una gran cantidad de conjuntos de usuario-contraseña. La base de datos donde se guarda esta información está cifrada mediante una única clave (contraseña maestra o *master password*), de forma que el usuario sólo tenga que memorizar una clave para acceder a todas las demás. Esto facilita la administración de contraseñas y fomenta que los usuarios escojan claves complejas sin miedo a no ser capaces de recordarlas posteriormente.

Es fundamental que la contraseña maestra sea lo suficientemente compleja para que sea difícil de romper, ya que si un atacante consiguiera conocer la contraseña maestra y acceder a la base de datos del programa, ganaría acceso a todas nuestras claves.

Por eso, también es importante elegir un gestor de contraseñas que ofrezca autenticación de doble factor, además de otros mecanismos de seguridad que protejan nuestras contraseñas. Existen gestores de contraseñas que almacenan los datos de forma local, en el ordenador, y también existen otros que almacenan los datos online, en la nube. La mayoría de los navegadores también implementa funciones de almacenamiento de contraseñas básicas.

A continuación presentamos algunos gestores de contraseñas más conocidos:

- LastPass: una herramienta gratuita basada en web, de código abierto, que se integra al navegador, por lo que puede ser utilizado en Windows, Mac, Linux y móviles. www.lastpass.com
- Dashlane: otra herramienta basada en web, cuenta con una versión gratuita y otra de pago. https://www.dashlane.com/es/passwordmanager
- 1Password: disponible para varios sistemas operativos. https://agilebits.com/onepassword
- KeePassX: una herramienta gratuita, de código abierto, disponible para varios sistemas operativos. http://www.keepassx.org
- KeePass: una herramienta gratuita de código abierta, para Windows. Es el antecesor de KeePassX. http://keepass.info

Muchas soluciones de antivirus incorporan funciones de administración de contraseñas, como por ejemplo:

- Norton Identity Safe
- Kaspersky Password Manager
- Avast Easy Pass
- McAfee LiveSafe

Debido a que la seguridad de las contraseñas almacenadas dependerá de una única contraseña maestra, esto puede constituir un punto único de fallo. Por eso siempre es recomendable combinar los gestores de contraseñas con otros mecanismos de seguridad. Un ejemplo puede ser dejar las cuentas importantes (correo, bancos) con contraseñas seguras que no se guarden en el gestor y protegidas con autenticación en dos pasos, y utilizar el gestor para cuentas menos sensibles tales como foros, sitios de descarga, etc, que muchas veces no poseen mecanismos de autenticación de doble factor integradas.

Correo electrónico

El correo electrónico se ha convertido en un medio de comunicación utilizado a diario, tanto en el ambiente personal como en el ambiente laboral. En el ambiente laboral por lo general contamos con un correo corporativo, proporcionado por nuestra empresa, por lo tanto para su utilización, por lo general, debemos atender las políticas de ésta: marco legal, políticas de seguridad, código de ética, etc.

El correo electrónico es uno de los principales puntos de entrada de los atacantes, ya sea como fuente de información valiosa (conversaciones confidenciales, datos sensibles, documentos, etc.) así como también como un medio de distribución de malware para conseguir acceso a la red de la empresa.

Los principales riesgos relacionados al correo electrónico son el spam y el phishing.

Spam

Es el correo electrónico que promociona diferentes productos y servicios a través de publicidad no solicitada, enviada masivamente a las direcciones de correo de los usuarios. Constituye uno de los principales medios de propagación de una importante cantidad de códigos maliciosos: virus, troyanos, gusanos y otros tipos de malware.

Cuando no se siguen buenas prácticas en el uso del correo electrónico, podemos convertirnos en receptores de spam así como también en generadores de spam, es decir, nuestras cuentas de correo pueden ser utilizadas para enviar spam a otros. Esto normalmente causa enormes problemas a las organizaciones, que observan diversos síntomas como: lentitud en el servicio de correo, los correos enviados no llegan a destino, intermitencia en otros servicios, entre otros.

Algunas de las recomendaciones y buenas prácticas para evitar ser víctimas y/o generadores de spam son las siguientes:

1. No confiar en correos spam con archivos adjuntos y explorar el archivo antes de ejecutarlo. Esto minimiza la posibilidad de ejecutar un malware.
2. Cuando se reciben adjuntos, prestar especial atención a las extensiones de los mismos, ya que suelen utilizar técnicas de engaño como la doble extensión, espacios entre el nombre del archivo y la extensión del mismo, u otras técnicas similares.
3. Como medida de seguridad extra, bloquear las imágenes de los correos y descargarlas cuando se asegure de que el correo no es dañino
4. Evitar publicar las direcciones de correo en sitios web de dudosa reputación como sitios pornográficos, foros, chats, entre otros. Esto minimiza la posibilidad de que la dirección se guarde en la base de datos de los spammers.
5. Proteger la dirección de correo utilizando una cuenta alternativa durante algún proceso de registro en sitios web y similares. Esto previene que la dirección de correo laboral sea foco del spam.
6. Utilizar filtros anti-spam que permitan el filtrado del correo no deseado.
7. No responder jamás el correo spam. Es preferible ignorarlos y/o borrarlos, ya que si se responde se confirma que la dirección de correo se encuentra activa.
8. Cuando recibimos un correo fraudulento, es importante reportarlo como spam. La mayoría de los servicios de correo incluyen la opción de “Marcar como Spam”, “Correo no deseado” o similar.
9. Evitar el reenvío de mensajes en cadena, ya que suelen ser utilizados por spammers para recolectar direcciones de correo activas.

10. Cuando deseamos enviar un mensaje a múltiples contactos, es recomendable hacerlo siempre Con Copia Oculta (CCO) para que quien lo recibe lea solo la dirección del emisor. Esto evita que los filtros anti-spam nos incluyan en listas negras. Cuando nuestra dirección es incluida en una lista negra, por lo general se observan dificultades para enviar correos.
11. Cuando vamos a enviar un correo a muchos contactos (normalmente más de 10 ~ 15), se debe evitar incluirlos a todos como destinatarios. Para el correo masivo se deben utilizar mecanismos como listas de distribución, herramientas o servicios de telemarketing, etc. Esto evita que los filtros anti-spam nos incluyan en listas negras.
12. Seguir buenas prácticas para las contraseñas, utilizando claves robustas, cambiándolas con periodicidad, activando la autenticación de doble factor siempre que sea posible, etc.

Phishing

Es una modalidad delictiva encuadrada en la figura de estafa o engaño realizado a través de

Internet, y constituye otra de las amenazas de seguridad más propagadas a través del correo electrónico. A través de este engaño el atacante busca que la víctima le proporcione información útil o confidencial.

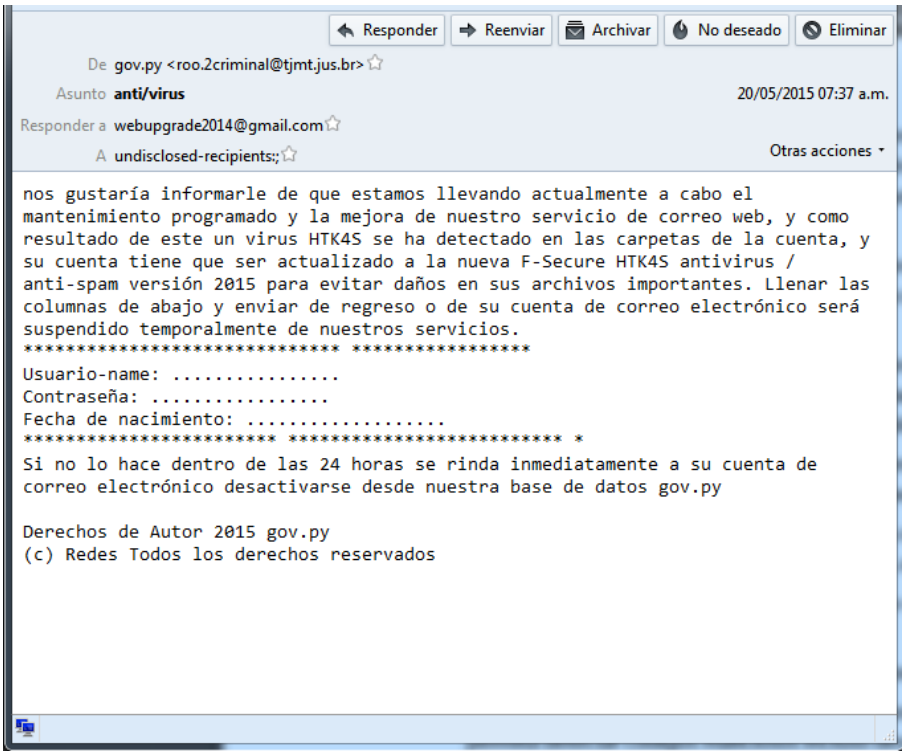


Figura: Ejemplo de phishing. Se observa que el mismo apunta específicamente a funcionarios de instituciones gubernamentales de Paraguay.

1. Tener en cuenta que las entidades bancarias y financieras no solicitan datos confidenciales a través de este medio, de esta manera se minimiza la posibilidad de ser víctima de esta acción delictiva.
2. Desconfiar de los correos que dicen ser emitidos por entidades que brindan servicios y solicitan cambios de datos sensibles (contraseñas, números de tarjeta, códigos de seguridad, etc.) ya que suelen ser engaños.
3. No hacer clic sobre enlaces que aparecen en el cuerpo de los correos electrónicos, ya que pueden redireccionar hacia sitios web clonados o hacia la descarga de malware. Hoy en día existen técnicas

mediante las cuales se puede infectar un equipo con solo entrar a un sitio web, sin que la víctima haya descargado ni ejecutado nada de forma intencional.

4. Asegurarse de que la dirección del sitio web al cual se accede comience con el protocolo https. La "s" final, significa que la comunicación con la página web es privada y que toda la información intercambiada con la misma viajará de manera cifrada.
5. Observar con atención el remitente del correo, no solo el nombre que figura sino también la dirección de correo. Si bien, existen técnicas que pueden camuflar la dirección de correo, esta medida puede protegernos en muchos casos.
6. Tener mucho cuidado con el correo que llega a la bandeja de correo no deseado. Si bien, en ocasiones el correo legítimo puede terminar en la bandeja de spam, en muchos casos el correo que se encuentra allí es malicioso. Si no estamos absolutamente seguros que es un correo legítimo, no debemos abrirlo.
7. Comunicarse telefónicamente con la persona u organización que dice ser el remitente para descartar la posibilidad de ser víctimas de un engaño, si se tiene dudas sobre la legitimidad de un correo.
8. Jamás se debe enviar contraseñas, números de tarjetas de crédito u otro tipo de información sensible a través del correo electrónico, ya que la comunicación podría ser interceptada y robada.
9. Habituarse a examinar periódicamente la actividad en las cuentas (bancarias, de correo, de redes sociales, etc.), a fin de detectar a tiempo alguna actividad extraña relacionada con la manipulación de la cuenta o transacciones no autorizadas.

Enlaces falsos ocultos

Cuando nos encontramos con un enlace dentro de un correo u otro tipo de mensaje, normalmente no vemos el enlace en sí sino un texto, que puede coincidir con el enlace real como puede no coincidir. Frecuentemente los ciberdelincuentes ocultan los enlaces maliciosos detrás de textos que simulan ser un enlace legítimo.
Para poder determinar el enlace real al que se va a acceder, debe posicionar el cursor del mouse sobre el enlace, sin hacer click sobre él. En la esquina inferior izquierda se podrá observar el enlace real. Si el mismo es sospechoso o no corresponde al esperado, nunca se debe hacer click.
En la siguiente figura se observa en los recuadros rojos los enlaces reales (http://br.youtube.jskgosi.co.kr/img/4763432/...), el cual es diferente al enlace mencionado en el texto (http://www.youtube.com/watch?v=...)

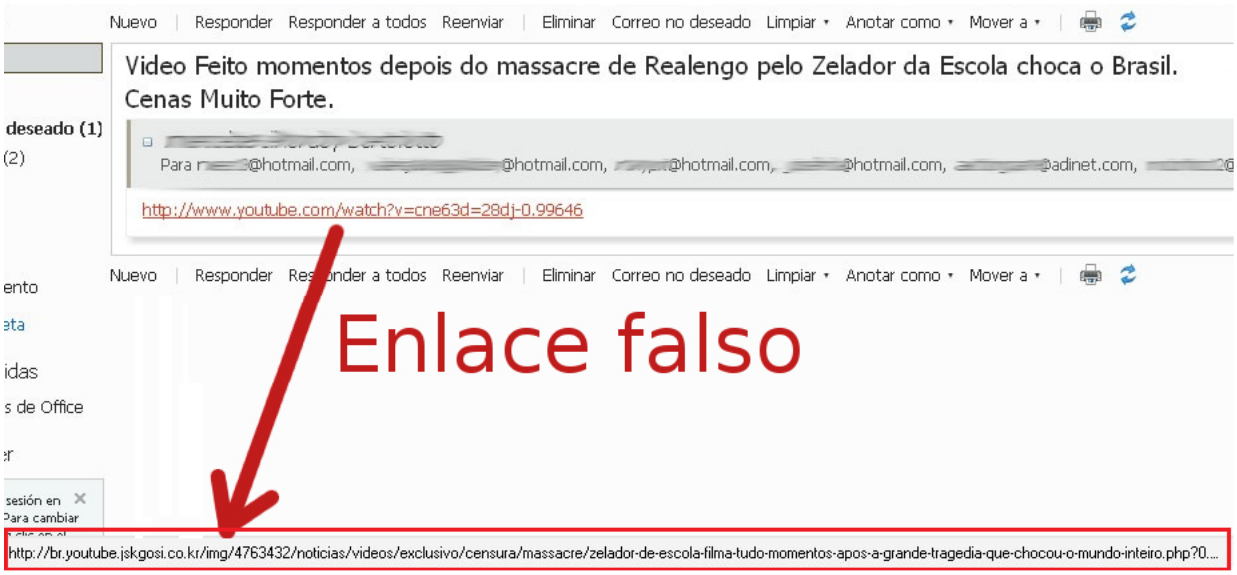


Figura: Ejemplo de enlace falso oculto

Remitentes falsos ocultos

Para un ciberdelincuente es muy fácil falsificar el remitente de un correo, de modo a que parezca que otra persona lo envió. La única forma de determinar con certeza el origen de un correo electrónico, es observando el código fuente.
En la siguiente figura, se observa un correo electrónico que aparentemente fue enviado por "Dirección de Infraestructura direccioninfra@senatics.gov.py".

