Manual de Seguridad Digital

Políticas de Seguridad Digital y Guías de Ayuda

Subsecretaría de Defensa

Palabras del Subsecretario de Defensa

El ciberespacio ha devenido en un ámbito de relación cotidiana de las personas, en torno al cual se está registrando el mayor proceso de innovación tecnológica de la economía mundial. Se está avanzando con mucha rapidez hacia la masificación de las tecnologías remotas, del Internet de las Cosas, del Big Data e incluso de la automatización que, combinadas, transformarán nuestro mundo ya revolucionado por los computadores e Internet.

Sin embargo, este incremento en el uso aumenta también nuestra dependencia y vulnerabilidad frente a las redes, que hoy se expresa en la ocurrencia, cada vez más frecuente, de incidentes y ataques informáticos. Esto nos obliga a mejorar las prácticas y reforzar los estándares de seguridad digital, tanto en nuestra vida personal como en el desempeño de las funciones propias de esta Subsecretaría de Defensa.

Para ello, hemos actualizado y simplificado las Políticas de Seguridad Digital institucionales y hemos creado guías prácticas que faciliten su implementación y adopción por parte de todas y todos los funcionarios de esta repartición pública.

Las nuevas Políticas de Seguridad Digital de la Subsecretaría de Defensa han sido elaboradas conforme a los lineamientos contenidos en la Política Nacional de Ciberseguridad, que es el primer instrumento del Estado de Chile que tiene por objeto resguardar la seguridad de las personas y de sus derechos en el ciberespacio, estableciendo cinco objetivos estratégicos y un conjunto de medidas que se debe adoptar para contar con un ciberespacio libre, abierto, seguro y resiliente.

Marcos Robledo Hoecker
Subsecretario de Defensa
Secretario ejecutivo, Comité Interministerial de Ciberseguridad

Índice general

I Políticas de Seguridad Digital

1 Definiciones y marco de aplicación 11
1.1 Propósito y contenido 11
1.2 Resumen de políticas de seguridad digital 11
1.3 Convenciones 12
1.4 Recursos digitales institucionales 12
1.5 Revisión y aprobación de la política de seguridad 12
1.6 Cumplimiento 13
1.7 Glosario 13

2 Uso aceptable de equipos electrónicos 15
2.1 Descripción 15
2.2 Objetivo 15
2.3 Alcance 15
2.4 Normas 16
2.4.1 Normas generales 16
2.4.2 En caso de robo, hurto o pérdida de equipos 16
2.4.3 Normas específicas sobre uso de teléfonos móviles 16
2.4.4 Prohibiciones 17

3 Uso aceptable de correo electrónico y redes 19
3.1 Descripción 19
3.2 Objetivo 19
3.3 Alcance 19
3.4 Normas 19
3.4.1 Uso de correo electrónico institucional 19
3.4.2 Uso de Internet y redes sociales 20
3.4.3 Representación de la Subsecretaría de Defensa 20
3.4.4 Prohibiciones 21

4 Uso de passwords 23
4.1 Descripción 23
4.2 Objetivo 23
4.3 Alcance 23
4.4 Normas 23
4.4.1 Creación de passwords 23
4.4.2 Protección de passwords 24
4.4.3 Delegación de identidad 24

5 Respuesta a incidentes de seguridad digital 25
5.1 Descripción 25
5.2 Objetivo 25
5.3 Alcance 25
5.4 Normas 25
5.4.1 Prevenir incidentes 25
5.4.2 Identificar incidentes 26
5.4.3 Remediar incidentes 26

II Guías de Seguridad Digital

6 Higiene Digital 29
6.1 Introducción 29
6.1.1 Identidades de una persona 29
6.1.2 ¿Qué es una identidad digital personal? 30
6.1.3 Protegiendo tus datos personales 31
6.1.4 Protegiendo tus dispositivos 32
6.1.5 Permisos de aplicaciones en tu teléfono 32
6.1.6 Protegiendo tu navegación 33
6.1.7 Repositorios oficiales de aplicaciones 33
6.2 Higiene digital personal 34
6.2.1 Recomendaciones básicas 34
6.2.2 Recomendaciones avanzadas 38