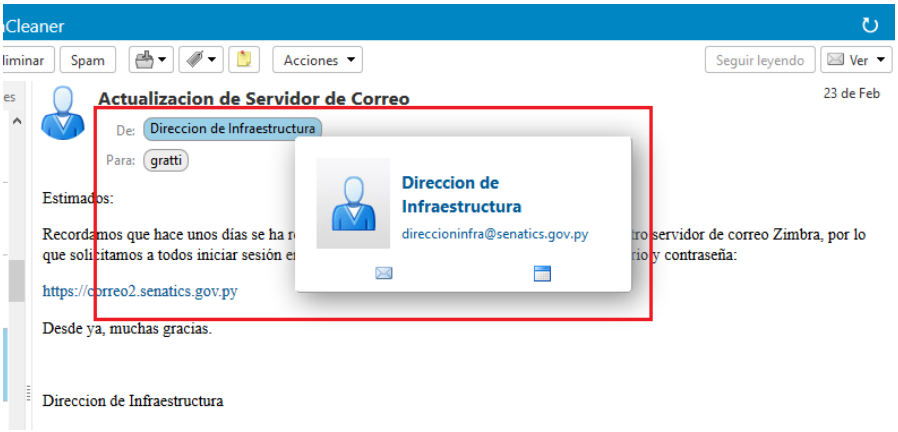


Figura: Mensaje con remitente falsificado

Sin embargo, en el código fuente se puede observar que el origen real del correo es completamente distinto y que no ha sido enviado desde el servidor de correo que aparenta (senatics.gov.py) sino desde server1.hmereles.com

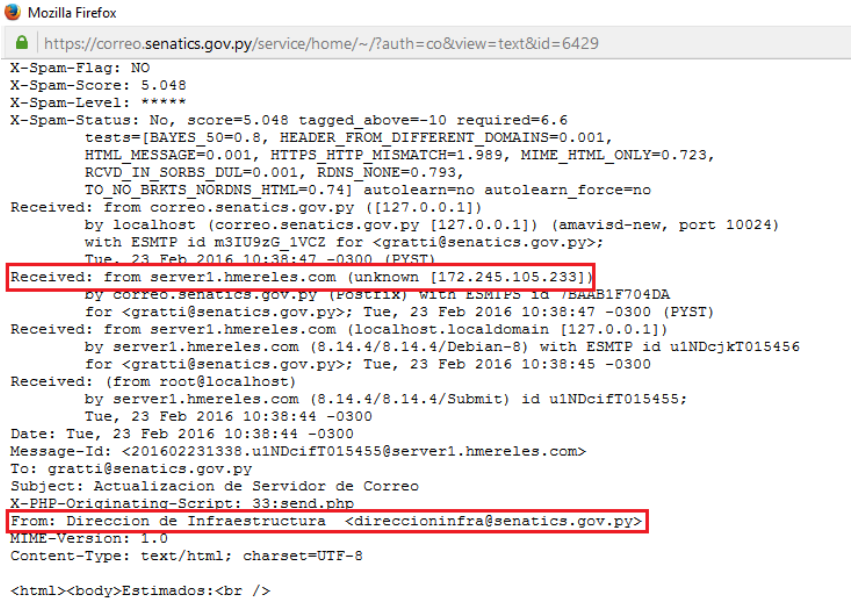


Figura: Código fuente del mensaje

De acuerdo a cada tipo de correo (Outlook, Google, Zimbra, Thunderbird, etc.) los pasos para visualizar el código fuente del correo pueden variar ligeramente. En el caso de Zimbra, para observar el código fuente se debe ir al mensaje en cuestión, seleccionar "Acciones" > "Mostrar origianl". Se abrirá una nueva ventana con el código fuente. Para determinar el origen y la ruta seguida por el mensaje, se debe observar los campos "Received from:", empezando de abajo hacia arriba.
En caso de encontrar alguna inconsistencia, se debe considerar el correo como sospechoso y reportarlo. Ante la duda, se debe comunicar personalmente con el supuesto remitente, de modo a determinar si realmente envió el mensaje.

Ingeniería Social

La ingeniería social es una técnica mediante el cual el atacante busca, a través de la interacción humana y haciendo uso de habilidades sociales, engañar a la víctima para obtener información personal o de una organización para acceder a sus sistemas informáticos.

Los ataque de ingeniería social muchas veces buscan, a través del engaño, que el usuario realice una acción tal como ingresar a un enlace o abrir un archivo, que infectan el equipo del usuario y le proporcionan al atacante un punto de entrada para la siguiente fase del ataque.

En la sección anterior se explicó brevemente el Phishing, que es una de las técnicas de ingeniería social más conocidas, sin embargo no es la única. Un ataque de ingeniería social puede ser por ejemplo:

1. Una llamada telefónica, donde el interlocutor se presenta como miembro del Departamento de Soporte Técnico de la compañía donde trabajamos y nos solicita que le proporcionemos nuestra contraseña de acceso a la red interna de la empresa para realizar operaciones de mantenimiento.

2. Un correo electrónico informándonos que hemos sido seleccionados para una promoción especial y que debemos enviar cierta información personal. Incluso, en algunos casos nos piden enviar dinero a una cuenta, bajo el pretexto de cubrir los gastos administrativos.

3. Un anuncio atractivo embebido en una página web (incluso puede ser un sitio totalmente confiable), el cual nos induce a hacer click sobre él. También pueden ser anuncios que alertan sobre un aparente peligro, tal como “Su máquina está infectada por un virus, haga click aquí para eliminarlo”. Otras veces pueden ser mensajes que nos indican que debemos instalar un supuesto complemento o programa para que la web funcione correctamente.

4. Un correo electrónico informándonos que se produjo un problema de seguridad que afecta nuestra cuenta bancaria o nuestro equipo y que por esta razón se requiere urgentemente nuestro usuario y contraseña para solucionarlo. Los mensajes que infunden el miedo en el usuario y que simulan una urgencia o peligro inminente muchas veces son efectivos e inducen a las víctimas a tomar las decisiones erróneas, debido al factor psicológico de la presión y el miedo.

5. Una publicación llamativa en las redes sociales, muchas veces aparentan ser videos impactantes, titulares de noticias llamativas, etc., las cuales al hacer click sobre ellas muchas veces nos piden nuestro usuario y contraseña para poder visualizarlos. En la mayoría de los casos, se trata de técnicas para robar nuestras credenciales.

Las técnicas pueden ser tan variadas como la creatividad del atacante lo permita, y muchas veces puede llegar a ser muy convincentes. En todas ellas, el factor común es el engaño al ser humano, manipulándolo a través de sus emociones: curiosidad, miedo, empatía, vanidad, etc.

Es por esto que para la ingeniería social, la protección más efectiva es la prudencia permanente, así como las buenas prácticas mencionadas, que deben ser adoptadas siempre, en todo momento y en todo lugar, tanto en entornos empresariales como personales.

Navegación Segura

Las técnicas de ataque a través de la navegación en Internet son tan diversas y cada día más sofisticadas por lo que muchas veces no es suficiente con seguir las buenas prácticas y recomendaciones básicas, y se requiere de protecciones más efectivas y proactivas.

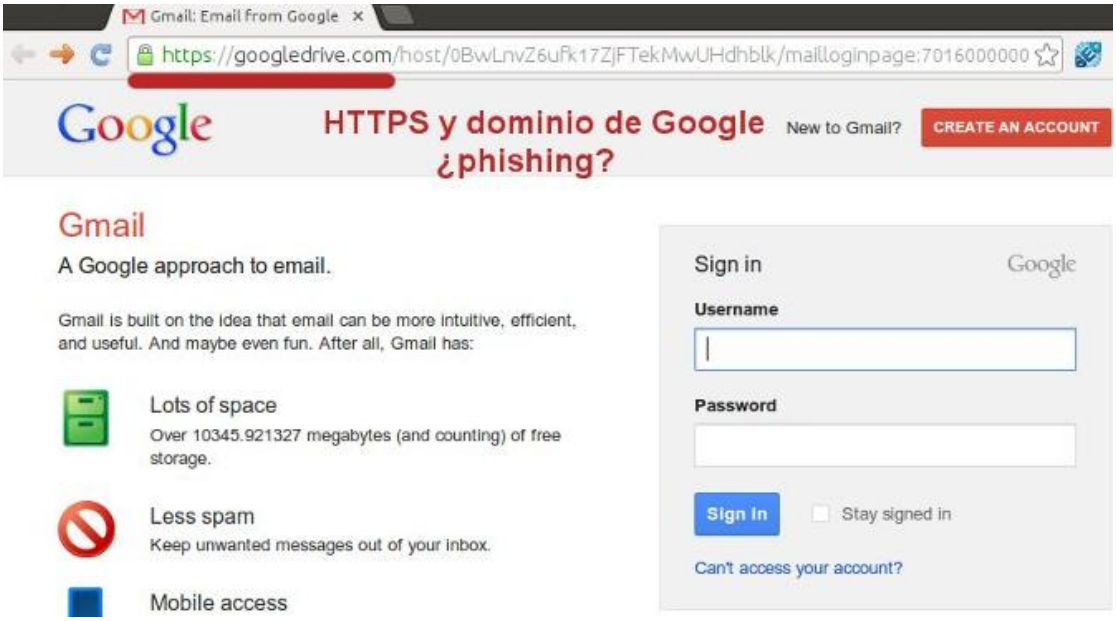


Figura: Ejemplo de phishing más sofisticado donde los atacantes alojan un sitio fraudulento, igual a la página de inicio de Gmail, alojada en Google Drive, engañado incluso a usuarios más cuidadosos

Es por eso que la industria de seguridad ha desarrollado diversas herramientas orientadas a usuarios de niveles de conocimiento básicos hasta avanzados, que lo pueden proteger durante la navegación. Entra estas herramientas, podemos resaltar las medidas de protección que están incluidas en los navegadores o que pueden ser integradas a los mismos a través de los complementos o *add-ons*.

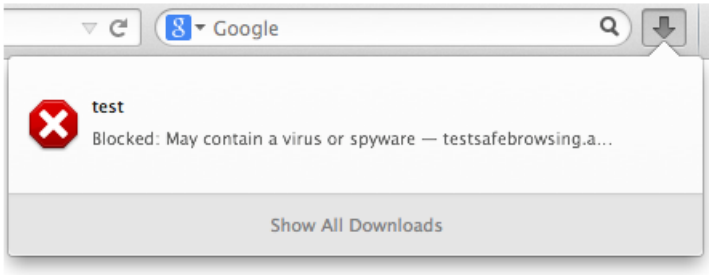
Veremos algunas de estas medidas de protección y cómo activarlas en los navegadores más utilizados.

Mozilla Firefox:

El navegador Firefox ofrece un mecanismo de protección contra Malware y Phishing integrada. Esta protección funciona mediante la comprobación de las listas de Phishing y Malware reportados. Estas listas se descargan automáticamente y se actualizan cada 30 minutos aproximadamente. Cuando Firefox detecta que estamos intentando ingresar a un sitio web que está listado como sitio malicioso o sospechoso, Firefox desplegará un mensaje de advertencia antes de que ingresemos.

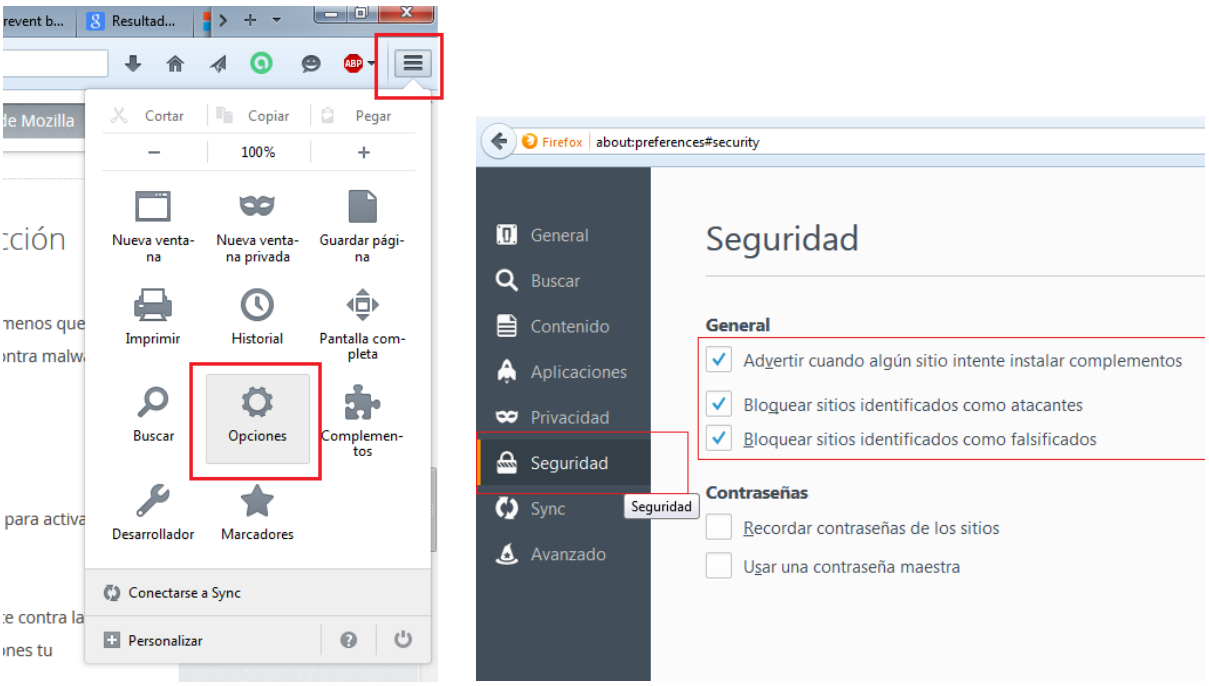
Cuando aparezca esta advertencia debemos tener un cuidado especial y evitar ingresar al sitio, ya que existe una alta probabilidad de que el mismo sea malicioso.

Si descargamos malware o programas espías, Firefox mostrará un mensaje en el Panel de descargas.



Estas protecciones se encuentran activadas por defecto en el navegador Mozilla, a menos que el usuario haya modificado esta configuración. La protección contra malware y phishing puede activarse desde el panel de Seguridad:

1. Hacemos clic en el botón Menú y elegimos “Opciones”.
2. Seleccionamos la pestaña “Seguridad”.
3. En la sección General, marcamos las opciones “Advertir cuando un sitio intente instalar complementos”, “Bloquear sitios identificados como atacantes” y “Bloquear sitios identificados como falsificados”.



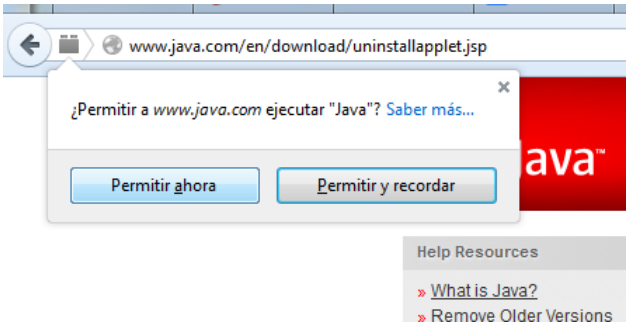
Para comprobar si la protección contra phishing está activa, se puede ingresar a la página de pruebas de phising: http://itisatrap.org/firefox/its-a-trap.html

Para confirmar que la protección contra malware está bloqueando los sitios web de ataque, se puede ingresar a la página de prueba de malware: http://itisatrap.org/firefox/its-an-attack.html

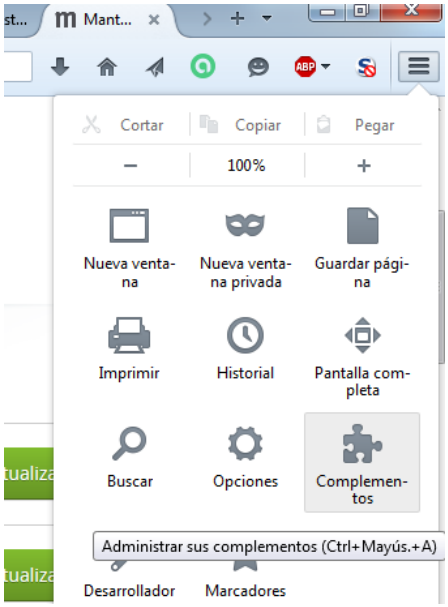
Obs.: Ambas son páginas de prueba que no dañarán a tu equipo. Si tienes activada la protección contra Phishing y Malware, no deberías poder cargar ninguna de esas páginas.

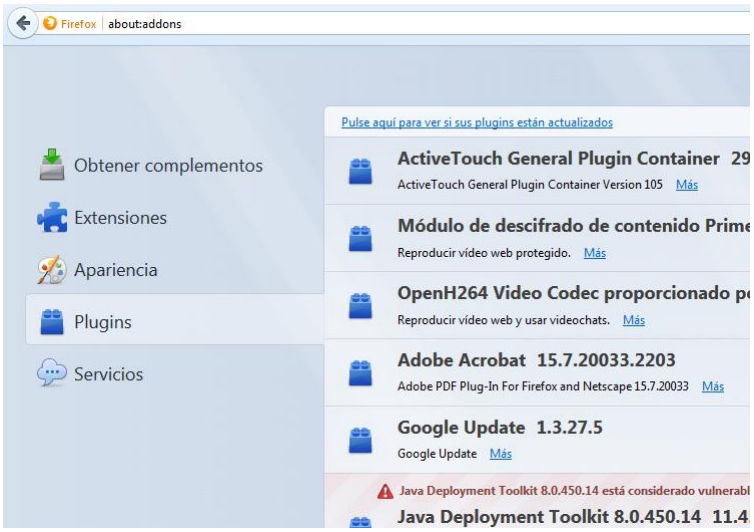
Muchas veces los atacantes se aprovechan de los plugins de los navegadores para atacarnos. Los *plugins* son herramientas que brindan funcionalidades adicionales al navegador, como por ejemplo Adobe Flash Player, que es el plugin que nos permite reproducir videos en muchos sitios.