6.3 Higiene con dispositivos digitales 39
6.3.1 Recomendaciones básicas . . . 39
6.3.2 Recomendaciones avanzadas . . . 41
6.4 Higiene en redes digitales 41
6.4.1 Recomendaciones básicas . . . 41
6.4.2 Recomendaciones avanzadas . . . 42

7 Guía de creación de passwords . . . 45
7.1 Introducción 45
7.1.1 ¿Qué es un buen password? . . . 45
7.1.2 Recomendaciones generales . . . 46
7.2 Método 1: Usa passphrases 46
7.2.1 ¿Qué es una passphrase? . . . 46
7.2.2 ¿Cómo usar una passphrase? . . . 47
7.3 Método 2: Usa un administrador de passwords 48
7.3.1 Lastpass . . . 49
7.3.2 Dashlane . . . 50
7.3.3 Keepass . . . 51
7.4 Método 3: Usa una tarjeta de passwords 52
7.4.1 Password cards . . . 52
7.4.2 Tarjetas Qwerty . . . 54
7.5 Tipos de ataques 55
7.5.1 Ataque de "fuerza bruta" . . . 55
7.5.2 Ataque de diccionario . . . 57

Referencias . . . 61

Políticas de Seguridad Digital

1 Definiciones y marco de aplicación . . 11
1.1 Propósito y contenido
1.2 Resumen de políticas de seguridad digital
1.3 Convenciones
1.4 Recursos digitales institucionales
1.5 Revisión y aprobación de la política de seguridad
1.6 Cumplimiento
1.7 Glosario

2 Uso aceptable de equipos electrónicos 15
2.1 Descripción
2.2 Objetivo
2.3 Alcance
2.4 Normas

3 Uso aceptable de correo electrónico y redes 19
3.1 Descripción
3.2 Objetivo
3.3 Alcance
3.4 Normas

4 Uso de passwords 23
4.1 Descripción
4.2 Objetivo
4.3 Alcance
4.4 Normas

5 Respuesta a incidentes de seguridad digital 25
5.1 Descripción
5.2 Objetivo
5.3 Alcance
5.4 Normas

1. Definiciones y marco de aplicación

1.1 Propósito y contenido

Una política es un documento que fija reglas en una institución sobre qué se puede y no se puede hacer. Las políticas existen en general para proteger a las personas que trabajan en una institución, para proteger los recursos de la institución, o para mantener el orden y la seguridad dentro de la institución.

Esta sección contiene un resumen de las políticas en uso en la Subsecretaría de Defensa, una lista de los recursos digitales relevantes, convenciones de escritura, y un breve glosario de términos y abreviaturas utilizadas a lo largo del documento.

Cada una de las siguientes secciones contiene una política de seguridad digital.

La versión actualizada de este documento puede encontrarse en `http://www.ssdefensa.cl/media/2018/01/manualseguridad.pdf`.

1.2 Resumen de políticas de seguridad digital

La Subsecretaría de Defensa cuenta actualmente con cuatro políticas de seguridad digital:

1. **Uso aceptable de equipos electrónicos**: describe qué constituye un uso aceptable de los recursos electrónicos institucionales: computadores de escritorio, computadores portátiles (laptops), teléfonos fijos y teléfonos móviles.
2. **Uso aceptable de correo electrónico institucional y redes**: describe qué constituye un uso aceptable del correo electrónico institucional y de las redes sociales a través de las redes institucionales; describe también qué constituye un uso aceptable de las redes de la institución y del ancho de banda.
3. **Uso de passwords**: describe qué constituye un uso aceptable de passwords para acceder a recursos institucionales a través de computadores o redes institucionales.
4. **Respuesta a incidentes de seguridad digital**: describe qué debe hacerse para prevenir incidentes de seguridad, y para identificar y remediar incidentes cuando suceden.