Firefox puede evitar que el plugin se active automáticamente, evitando muchos problemas y nos permite decidir entre ejecutarlo automáticamente, ejecutarlo por una sola vez o actualizarlo. La mayoría de las veces no es recomendable habilitar plugins globalmente y/o sin autorización.



Para chequear los plugins instalados y sus configuraciones, podemos ingresar al Menú y luego a “Complementos”. Luego seleccionamos la pestaña “Plugins”, donde veremos la lista de nuestras plugins.





Para chequear las actualizaciones de nuestros plugins, podemos visitar https://www.mozilla.org/es-ES/plugincheck/

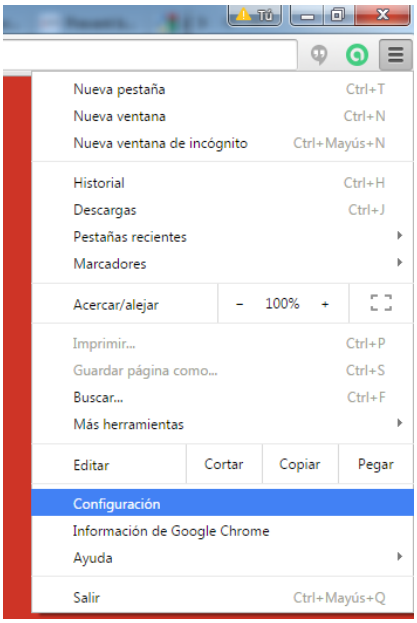
Google Chrome:

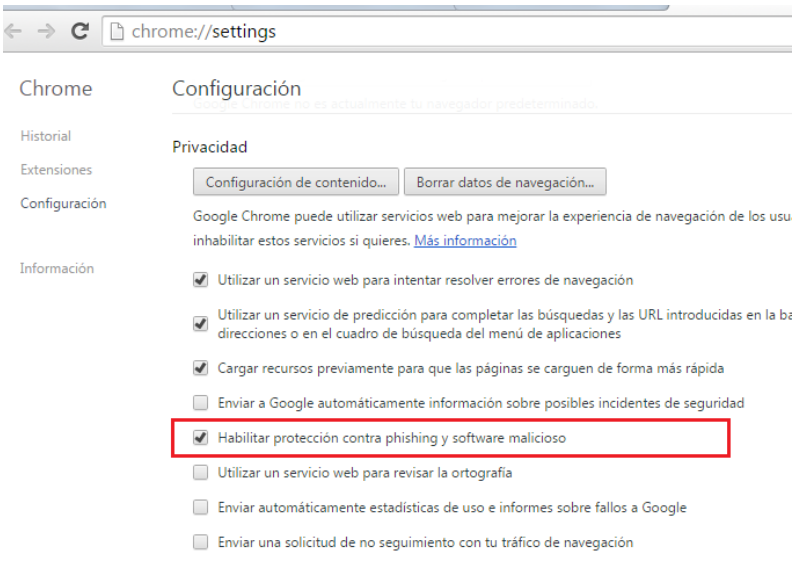
Chrome ofrece un sistema de protección contra phishing y otros sitios maliciosos muy similar a Firefox. La protección viene habilitada por defecto. Si queremos habilitarla:

1. En la esquina superior derecha entramos al menú y seleccionamos “Configuración”.

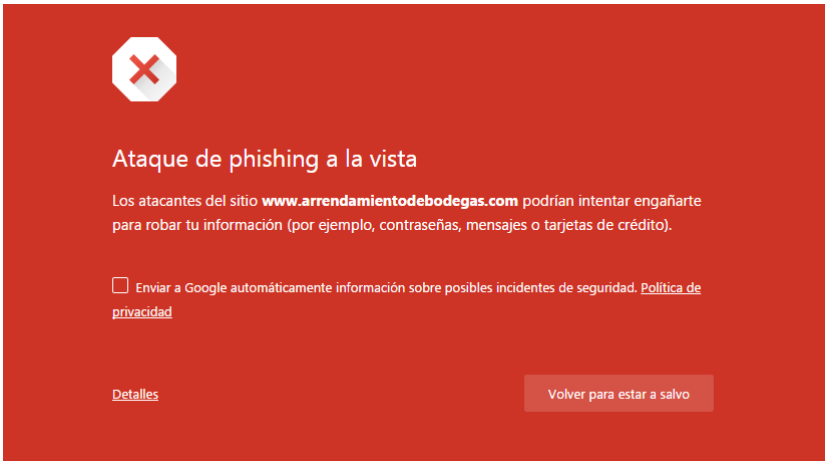
2. Vamos al final de la página y seleccionamos “Mostrar opciones avanzadas”

3. En la sección de “Privacidad”, tildamos la opción “Habilitar protección contra phishing y software malicioso”





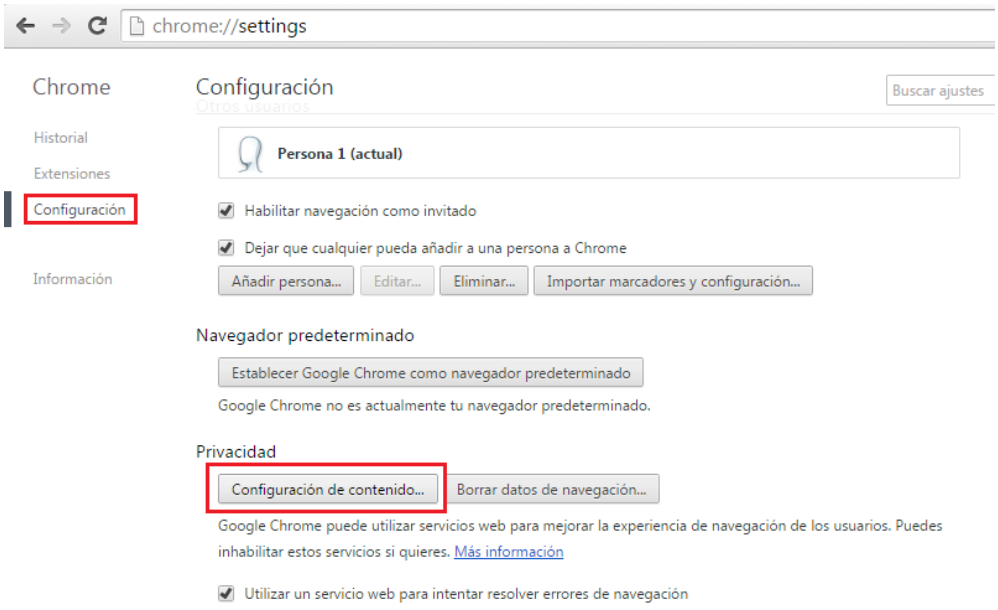
Cuando Chrome detecta que estamos intentando acceder a un sitio que está listado como malicioso o sospechoso, nos aparecerá una advertencia, evitando que ingresemos al sitio.



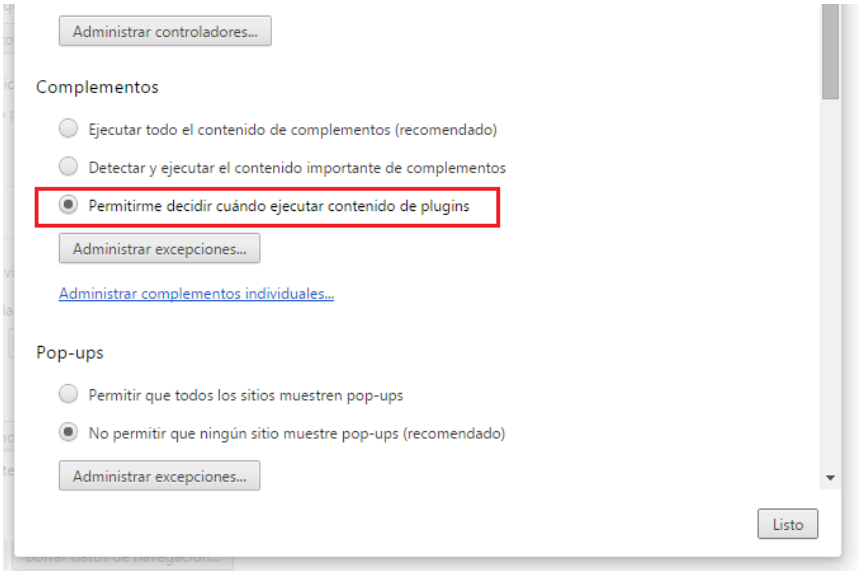
Para chequear los plugins instalados y sus configuraciones, escribimos chrome://plugins/ en la barra del navegador. Sin embargo Chrome solo permite activar o desactivar completamente un plugin y, al contrario

que Firefox, no permite activarlos selectivamente de forma individual. Sin embargo, permite configurar, de forma global, que todos los plugins y complementos sean ejecutados con el consentimiento del usuario.

1. Entramos a “Configuración” y en la sección “Privacidad”, seleccionamos “Configuración de contenido”; o escribimos chrome://settings/content/ en la barra del navegador.



2. En la sección “Complementos”, elegimos la opción “Permitirme decidir cuándo ejecutar contenido de plugins”

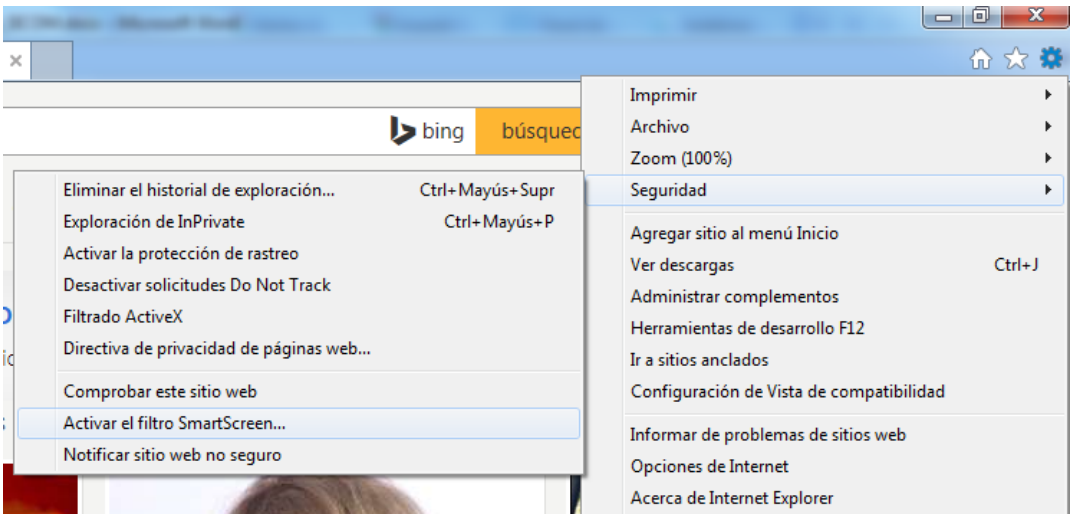


Internet Explorer:

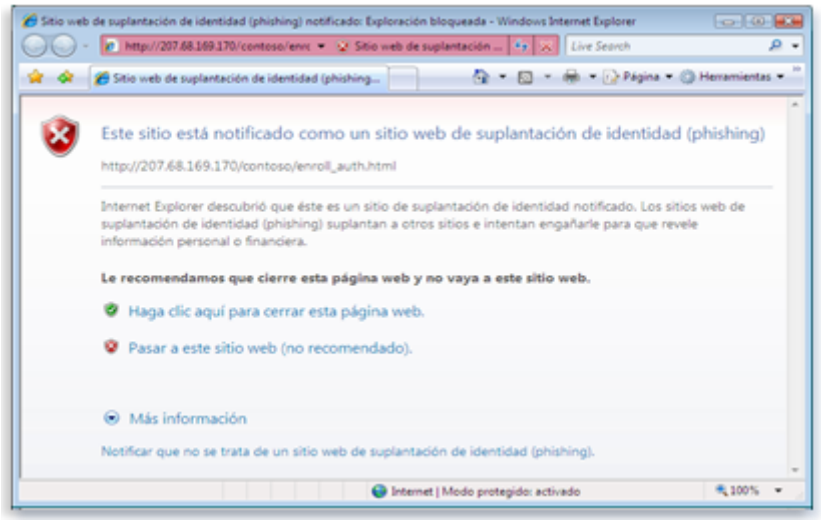
Microsoft ofrece también una protección contra sitios de phishing, llamada SmartScreen, la cual funciona de forma muy similar que los demás navegadores.

El filtro viene activado por defecto, sin embargo sin no lo tenemos activo:

1. En la esquina superior derecha, entramos al Menú
2. Seleccionamos “Seguridad”.
3. Seleccionamos “Activar el filtro SmartScreen”



Cuando Explorer detecta que estamos intentando ingresar a un sitio listado como malicioso o sospechoso, nos aparece una advertencia, impidiendo que ingresemos al sitio.



Safari:

Al igual que los demás, Safari ofrece una protección antifraude ante phishing.

1. Vamos a Ajustes > Safari
2. Tildamos “Aviso de sitio web fraudulento “

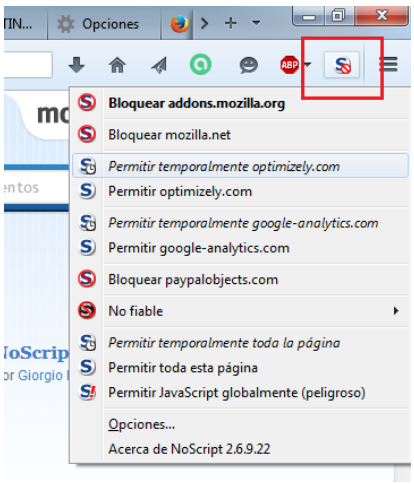
Complementos de Seguridad

- AdBlock-Plus:

  Este *add-on* ayuda a bloquear la publicidad molesta e intrusiva, tales como pop-ups, banners, etc., normalmente conocidos como *adware*. Estos normalmente son puntos de entrada para ataques. Hay que destacar que este complemento no bloquea la publicidad no-intrusiva. Está disponible para la mayoría de los navegadores y sistemas operativos, y puede ser instalado desde: https://adblockplus.org.

- No-Script:

  Javascript, Java, Flash y otros plugins son uno de los vectores de ataque preferido por los delincuentes. Si bien, muchos sitios requieren Javascript y plugins para funcionar correctamente, es recomendable deshabilitarlo por defecto y permitirlo sólo en las páginas en las que confiamos. NoScript sólo permite JavaScript, Java y otros plugins en los sitios web de confianza que nosotros elegimos voluntariamente. Este planteamiento preventivo basado en una lista blanca evita que se puedan explotar vulnerabilidades (conocidas o incluso desconocidas) sin pérdida de funcionalidad.



Para instalarlo, abre el siguiente enlace desde Firefox: https://addons.mozilla.org/es/firefox/addon/noscript/

- ScriptSafe

  Esta extensión, muy similar a No-Script para Firefox, impide que las páginas que visitamos ejecuten código en Javascript o complementos basados en Flash por defecto. Como muchos sitios no funcionarán correctamente, debemos agregarlos manualmente a la lista blanca. Para instalarlo, accedemos al siguiente enlace desde Google Chrome: https://chrome.google.com/webstore/detail/scriptsafe/oiigbmnaadbkfbmpbfijlflahbdbdgdf

- HTTPS Everywhere

  Siempre que sea posible se conectará a la versión HTTPS de una página web, para evitar que un atacante pueda interceptar datos sensibles tales como contraseñas, información bancaria, etc. Está disponible para Firefox, Chrome, Opera y Firefox para Android. https://www.eff.org/https-everywhere

- Ghostery

  Detecta software espía, de seguimiento, contadores y otros tipos de software invasivos al usuario, ofreciendo la posibilidad de bloquear los scripts que les permiten capturar y guardar nuestros datos. Está disponible para casi todos los navegadores y sistemas operativos, tanto de escritorio como móviles. https://www.ghostery.com/es/download

Seguridad en equipos

Los equipos informáticos, tales como computadoras, dispositivos móviles, etc. constan de dos componentes fundamentales:

- Sistema operativo: Windows, Linux, OS X, Android, etc.
- Programas o aplicaciones: Office, Java, los navegadores, etc.

Tanto el sistema operativo como los programas tienen fallas de seguridad o vulnerabilidades, las cuales son descubiertas frecuentemente y que deben ser corregidas.

Muchas veces los ataques cibernéticos se centran en encontrar estas fallas de seguridad en nuestros equipos para explotarlas e ingresar así a nuestros sistemas y acceder a nuestra información. Para esto, normalmente los atacantes diseñan programas maliciosos, denominados de forma genérica *malware*.

Los malware se clasifican en virus, troyanos, spyware y muchos otros tipos, de acuerdo a sus características. Por ejemplo, un tipo de malware que ha aumentado drásticamente en los últimos años es el ransomware, que "secuestra" nuestros archivos: los encripta y nos exige un pago para desencriptarlos.

El ransomware es especialmente dañino ya que, además del daño al equipo y al sistema, produce un daño a la información. Aún cuando fuera posible eliminar la infección de ransomware, en la mayoría de los casos, los archivos encriptados no pueden recuperarse. La única manera de asegurar la recuperación de los archivos, sin pagar al ciberdelincuente, es teniendo una copia de seguridad (*backup*) de los mismos. En la sección de Backup podrá encontrar recomendaciones y herramientas para ello.

Figura: Ejemplo de Ransomware TeslaCrypt

Más allá de las clasificaciones, la mayoría de los ataques relacionados a malware explotan una vulnerabilidad en el equipo para infectarlo.

Algunas buenas prácticas para mantener nuestros equipos seguros son las siguientes:

- No descargar programas de dudosa reputación. Siempre que vamos a descargar un programa, debemos asegurarnos de hacerlo desde la página oficial.

- Utilice siempre sistemas operativos y software original. Las versiones no originales (“piratas”) o modificadas (“crackeadas”) la mayoría de las veces no pueden acceder a las actualizaciones de seguridad, por lo que las fallas de seguridad descubiertas quedan expuestas y aumenta la probabilidad de quedar infectado con malware. Además, muchas veces el software ilegal contiene software malicioso que se instala sin que el usuario lo sepa.

- El correo de spam y phishing suele estar relacionado con la distribución de malware, por lo que es importante tomar las precauciones al entrar a los enlaces y/o abrir los adjuntos presentes en este tipo de mensajes.

- Mantener el sistema operativo y los programas actualizados. En la siguiente sección se profundizará en este aspecto.

- Deshabilitar las carpetas compartidas siempre que sea posible. Esto evita la propagación de gusanos que aprovechen ese vector como método de infección.

- Deshabilitar la ejecución automática de dispositivos USB. Los dispositivos de almacenamiento removibles que se conectan al puerto USB constituyen un vector de ataque muy empleado por el malware para la propagación, sobre todo, de gusanos.

- Contar con soluciones de antivirus, antimalware y/o firewall. En la sección “Antivirus, antimalware y firewall” se verá mayores detalles.

Actualización de Sistema Operativo y Software

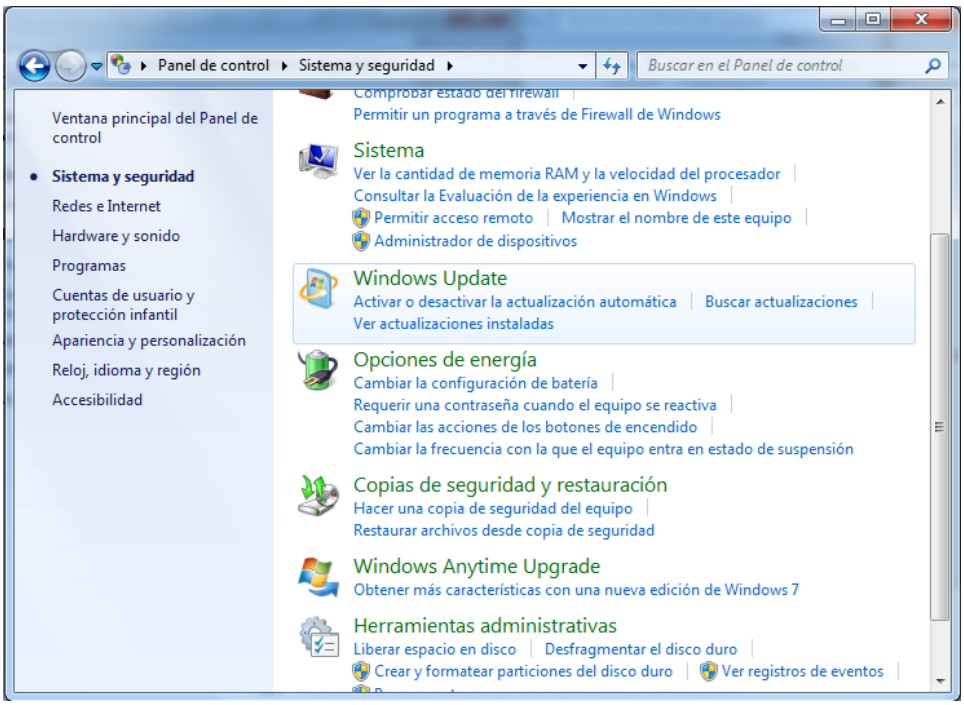
Cuando una vulnerabilidad es descubierta, el fabricante del producto afectado normalmente la corrige a través de lo que llamamos un parche o actualización. Es fundamental aplicar estas actualizaciones de modo a proteger nuestros sistemas y nuestra información.

Hoy en día, la mayoría de los sistemas operativos y programas ofrecen la posibilidad de chequear e instalar las actualizaciones de forma automática. Muchas veces esta opción viene activada por defecto, sin embargo es recomendable verificarlo. Estas actualizaciones automáticas nos facilitan enormemente el proceso de buscar las actualizaciones, descargarlas e instalarlas manualmente. Además, evita que descarguemos actualizaciones no oficiales que muchas veces son programas maliciosos.

A continuación veremos cómo activar las actualizaciones automáticas en algunos sistemas operativos y programas.

Windows

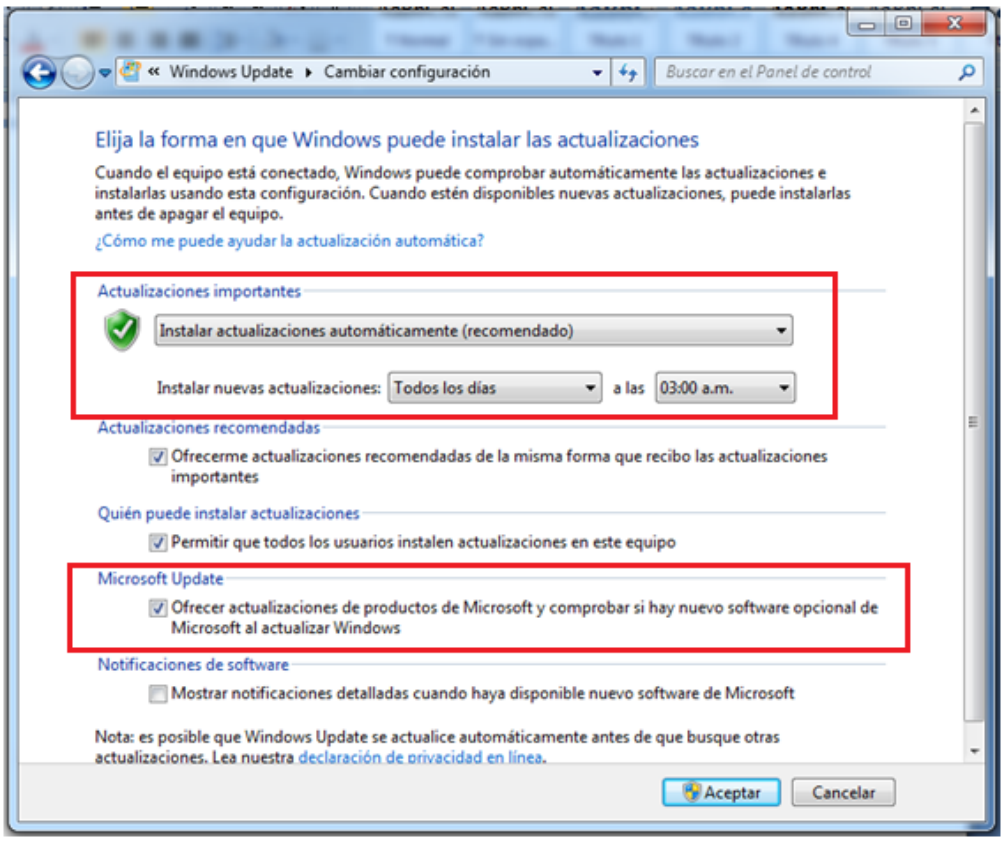
1. Ingresamos al Panel de Control, entramos a la sección “Sistema y Seguridad” y luego a “Windows Update”. En caso de que tengamos configurada la vista por íconos, desde el Panel de Control seleccionamos directamente “Windows Update”



2. Selecciona “Activar o desactivar la actualización automática”.

3. En la sección de Actualizaciones importantes, elige la opción “Instalar actualizaciones automáticamente (recomendado)”. Puedes elegir la frecuencia y la hora a la que quieres instalarlas.

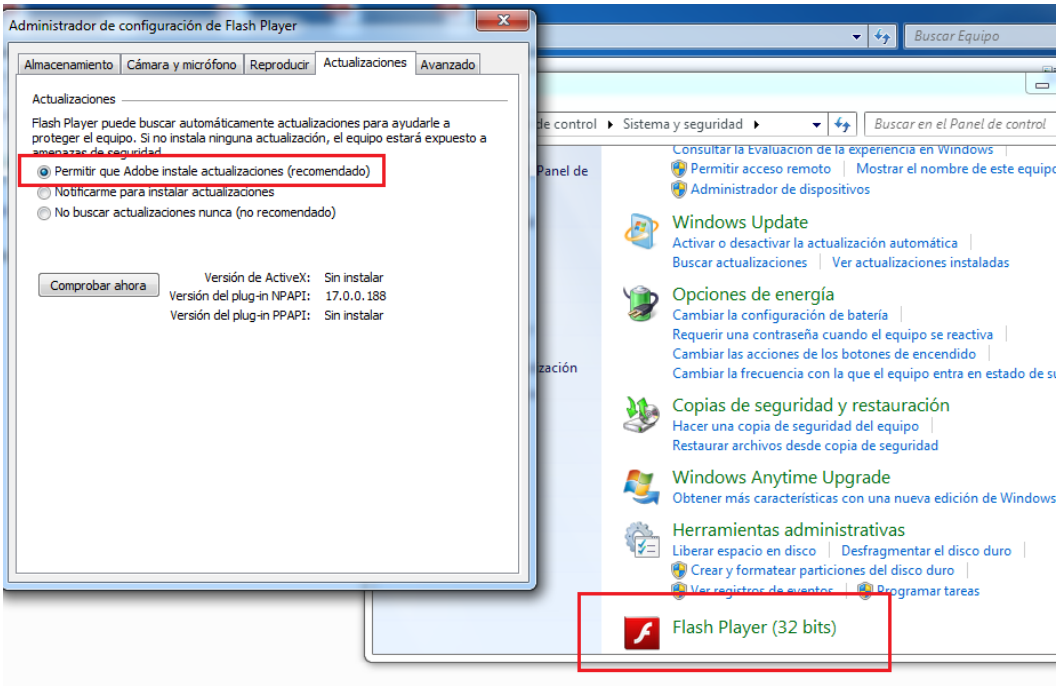
4. En la sección de Microsoft Update, tildar la opción “Ofrecer actualizaciones de productos Microsoft”.



5. Si queremos verificar si hay actualizaciones disponibles, desde “Panel de Control” > “Sistema y Seguridad” > “Windows Update” seleccionamos “Buscar actualizaciones”.

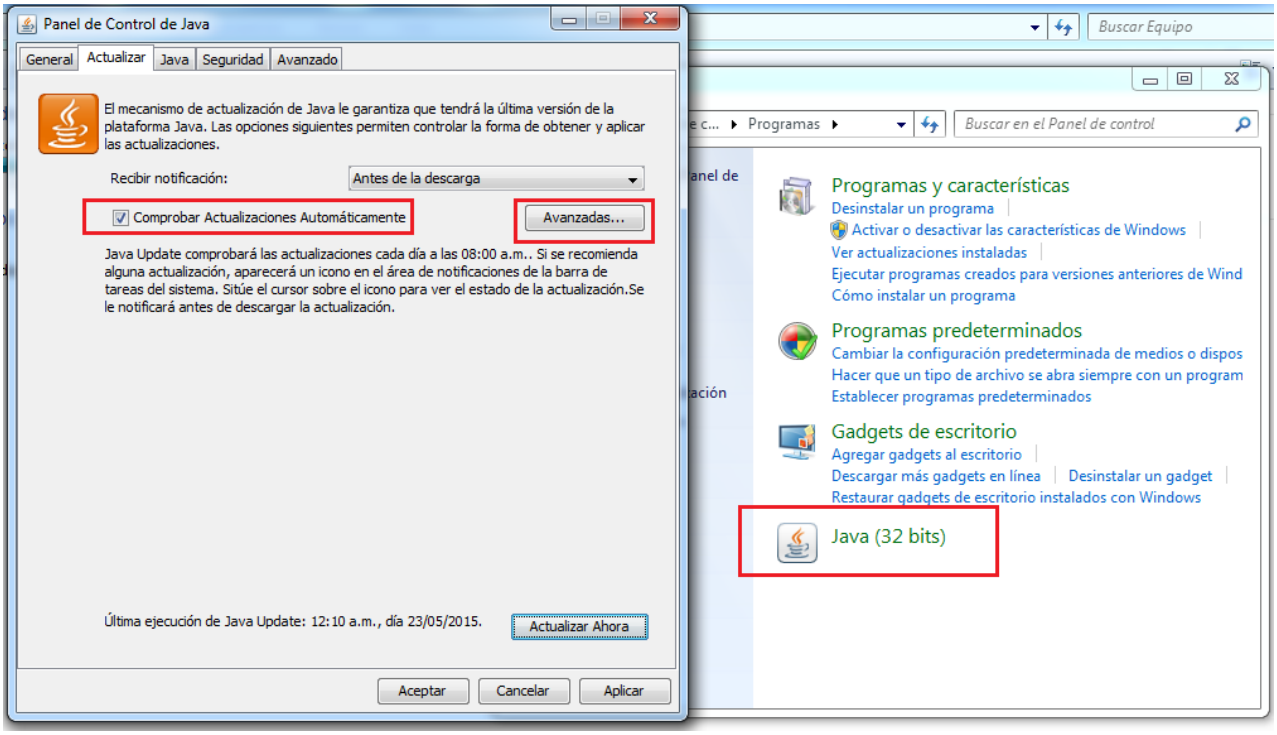
Flash

1. En “Panel de Control” > “Sistema y Seguridad” seleccionamos Flash.
2. Se abrirá una ventana, seleccionamos la pestaña Actualizaciones.
3. Seleccionamos la opción “Permitir que Adobe instale actualizaciones (recomendado). Debemos tener premisos de administrador para realizar esto.
4. Si queremos chequear las actualizaciones manualmente, seleccionamos “Comprobar ahora”



Java:

1. Ingresamos a “Panel de Control” > “Programas” y seleccionamos Java.
2. Tildamos la opción “Comprobar actualizaciones automáticamente”.
3. En “Avanzadas..” podemos configurar la frecuencia y la hora en la que queremos buscar e instalar las actualizaciones.