1.3 Convenciones

A lo largo de este documento, se ha hecho esfuerzos para describir los cargos y ocupaciones de manera neutra en términos de género. Sin embargo, cuando ha sido necesario escoger un término, por brevedad y facilidad de expresión se utilizan apelativos masculinos (p.ej., subsecretario). Esto no debe ser interpretado como discriminatorio en términos de género.

1.4 Recursos digitales institucionales

Un recurso digital institucional es todo sitio web, base de datos, directorio digital, listas de correo electrónico, intranets, aplicaciones, o en general cualquier software u objeto digital que pertenece a la Subsecretaría de Defensa, y que es usado y compartido entre dos o más usuarios.

Los recursos institucionales digitales que actualmente se encuentran disponibles son los siguientes:

1. **Correo electrónico institucional**: El correo electrónico es el principal mecanismo de comunicación entre funcionarios. Existen dos aplicaciones para acceder al correo electrónico institucional:
   a) **Microsoft Outlook**: Este es el medio principal y preferente de acceso al correo electrónico institucional. Requiere del uso de un computador provisto por la SSD, y de la instalación del software MS Outlook. Para acceder al correo electrónico a través de este medio se requiere de un username y password.
   b) **Zimbra**: Este es un medio alternativo de acceso al correo institucional. No requiere de un computador provisto por la SSD; sí se requiere de un browser y de autentificarse a través de username y password cada vez que se ingresa a la aplicación. Se puede acceder a este recurso en la siguiente URL: `https://zimbra.ssdefensa.cl/`
2. **Sistema de gestión de documentos y archivos digitales (Sistedoc)**: Sistema de gestión de documentos a través de un browser. Para acceder a este recurso se requiere de un username y password.
3. **Intranet institucional**: Sitio web institucional con información diversa. Para acceder a este recurso se requiere de un username y password.

1.5 Revisión y aprobación de la política de seguridad

1. La presente política se revisará completamente una vez al año a contar de su última aprobación. Dicha revisión será efectuada por el área de auditoría, a través de un procedimiento definido por dicha área. El objetivo de la revisión será:
   a) Verificar si la política está de acuerdo con cambios en la legislación vigente, y con las normativas publicadas desde la última revisión.
   b) Verificar si la política requiere de modificaciones debido a cambios que se haya producido en la Subsecretaría de Defensa. Estos cambios pueden ser organizacionales, administrativos, políticos, etc.
2. En cualquiera de los casos anteriores, la política será modificada y la nueva versión será revisada y aprobada mediante resolución exenta del Subsecretario de Defensa.
3. El responsable de mantener actualizada esta política y de difundirla al personal de la Subsecretaría de Defensa es el Encargado de Seguridad.

1.6 Cumplimiento

1. El área informática chequeará periódicamente el cumplimiento de cada una de las políticas vigentes a través de varios métodos, pudiendo incluir entre otras medidas la revisión presencial y remota de equipos electrónicos institucionales, monitoreo por video, y auditorías internas y externas.
2. Cualquier excepción a esta política deberá ser aprobada previamente por el área informática.
3. Todo usuario que sea sorprendido incumpliendo cualquiera de las normativas contenidas en esta política será advertido a través de correo electrónico institucional, y el incumplimento será informado al Encargado de Seguridad. En caso de que el correo electrónico institucional no esté operativo, se informará al usuario presencialmente o a través de correo certificado.
4. Si un usuario es sorprendido incumpliendo una normativa por segunda vez, el incumplimiento será reportado al Subsecretario de Defensa y será sancionado administrativamente, conforme a lo dispuesto en el Título V de la Ley 18.834, que aprueba el Estatuto administrativo.

1.7 Glosario

Browser o navegador : Software que permite visualizar páginas web. Existen muchas marcas distintas de browsers: los más conocidos son Chrome y Chromium (de Google), Firefox (de Fundación Mozilla), Opera (de Fundación Opera), y Safari (de Apple). El browser Internet Explorer (de Microsoft) está siendo discontinuado, y su uso no se recomienda.