Panel de Control de Java
General
Actualizar
Java
Seguridad
Avanzado
El mecanismo de actualización de Java le garantiza que tendrá la última versión de la plataforma Java. Las opciones siguientes permiten controlar la forma de obtener y aplicar las actualizaciones.
Recibir notificación:
Antes de la descarga
Comprobar Actualizaciones Automáticamente
Avanzadas...
Java Update comprobará las actualizaciones cada día a las 08:00 a.m.. Si se recomienda alguna actualización, aparecerá un icono en el área de notificaciones de la barra de tareas del sistema. Sitúe el cursor sobre el icono para ver el estado de la actualización.Se le notificará antes de descargar la actualización.
Última ejecución de Java Update: 12:10 a.m., día 23/05/2015.
Actualizar Ahora
Aceptar
Cancelar
Aplicar
Buscar Equipo
Programas
Buscar en el Panel de control
Programas y características
Desinstalar un programa
Activar o desactivar las características de Windows
Ver actualizaciones instaladas
Ejecutar programas creados para versiones anteriores de Wind
Cómo instalar un programa
Programas predeterminados
Cambiar la configuración predeterminada de medios o dispos
Hacer que un tipo de archivo se abra siempre con un program
Establecer programas predeterminados
Gadgets de escritorio
Agregar gadgets al escritorio
Descargar más gadgets en línea
Desinstalar un gadget
Restaurar gadgets de escritorio instalados con Windows
Java (32 bits)

Mac OS X

- En OS X Lion y anterior, seleccionamos el menú Apple > “Preferencias del Sistema…” > “Actualización de Software”.
- En OS X Mountain Lion y posterior, seleccionamos el menú Apple > “Preferencias del Sistema…” > “App Store”.

- Tildamos la opción “Buscar actualizaciones automáticamente”, así como las 3 opciones siguientes: descargas nuevas actualizaciones, instalar actualizaciones de aplicaciones y actualizaciones de seguridad

- Para buscar manualmente las actualizaciones disponibles, seleccionamos “Mostrar actualizaciones”.

Actualización de apps compradas en Mac App Store

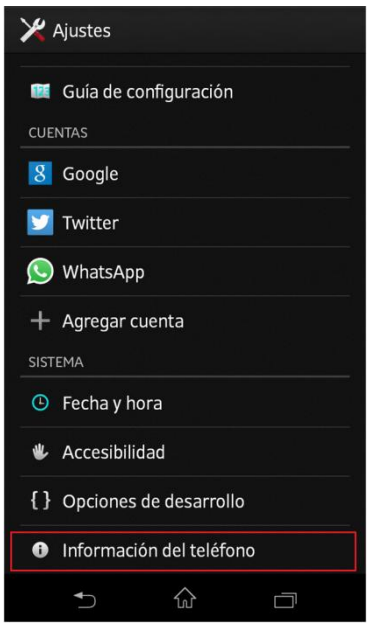
La opción de Actualización de Software no muestra las actualizaciones disponibles para las apps adquiridas en el Mac App Store.

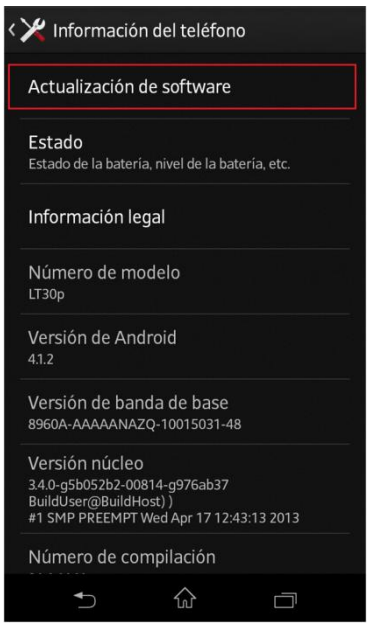
- Abrimos el App Store en tu Mac y seleccionamos la pestaña "Actualizaciones”. Veremos todas las actualizaciones disponibles para las apps instaladas actualmente en el equipo.
- Seleccionamos "Actualizar todo" para instalar todas las actualizaciones de software disponibles. Si es solicitado, introducimos un nombre de administrador y la contraseña y, a continuación, el ID de Apple y la contraseña.


Destacado
Top charts
Categorías
Comprado
Actualizaciones
2 actualizaciones disponibles
ACTUALIZAR TODO
Actualización de Software
Es necesario reiniciar
Hay actualizaciones disponibles para tu ordenador
ACTUALIZAR
Actualización de OS X 10.8.1
Se recomienda instalar la actualización 10.8.1 a todos los usuarios de OS X Mountain Lion, ya que mejora la estabilidad y la compatibilidad del ordenador y soluciona problemas generales del sistema... Más
Aperture
Apple
Versión 3.3.2
Publicado 25/07/2012
• Supports compatibility with OS X Mountain Lion
• Addresses issues that could affect performance when entering and exiting Full Screen mode
• Auto White Balance can now correct color using Skin Tone mode, even when Faces is disabled
• Projects and albums in the Library Inspector can now be sorted by date in addition to... Más
ACTUALIZAR
Copyright © 2012 iTunes S.à r.l. Todos los derechos reservados. Política de privacidad | Términos y condiciones | Preguntas frecuentes

Android

- Entramos a “Ajustes” o “Configuraciones de teléfono”. Normalmente encontramos el acceso directo en la barra de menú superior o en alguna de las pantallas de inicio.
- Seleccionamos la opción “Acerca del dispositivo” o “Información del teléfono”.
- Seleccionamos “Actualización de software” y luego “Actualizar”.





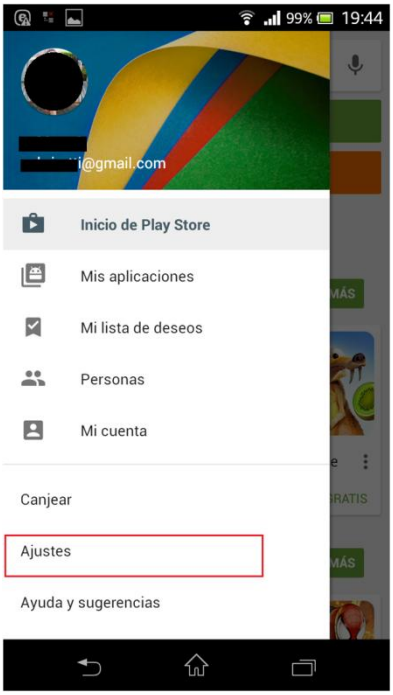
Obs.: La actualización del sistema operativo Android puede variar dependiendo de la versión y del modelo del teléfono móvil. Además, la disponibilidad de las actualizaciones dependerá de varios factores (modelo, versión, fabricante, zona, operadora telefónica, etc.)

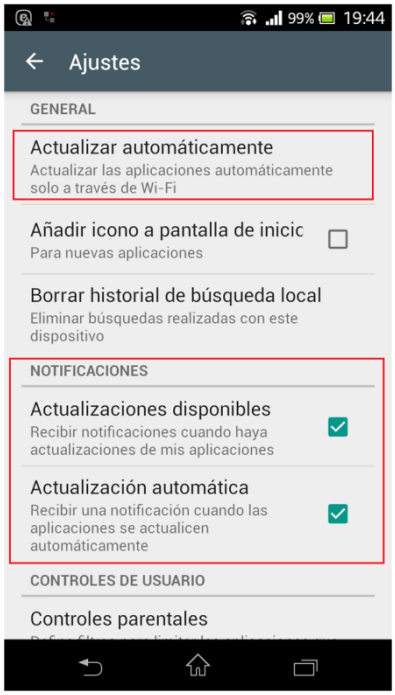
Aplicaciones de Google Play Store

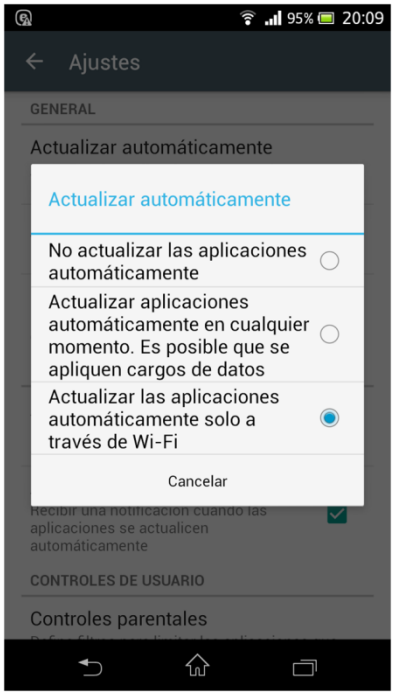
- Abrimos el Google Play Store desde el acceso directo y seleccionamos en la esquina superior izquierda.
- Seleccionamos “Ajustes”
- Seleccionamos la opción “Actualizar automáticamente”. Tendremos tres opciones:
  - No actualizar automáticamente
  - Actualizar automáticamente en cualquier momento
  - Actualizar automáticamente solo a través de Wi-Fi

En general, se recomienda elegir la opción “Actualizar automáticamente solo a través de Wi-Fi”, debido a que las actualizaciones pueden consumir gran parte del plan de datos. Sin embargo, en caso de contar con un plan de datos suficiente, se puede elegir actualizarlas automáticamente en cualquier momento.

- Si deseamos recibir notificaciones de las actualizaciones disponibles y cuando una aplicación se haya actualizado, en la sección de Notificaciones tildamos las opciones “Actualizaciones Disponibles” y “Actualización automática”.


99% 19:44
[redacted]i@gmail.com
Inicio de Play Store
Mis aplicaciones
Mi lista de deseos
Personas
Mi cuenta
Canjear
Ajustes
Ayuda y sugerencias


99% 19:44
Ajustes
GENERAL
Actualizar automáticamente
Actualizar las aplicaciones automáticamente solo a través de Wi-Fi
Añadir icono a pantalla de inicic
Para nuevas aplicaciones
Borrar historial de búsqueda local
Eliminar búsquedas realizadas con este dispositivo
NOTIFICACIONES
Actualizaciones disponibles
Recibir notificaciones cuando haya actualizaciones de mis aplicaciones
Actualización automática
Recibir una notificación cuando las aplicaciones se actualicen automáticamente
CONTROLES DE USUARIO
Controles parentales


95% 20:09
Ajustes
GENERAL
Actualizar automáticamente
Actualizar automáticamente
No actualizar las aplicaciones automáticamente
Actualizar aplicaciones automáticamente en cualquier momento. Es posible que se apliquen cargos de datos
Actualizar las aplicaciones automáticamente solo a través de Wi-Fi
Cancelar
CONTROLES DE USUARIO
Controles parentales

Antivirus, Antimalware y Firewall

Actualmente, la mayoría de los antivirus se convirtieron en suites de seguridad, que integran varias funciones, además de la detección de virus: firewall, anti-malware, sistema de detección de incidente basado en host, backup, antirrobo, entre muchas otras. Aún así, frecuentemente se le sigue denominando "antivirus" simplemente.

Los *firewalls* o cortafuegos, programas antivirus y programas antimalware trabajan en conjunto y deben utilizarse para proveer el máximo nivel de seguridad para proteger su computadora. Anteriormente la mayoría de las soluciones antivirus se limitaban a analizar los archivos de nuestro disco cuando ejecutábamos un análisis para detectar una infección. Sin embargo, hoy en día, la industria de seguridad evolucionó enormemente, y no se limita a esto, sino que busca protegernos de forma proactiva de manera a prevenir los diversos tipos de ataques.

Los programas maliciosos existen en todos los sistemas operativos, incluido Linux y Mac OSX, contrariamente a lo que a veces se cree. Es por eso que también se deben adoptar no solo buenas prácticas sino también herramientas de seguridad como firewalls y anti-malware en estos sistemas operativos.

La mayoría del software de seguridad pre instalado en computadora solamente funciona por un pequeño período de tiempo de prueba; para acceder a todas las funcionalidades de un antivirus normalmente se debe pagar una suscripción. El software de seguridad solamente nos protege contra amenazas nuevas si está actualizado, lo cual suele ser una característica reservada a las versiones de pago, por lo cual siempre se recomienda invertir en este tipo de soluciones. La mayoría de las veces las pérdidas generadas por un ataque es mucho mayor que el costo de estas soluciones.

Aunque la mayoría de los programas antivirus también tienen la capacidad de combatir malware, debido a la creciente sofisticación de los programas de malware, lo mejor es utilizar un programas anti malware además de un programa antivirus. Cada uno se especializa en detectar amenazas ligeramente distintas, por lo tanto su uso colectivo podría ofrecerle mayor seguridad. La compatibilidad entre ambos dependerá del producto elegido y normalmente es especificada en las páginas web de los fabricantes.

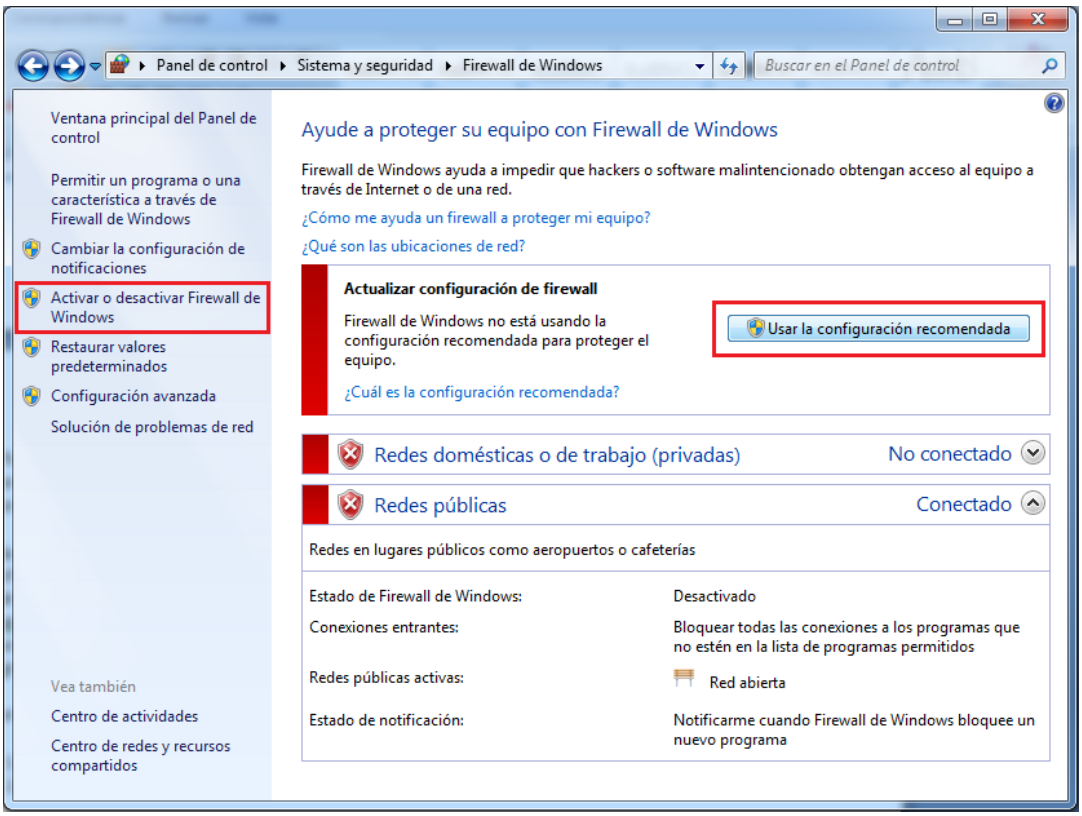
Firewall

Un firewall ayuda a prevenir que la información entre o salga de nuestra computadora sin nuestra autorización, controlando lo que es visible desde Internet y bloqueando las comunicaciones de fuentes no autorizadas.

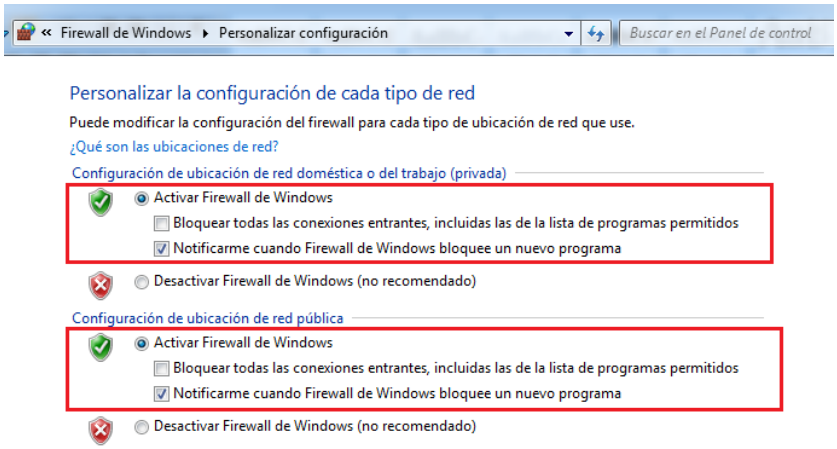
Cada computadora que está conectada al Internet debe tener un firewall activado en todo momento. Muchos sistemas operativos ya vienen con firewalls integrados, como en el caso de Windows, los cuales están activados de forma predeterminada. Sin embargo, existen soluciones más avanzadas, ya sea integradas a soluciones antivirus o soluciones independientes. En caso de que optemos por estas soluciones, se debe desactivar el firewall del sistema operativo, delegando esta función a la solución que elegimos.

A continuación veremos cómo activar el firewall en Windows:

1. Ingresamos al Panel de control > "Sistemas y Seguridad" > "Firewall de Windows".
2. Si el firewall está desactivado, veremos como advertencia unos cuadros de texto rojos y un escudo rojo con una cruz. Para activarlo hacemos click en "Usar la configuración recomendada" o "Activar o desactivar Firewall de Windows".



3. En caso de haber seleccionado “Activar o desactivar Firewall..” aparecerá una nueva ventana donde seleccionamos “Activar Firewall de Windows” tanto para redes privadas como públicas.

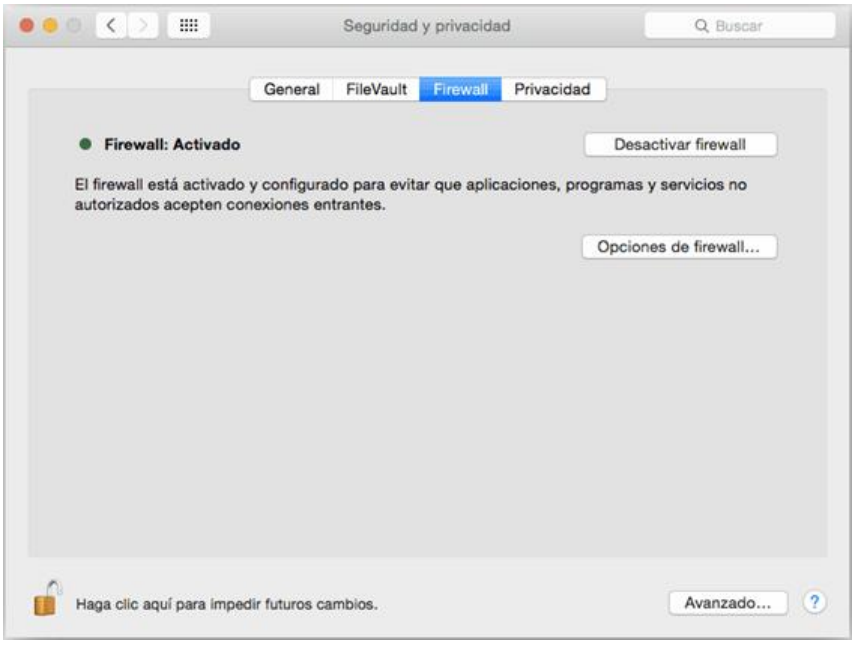


Obs.: Usando la configuración recomendada evitaremos una superposición de funciones de firewall en caso de que contemos con otro programa tal como un antivirus que cuente con un firewall integrado.

Para activarlo en Mac OS X:

1. Ingresamos a “Preferencias del Sistema” en el menú Apple.
2. Seleccionamos “Seguridad” o “Seguridad y privacidad”.
3. Seleccionamos la pestaña “Firewall”.
4. Desbloqueamos el panel haciendo clic en el candado de la esquina inferior izquierda e introduciendo el nombre de usuario y la contraseña del administrador.

5. Hacemos clic en "Activar firewall”.



Antivirus

Los programas antivirus de software ayudan a proteger nuestros equipos de virus que pueden destruir datos, robar información y datos personales y/o hacer que el equipo no funcione correctamente y sea más lento. El software antivirus escanea su computadora para detectar patrones que pueden indicar que el aparato ha sido infectado. Estos patrones se basan en firmas, definiciones o virus que ya son conocidos. Los autores de los virus continuamente están actualizando o desarrollando nuevos virus. Por lo tanto, es importante contar siempre con el antivirus actualizado, de modo a contar con las últimas definiciones o firmas. Esto muchas veces sólo está disponible en las versiones de pago.

Existen muchas compañías que producen software antivirus. Algunos de los más conocidos son:

- ESET Smart Security - http://www.eset-la.com/hogar
- Norton Security - http://es.norton.com/norton-security-antivirus
- Avast - https://www.avast.com/es-ww/index#compare-home
- Kaspersky Antivirus - http://latam.kaspersky.com/productos/productos-para-el-hogar/anti-virus
- Microsoft Security Essentials - http://windows.microsoft.com/en-us/windows/security-essentials-download

Si bien, la mayoría de los antivirus están disponibles para sistemas operativos Windows, cada día existen más antivirus para otros sistemas operativos como Mac OS X y Android. Se debe tener en cuenta que las amenazas de seguridad existen, en mayor o menor medida, en todos los sistemas operativos, por lo que es recomendable contar con soluciones antivirus en todos los sistemas operativos.

Anti malware

La palabra malware abarca una amplia categoría de amenazas incluyendo spyware (software espía), adware (software publicitario), caballos de Troya y otros programas no deseados que podrían ser instalados en nuestra computadora sin nuestro conocimiento o consentimiento.

Si bien estos programas maliciosos no se definen como “virus”, pueden ser igual o más dañinos. El spyware, por ejemplo, puede recopilar nuestra información a través de Internet sin que lo notemos, interceptando prácticamente cualquier dato: actividad en Internet, correos electrónicos, contactos y lo que escribimos.

Los programas anti malware y anti spyware ayudan a eliminar muchas de estas amenazas. Los siguientes son ejemplos de sitios que ofrecen programas gratuitos de anti malware:

- Malwarebytes - http://es.malwarebytes.org
- Super Anti-Spyware - www.superantispyware.com
- Spybot Search and Destroy - www.safer-networking.org/en/index.html

Obs.: Al igual que los antivirus y las suites de seguridad, estos programas cuentan con funcionalidades básicas en sus versiones gratuitas o de prueba. Para acceder a una protección más completa y proactiva, se recomienda utilizar las versiones de pago.

Protección de datos

La información almacenada en equipos muchas veces puede caer en manos equivocadas debido a diversas situaciones, como por ejemplo, ante el extravío o robo de los equipos portátiles o ante una intrusión al mismo.

Es por esto que es fundamental tomar medidas para proteger estos datos de modo a que no sea fácilmente accesible por extraños, así como también tomar medidas preventivas para no perderlos, por ejemplo en caso de daño del equipo, pérdidas o robo.

Contraseña de inicio de sesión

En casi todos los sistemas operativos, incluso en dispositivos móviles, es posible establecer una contraseña para el inicio de sesión. Esta es una primera medida de seguridad que ayuda a prevenir que personas no autorizadas accedan a la información del equipo o realicen acciones como instalar software no autorizado, modificar archivos de sistema, etc.

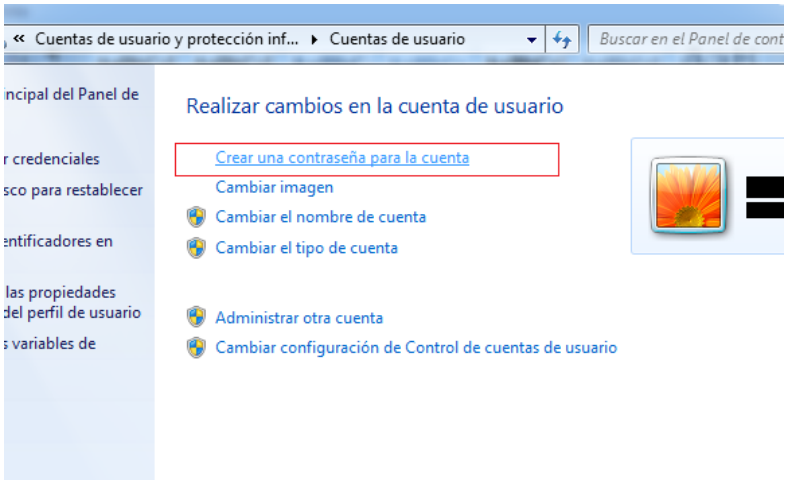
En los sistemas operativos de PCs la contraseña de inicio de sesión normalmente se establece cuando se instala por primera vez, sin embargo, si fue dejada en blanco, puede configurarse posteriormente. En los dispositivos móviles, la contraseña de inicio de sesión la mayoría de las veces debe establecerse manualmente, ya que durante la configuración inicial generalmente no es exigida.

A continuación veremos cómo establecer o cambiar una contraseña de inicio de sesión en los sistemas operativos más utilizados.

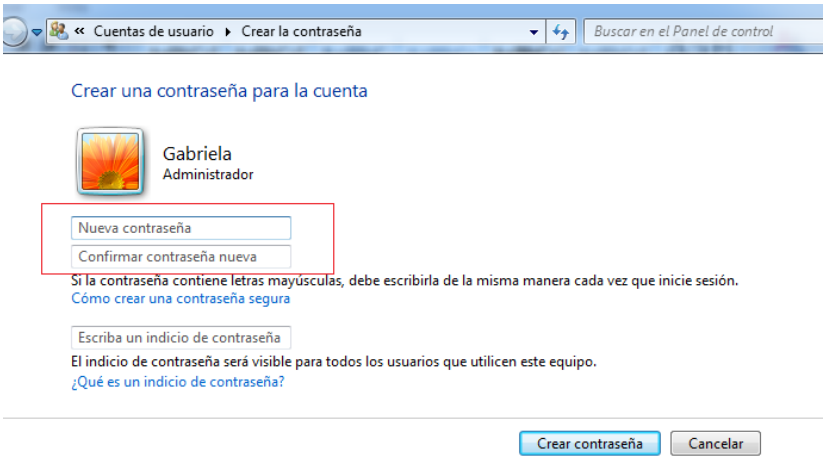
Windows:

1. Ingresamos a Panel de Control > “Cuentas de usuario”

2. Seleccionamos “Crear contraseña para la cuenta”.



3. Ingresamos una contraseña y la confirmamos. De forma opcional se puede escribir un incidió de contraseña, sin embargo, como este indicio será visible para todos, se recomienda tener cuidado con dar muchos detalles en este campo. Si fuera posible, evitar poner un indicio.



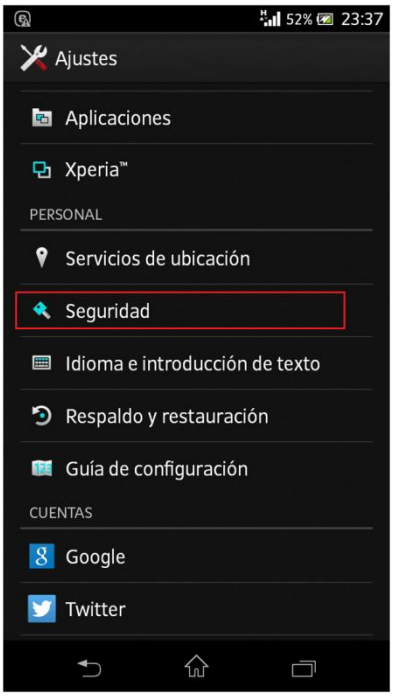
Android:

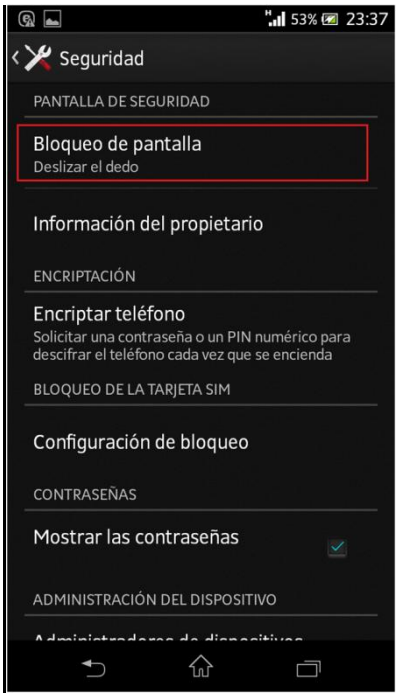
1. Entramos a “Ajustes” o “Configuración de teléfono”.

2. Seleccionamos “Seguridad” y luego “Bloqueo de pantalla”.

3. Elegimos uno de los métodos de bloqueo: patrón, PIN, contraseña u otro tipo de control que ofrece el teléfono. Seguimos las instrucciones de acuerdo a la opción elegida.

   Obs.: las opciones pueden variar de acuerdo al fabricante, modelo y versión del sistema operativo del teléfono.





Encriptación de datos

La contraseña de inicio de sesión si bien es una medida de protección básica, en la mayoría de los casos no es suficiente para proteger los datos, es por eso que es fundamental implementar soluciones de cifrado de los datos importantes.

Cifrar los datos implica que cada vez que se quiera acceder a los mismos, se deban descifrar, lo que agrega un nivel de complejidad al acceso simple.

La clave es una parte esencial del mecanismo de cifrado de datos, ya que representa la única posibilidad de descifrar la información y, por tanto, leerla. Por ello, resulta fundamental escoger una clave robusta, ya que significará que la barrera entre los datos y los intrusos será más difícil de cruzar.

Por lo general, se deben establecer criterios para determinar qué datos se van a cifrar y cuáles no, de acuerdo al valor que tienen para el negocio.

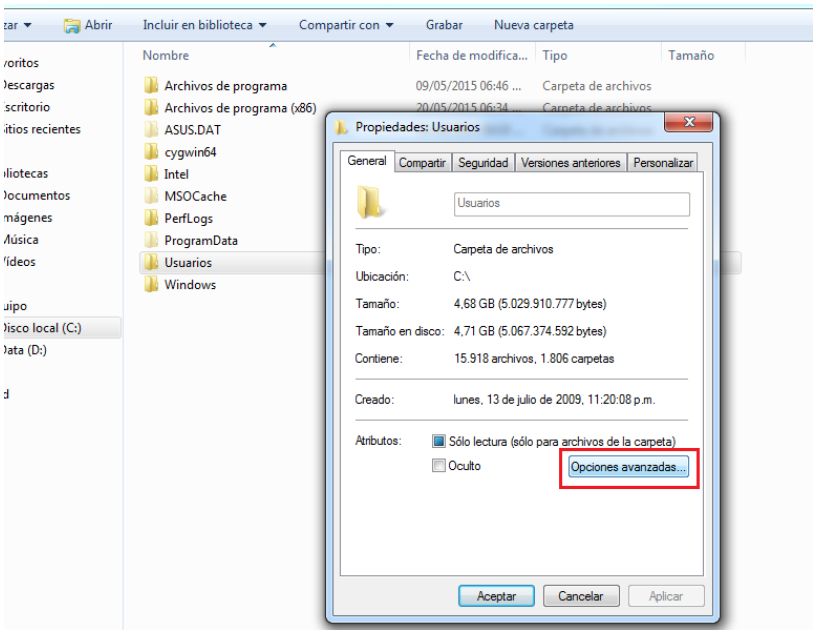
Puede cifrarse el disco entero, de tal manera que cada vez que se encienda la computadora se deba ingresar la clave para tener acceso a la misma. También existe la alternativa de cifrar sólo algunas carpetas o archivos específicos. Esto incluso se puede extender a cualquier dispositivo que transporte información delicada, como memorias USB.

La mayoría de los sistemas operativos ofrecen herramientas de cifrado nativas, pero también existen aplicaciones de terceros que pueden ser instaladas en caso de requerir soluciones más avanzadas.

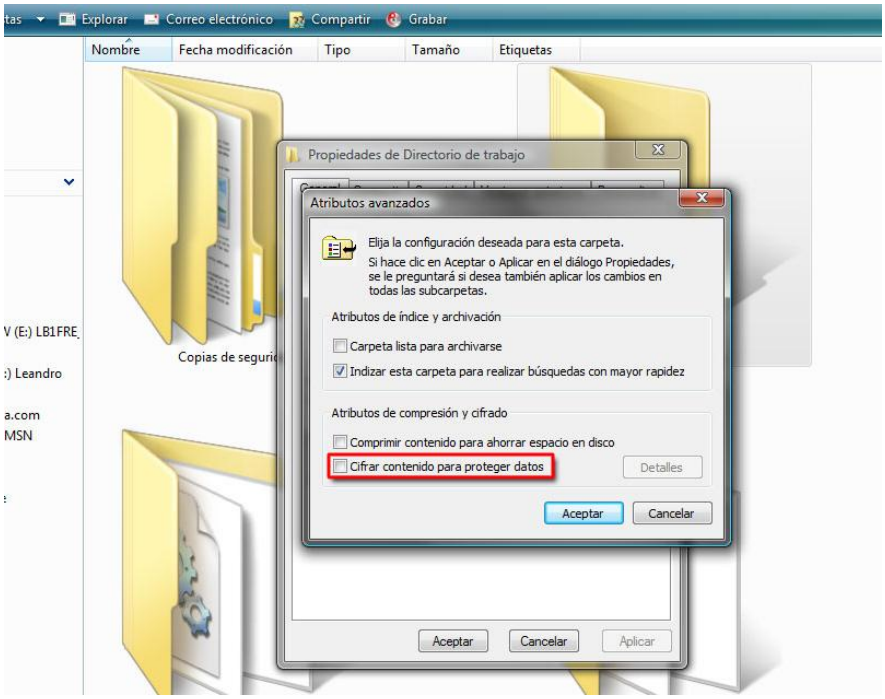
Windows:

EFS (Encryptad File System) es un servicio de cifrado de carpetas incorporado en la mayoría de las versiones de Windows desde XP en adelante. Después de cifrar carpetas mediante EFS, otros usuarios del sistema no podrán abrirla, sólo se podrá acceder mediante el inicio de sesión de Windows que los cifró.

1. Hacemos clic derecho en la carpeta que deseamos encriptar y luego seleccionamos “Propiedades”.
2. En la pestaña General seleccionamos "Opciones avanzadas..".



3. Tildamos la casilla "Cifrar contenido para proteger datos”.



4. Windows preguntará si desea cifrar una sola carpeta o todas las subcarpetas y archivos de la carpeta. Seleccionamos "Aplicar cambios a este directorio, subdirectorios y archivos”.
5. Al finalizar, todas las carpetas que se han cifradas tendrán el nombre en verde, indicando que todas ellas están encriptadas.

Obs.: EFS no es compatible con todas las versiones de Windows, por lo que puede no funcionar en algunas. Es soportado por Windows 2000 Pro; XP Pro; Vista Business, Enterprise y Ultimate, 7 Pro, Enterprise y Ultimate; 8 y 8.1 Pro y Enterprise.

Bitlocker:

Además de la herramienta de cifrado de archivos EFS, Microsoft ofrece una solución de encriptación de disco denominada Bitlocker, disponible de forma nativa en algunas versiones (Vista o 7 Ultimate y Enterprise, 8.1 Pro o Enterprise).

Se trata de una solución de encriptación de disco que puede ser activada desde el Panel de Control. Seleccionamos “Configurar Bitlocker” > “Activar”. Bitlocker realizará una verificación, en caso necesario apagará el equipo y tendremos que encenderlo de forma manual. A continuación, se deberán seguir las instrucciones que aparecerán para la encriptación con Bitlocker.

Mac OS X

FileVault es una herramienta que viene por defecto dentro del sistema operativo. FileVault, sin embargo, sirve para cifrar todo el disco, no solamente algunas carpetas seleccionadas. Al encriptar un disco, se crea una clave de recuperación como medida de protección. Si olvidamos la contraseña de inicio de sesión, se puede usar la clave de recuperación para desbloquear los contenidos codificados de un disco.

1. Ingresamos a “Preferencias del Sistema” > “Seguridad”, y luego, la pestaña FileVault. Una vez dentro de esa pestaña, pulsamos en el candado de la esquina inferior izquierda para poder desbloquear la herramienta mediante la contraseña de administrador.
2. Seleccionamos “Activar FileVault…”

3. Aparecerá una pantalla con una clave de recuperación que servirá como medida de seguridad en caso de que olvidemos la contraseña que luego elegiremos.
4. En la siguiente ventana se debe elegir si queremos que Apple guarde o no esa clave de recuperación. De esta forma en caso de que se olvidemos la contraseña y esta clave de recuperación, llamando al servicio técnico de Apple ellos podrían entrar en el sistema y recuperarla. Si le indicamos que queremos que se guarde la clave de recuperación en Apple, se nos solicita tres preguntas de seguridad.

5. Al finalizar, nos indicará que debemos reiniciar el equipo para comenzar con la encriptación del disco.

Aplicaciones de terceros:

En general, las herramientas nativas tanto de Windows como de Mac OS X son bastante básicas, por lo que ante intrusiones más sofisticadas, las mismas no serán una protección eficaz. A continuación presentamos una serie de programas de encriptación de archivo y de disco para los diversos sistemas operativos, sencillas de usar, algunas son gratuitas, otras son de pago:

Windows:

- AxCrypt - http://www.axantum.com/AxCrypt/Default.html
- Challenger - http://www.encryption-software.de/challenger/en/index.html
- Conceal - http://www.dataconceal.com

Mac OS X:

- Scrambler - https://codingturtle.com/scrambler
- Espionage - http://www.espionageapp.com
- DocWallet - https://itunes.apple.com/en/app/pages/id645501839

Linux:

- Nautilus Encryption Utility
- Seahorse (GnuPG)

Multiplataforma (Windows, Linux, Mac):

- VeraCrypt - https://veracrypt.codeplex.com/
- AES Crypt - http://www.aescrypt.com/windows_aes_crypt.html
- 7zip - http://7-zip.org/download.html
- KeyParc - http://www.keyparc.com/web/en

Backup

Además de proteger nuestros datos de personas no autorizadas, tenemos que tener en cuenta mecanismos que nos permitan recuperar la información en caso de perder un equipo, ya sea por robo, daño u otros. Las copias de seguridad o *backup* de la información importante deben ser realizadas periódicamente.

Existen herramientas y soluciones de backup, tanto offline, que se almacenan en un medio físico, así como soluciones en la nube.

Para minimizar las posibilidades de pérdida de datos importantes, se recomienda adoptar buenas prácticas mínimas:

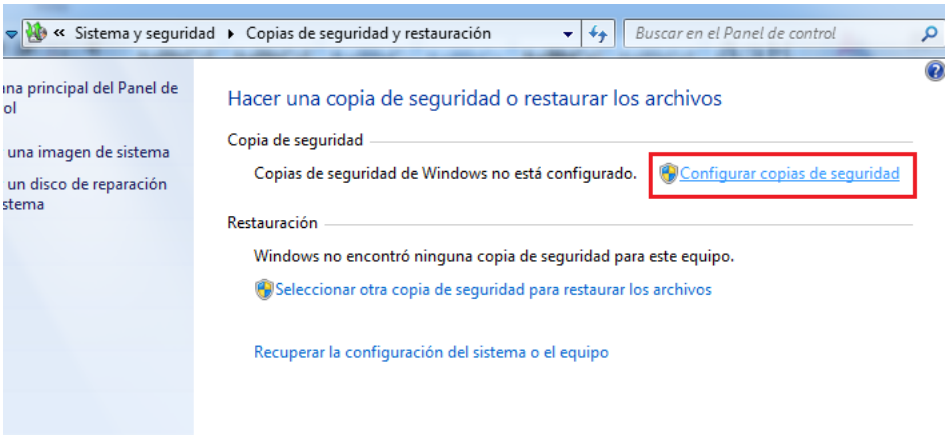
- En caso de realizar un backup almacenado en un medio físico, es recomendable contar con copias almacenadas en un dispositivo diferente al original tal como un disco duro externo u otro ordenador, en lo posible en más de un medio. De lo contrario, en caso de daño o robo del equipo original, muchas veces también perderemos la copia de seguridad.
- Las copias de seguridad deben realizarse de manera periódica, de manera a poder recuperar una versión lo más actualizada posible.
- Es necesario comprobar regularmente que las copias de seguridad funcionen, de modo a asegurar que en caso de pérdida ésta pueda ser restaurada.

Al igual que las herramientas de encriptación, muchos sistemas operativos cuentan con herramientas básicas de backup integradas de forma nativa. Sin embargo, para soluciones más avanzadas y efectivas, muchas veces son necesarias herramientas y aplicaciones de terceros.

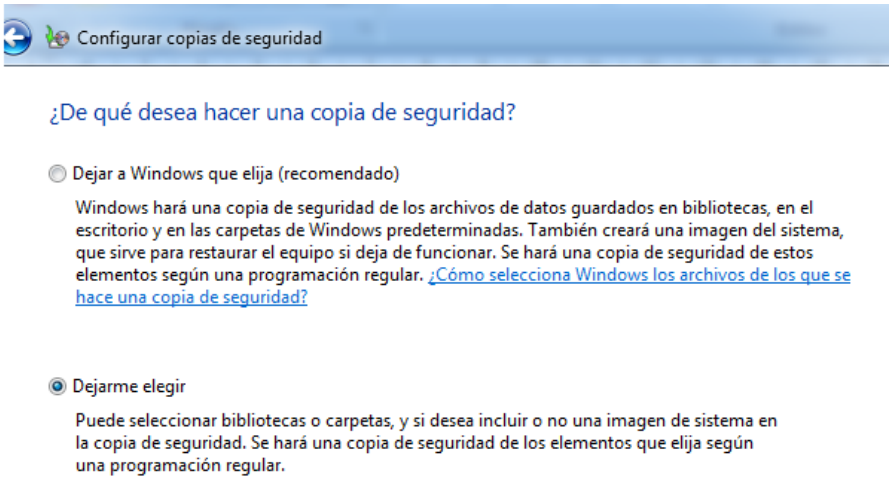
A continuación presentaremos algunas soluciones de backup más conocidas:

Windows

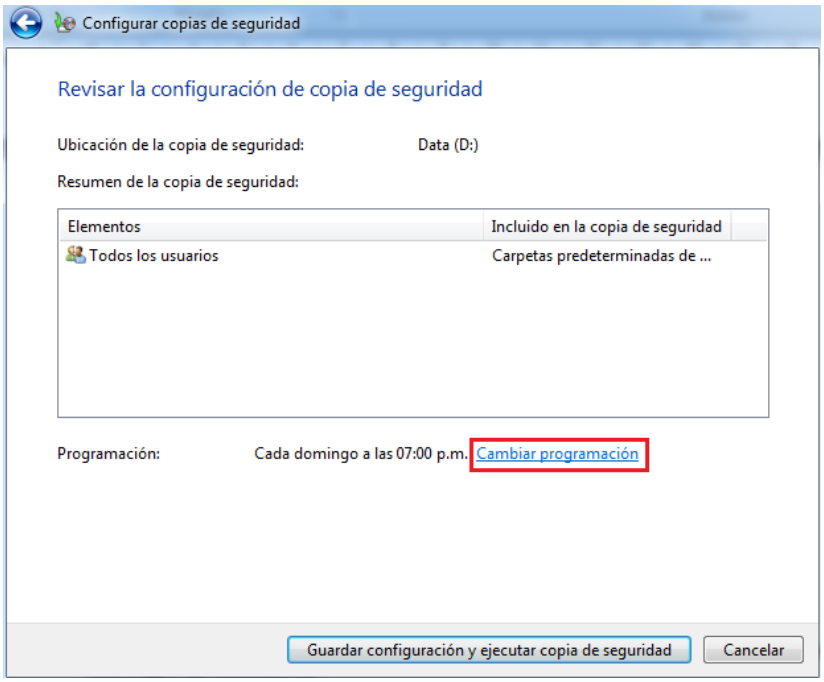
1. Entramos a Panel de Control > “Sistema y Seguridad” > “Copias de Seguridad y Restauración”
2. Seleccionamos “Configurar copias de seguridad”



3. A continuación debemos elegir el destino donde se va a almacenar la copia de seguridad. Podemos elegir una partición del disco del equipo o un medio externo (CD, disco duro externo, etc.)
4. Debemos seleccionar si deseamos que Windows elija los archivos de los cuales realizará un backup o si deseamos elegirlos nosotros mismos.



5. Seleccionamos las carpetas que deseamos que se copien. Además, elegimos si deseamos copiar una imagen del sistema o no.
6. A continuación veremos los detalles de la configuración que hemos realizado. Podemos programar la frecuencia y el horario en que se realizará la copia, seleccionando “Programar”.



7. Al finalizar, seleccionamos “Guardar configuración y ejecutar copia de seguridad”, con lo que se iniciará el proceso de backup.

En caso de que necesitemos restaurar una carpeta o archivo desde una copia de seguridad almacenada localmente:

8. Vamos a la carpeta, hacemos click derecho sobre ella y seleccionamos Propiedades.
9. En la pestaña “Versiones anteriores” veremos un listado de todas las versiones de copias de seguridad que tengamos almacenadas de esa carpeta.

En caso de que necesitemos restaurar toda una copia de seguridad o una imagen del sistema:

10. Abrimos Panel de Control > “Sistema y Seguridad” > “Copias de Seguridad y Restauración”
11. En la sección “Restauración” podremos visualizar las copias de seguridad almacenadas localmente o podremos importarlas de un medio externo, entrando a “Seleccionar otra copia de seguridad para restaurar los archivos”.

Servicios en la nube

- Google Drive: espacio gratuito de 15 GB, aplicaciones disponibles para Chrome, Windows, iOS, Android.
- OneDrive: espacio gratuito: 7GB, aplicaciones disponibles para Windows Vista, 7, 8, OS X, Xbox 360, Xbox One, iOS, Android, Windows Phone. Desde Windows 8.1 viene integrado con el sistema operativo.
- MEGA: espacio gratuito de 50 GB, aplicaciones disponibles para Chrome, Firefox, Windows, iOS, Android, Blackberry.
- Dropbox: espacio gratuito de 2 GB, con aplicaciones disponibles para Windows, Linux, OS X, Android, iOS, Blackberry, Kindle Fire.

Borrado remoto

En caso de extravío o robo de un dispositivo, muchas veces es prudente tener mecanismo de borrar nuestra información o bloquear nuestro equipos, de modo a que una persona no autorizada no acceda a nuestro equipo, no pueda acceder a nuestra información.

También para este aspecto existen diversas herramientas *anti-theft*, algunas nativas al sistema operativo, como en el caso de Android, o software de terceros que pueden ser instalados en los equipos, tanto PCs como móviles. Muchas veces los antivirus y otras herramientas de seguridad incorporan soluciones de borrado remoto y/o localización.

Hay que tener en cuenta que las aplicaciones de borrado remoto no siempre garantizan que este sea efectivo o que se pueda realizar, ya que en primer lugar es necesario que el equipo robado se conecte a Internet para poder hacerle llegar las órdenes de borrado o localización.

Además, para añadir una capa extra de seguridad, es recomendable que el disco duro se encuentre cifrado, para asegurarse de que el contenido del disco no se puede recuperar mediante herramientas de análisis o recuperación de archivos.

También es recomendable que el ordenador cuente con una contraseña de acceso como administrador o bien que se requiera al iniciar la sesión del usuario. Un truco que puede funcionar en ocasiones, y que es implementado por muchas aplicaciones *anti-theft*, consiste en crear una cuenta de invitado, que permita acceder al ordenador sin contraseña. Este tipo de cuentas de invitados no permiten acceder a los contenidos del administrador, pero sí que se haga uso del ordenador. En caso de acceso no autorizado, al entrar en Internet desde esta cuenta se permitirá que las aplicaciones de localización y borrado automático se activen.

En caso de que se formatee el ordenador o que una persona intente arrancar el equipo desde un dispositivo externo, este tipo de aplicaciones *anti-theft* no funcionarán, ya que no arrancarán. Por eso, en los casos más críticos, cuando la información es realmente valiosa, para impedir este formateo por parte de un posible ladrón, la opción más recomendable pasa por activar una contraseña en la BIOS y desactivar que se pueda arrancar el ordenador desde cualquier dispositivo externo. Esta medida más avanzada no será cubierta en esta guía.

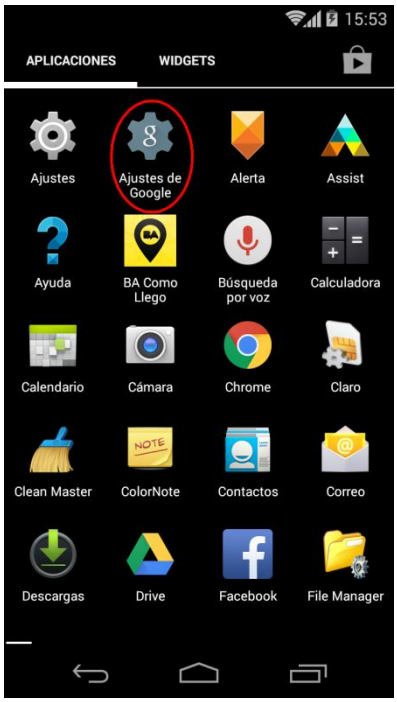
A continuación presentamos algunas posibles soluciones para el borrado remoto, que podrá ayudar para muchos casos:

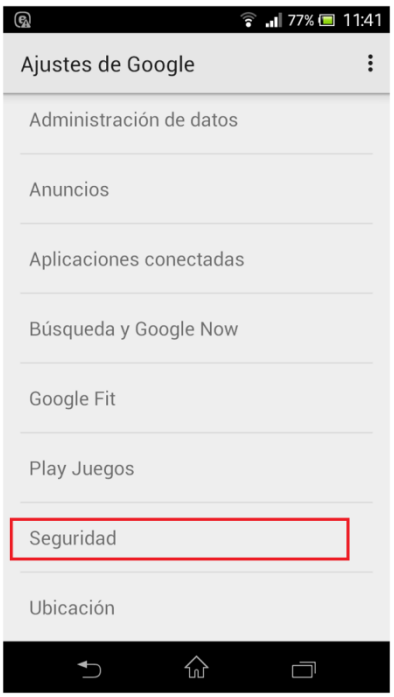
Android:

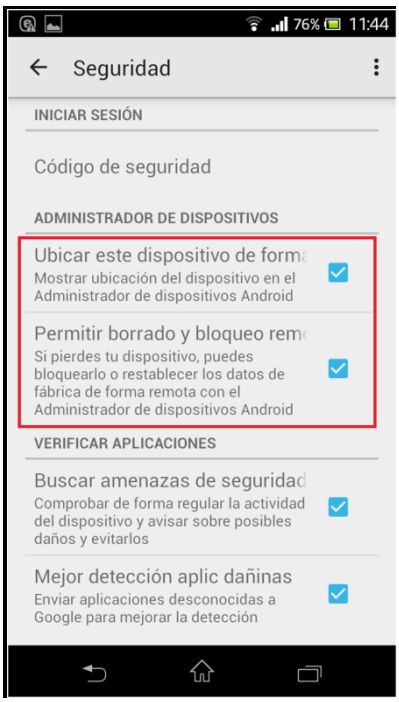
Desde el Administrador de dispositivos Android es posible utilizar las siguientes funcionalidades:

- Encontrar tu dispositivo, para mostrar la ubicación de tu dispositivo.
- Hacer sonar, bloquear o borrar los datos de un dispositivo perdido

1. En el menú de aplicaciones del dispositivo, abrimos “Ajustes de Google” y seleccionamos “Seguridad**”**.
2. En la sección "Administrador de dispositivos", tildamos la opción "Ubicar este dispositivo de forma remota" y "Permitir borrado y bloqueo remoto".

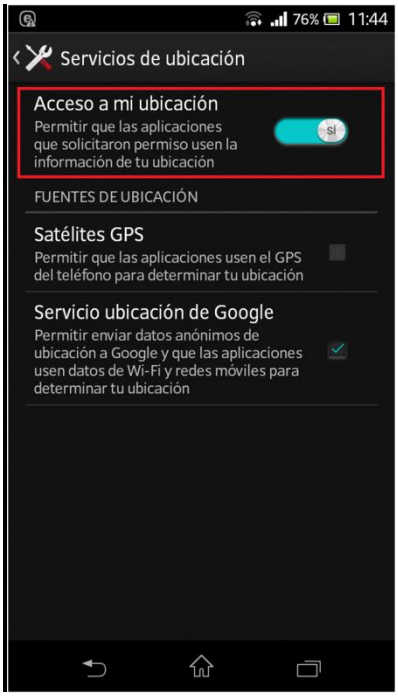


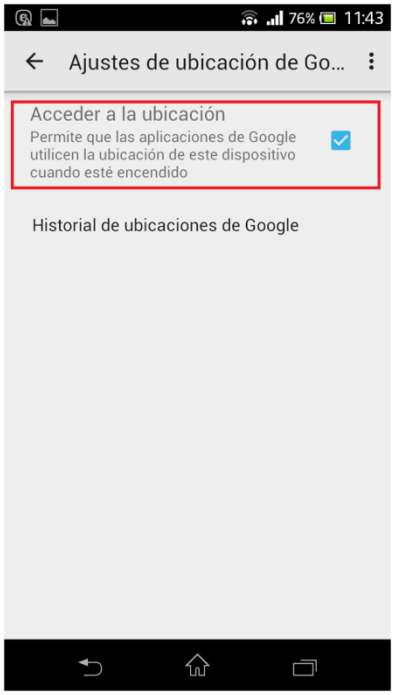




Obs.: Para poder activar la opción de Ubicación del dispositivo, es necesario tener habilitados los permisos de acceso a la ubicación por parte de aplicaciones de Google. Esto se configura tanto en los ajustes de Google como del teléfono:

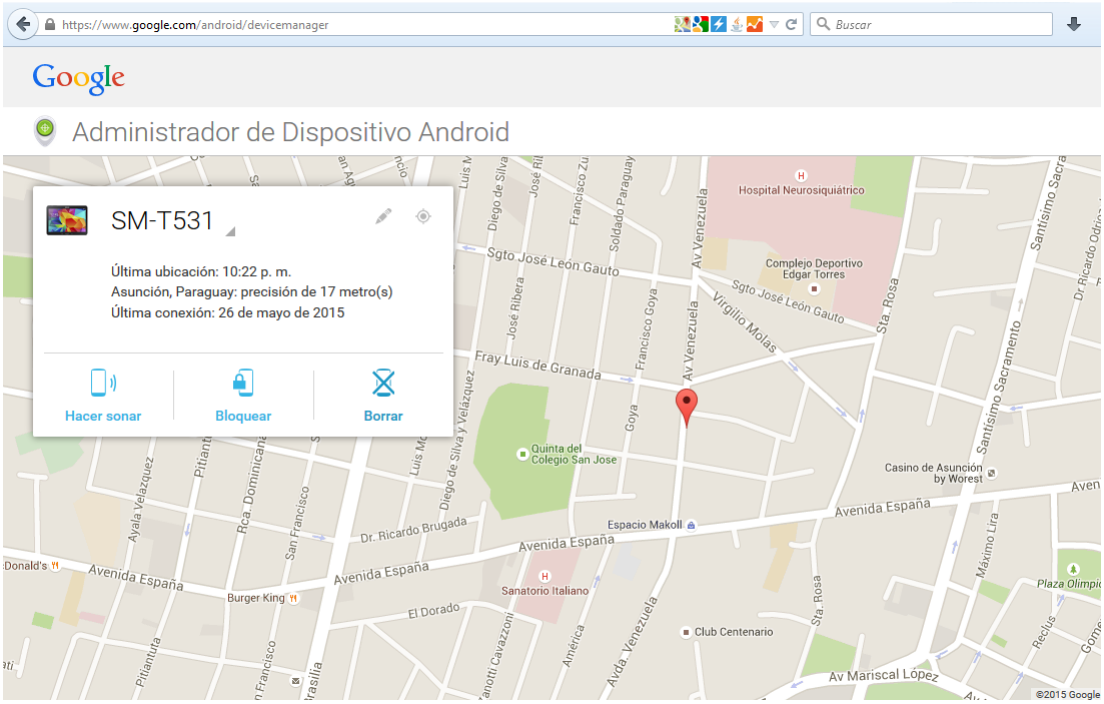
3. Vamos a “Ajustes” o “Configuración del teléfono” > “Servicios de ubicación” o “Ubicación” y permitimos el “Acceso a mi ubicación”. Debemos elegir también una fuente de ubicación, puede ser vía GPS, ubicación de Google o ambos.
4. Vamos a “Ajustes de Google” > “Ubicación” y tildamos la opción “Acceder a la ubicación”.





Para ubicar, bloquear y/o borrar remotamente los datos de tu teléfono móvil:

1. Iniciamos sesión con nuestra cuenta de Google en la página http://www.android.com/devicemanager
2. En el caso de tener varios dispositivos, desplegamos la lista con la flecha que aparece junto al nombre del dispositivo y seleccionamos el que queremos ubicar.
3. El Administrador de dispositivos Android mostrará la ubicación aproximada del dispositivo seleccionado, en caso de que estuviera conectado a una red.
4. Seleccionamos “Hacer sonar”, “Bloquear” o “Borrar”, de acuerdo a nuestro deseo. Se enviará una orden al teléfono que se ejecutará cuando éste se conecte a Internet.



Mac OS X y iOS:

Apple ofrece una solución de localización, bloqueo y borrado remoto muy similar a la de Android, a través de su servicio iCloud y la aplicación Find my iPhone.

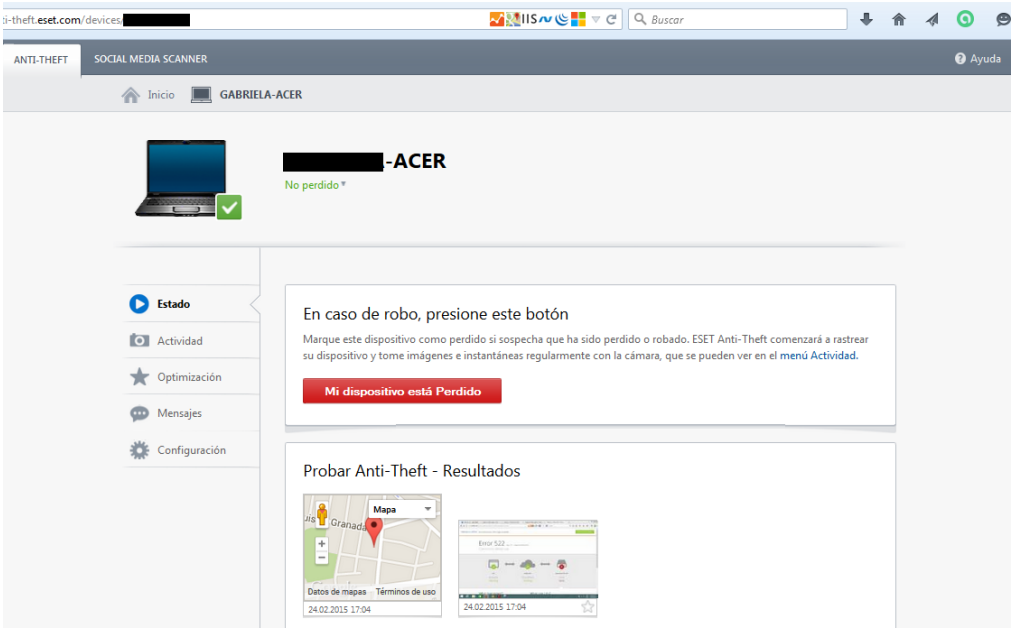
1. En el caso de un dispositivo móvil, en la pantalla de inicio del dispositivo, ingresamos a “Ajustes” > “iCloud”. En el caso de una Mac, vamos al menú Apple > “Preferencias del Sistema” y seleccionamos iCloud. Iniciamos sesión con el ID de Apple.
2. Si “Buscar mi iPhone” o “Buscar mi Mac” está desactivado, lo seleccionamos para activar.

Obs.: Para mayor seguridad, se puede configurar un código que deberá ser introducido por quien desee acceder a las aplicaciones y la información del dispositivo. Para ello vamos a Ajustes > “Código” o “Touch ID y código”. En iOS 5 o iOS 6, vamos a Ajustes > General > Bloqueo con código.

Para ubicar, bloquear y/o borrar los datos, se debe iniciar sesión en http://icloud.com/find. La orden correspondiente será enviada al dispositivo y se ejecutará cuando se conecte a Internet.

Otras herramientas:

1. Prey: es una aplicación orientada a localizar y proteger un equipo en caso de pérdida o robo, disponible para varias plataformas (Windows, Mac Os X, Linux, Android e iOS). Es de uso gratuito para un único dispositivo. https://preyproject.com
2. ESET Anti-Theft: esta herramienta viene integrada en la mayoría de las soluciones de seguridad de ESET. Incluye funciones de localización, bloqueo remoto, borrado, tomar fotografía, capturas de pantalla, etc. Está disponible para Windows y Android. Tiene una versión de prueba gratuita.



3. Norton: las soluciones de Symantec (Norton Security y Norton Mobile Security) incluyen funciones de localización, bloqueo, borrado, fotografías, etc. Está disponible para Windows, Android, Mac y iOS. Tiene una versión de prueba gratuita.

Conclusión

Como podemos ver, las amenazas cibernéticas aumentan cada día, las técnicas de los atacantes se perfeccionan constantemente, buscando acceder a lo más valioso: nuestra información.

Sin embargo, así como aumentan las amenazas, también evoluciona la industria de seguridad, ofreciéndonos cada día más herramientas y soluciones que nos ayudan a protegernos ante estas amenazas.

Estas herramientas sin embargo no pueden constituir nuestra única línea de defensa: las buenas prácticas de seguridad son fundamentales. La protección de nuestras credenciales, nuestros equipos, nuestros sistemas operativos, nuestra navegación son algunos de los aspectos mínimos que tenemos revisar y mejorar constantemente.

Debido a este escenario tan cambiante cuando hablamos de ciberseguridad, es fundamental la concienciación y capacitación continua. Conocer los riesgos nos ayudará a protegernos de éstos.

Y por último debemos mencionar que, definitivamente, no existirá nunca una seguridad total y definitiva. La seguridad es un proceso continuo, donde día a día debemos tratar de colocar nuevas barreras.