Contactos personales : Respecto de un usuario de la Subsecretaría de Defensa, se refiere a datos de contacto de personas que no tienen una relación laboral con el usuario.

Cuentas personales : Todas aquellas cuentas de correo electrónico o redes sociales que pertenecen a un usuario de la Subsecretaría de Defensa, pero que son de uso privado e individual, y que no son controlados ni provistos por la Subsecretaría de Defensa.

Correo electrónico institucional : Cuenta de correo electrónico asignada a un usuario de la Subsecretaría de Defensa y administrada por ésta. Las direcciones de correo electrónico institucional siempre tienen la forma de `username@ssdefensa.gob.cl`; por ejemplo, si el usuario "Juan Pérez" posee el username **jperez**, su correo electrónico institucional será `jperez@ssdefensa.gob.cl`.

Correo electrónico personal : Toda cuenta de correo electrónico que pertenece a un usuario de la Subsecretaría de Defensa, pero que es provista por un proveedor externo, no contratado por la Subsecretaría de Defensa; p.ej., Gmail, Yahoo, etc.

Equipo electrónico institucional o Equipo institucional : Cualquier aparato electrónico que sea propiedad de la subsecretaría de defensa, y que es temporalmente puesto a disposición de un usuario para ayudarlo a cumplir con su labor. Por ejemplo, un computador de escritorio, un computador portátil, un teléfono móvil (smarphone), un teléfono fijo, una impresora, un router, un switch, etc.

Equipo electrónico personal : Aquel aparato electrónico que sea propiedad de un usuario de la Subsecretaría de Defensa.

Grupo de informática o Área informática : Grupo de personas que proveen servicios de apoyo a funcionarios de la Subsecretaría de Defensa en las siguientes actividades:

1. Instalación y soporte de equipos electrónicos institucionales, junto con la conexión a redes de estos equipos.
2. Instalación y administración de aplicaciones y programas en los equipos anteriores.

Horario hábil : Lunes a viernes, de 08:00 a 17:00 horas, exceptuando días feriados.

Horario inhábil : Cualquier instante que queda fuera de la definición de horario hábil.

Incidente de seguridad : Cualquier evento que involucre equipos institucionales o redes institucionales, y que contravenga alguna de las normas de la Subsecretaría de Defensa.

Listas negras (blacklists) : Listas públicas de nombres de dominios, URLs o direcciones IP que han sido reportados por distribuir malware o por enviar correo electrónico no deseado (spam). Estas listas usualmente son administradas por empresas de seguridad o grandes corporaciones (p.ej., Google, Apple) para proteger a los usuarios que hacen uso de sus productos o servicios.

Password provisional : Aquel password que es asignado de manera temporal para acceder por primera vez a un servicio o recurso digital institucional. Usualmente, un password provisional es comunicado al titular ya sea verbalmente o por escrito.

Recurso digital institucional : Todo sitio web, base de datos, directorio digital, listas de correo electrónico, intranets, aplicaciones, o en general cualquier software u objeto digital que pertenece a la Subsecretaría de Defensa, y que es usado y compartido entre dos o más usuarios.

Redes sociales : Facebook, Twitter, LinkedIn, Instagram, Pinterest, y en general cualquier otro servicio de comunicación masiva en Internet.

Redes institucionales : Todas aquellas redes y equipos de comunicaciones de propiedad de la Subsecretaría de Defensa, que sean utilizados para comunicar a dos o más usuarios entre sí y a Internet. Esta denominación incluye cables de red, puntos de red, routers, switches, firewalls, IPS, IDS, y en general cualquier otro equipo de comunicaciones en uso en instalaciones de la Subsecretaría.

Username : Nombre de usuario utilizado para identificar a un usuario de manera única.

Usuario o funcionario : Cualquier persona que trabaja para la Subsecretaría de Defensa, independientemente del tipo de vinculación laboral que mantenga con la institución. En este documento ambos términos se usan indistintamente.

2. Uso aceptable de equipos electrónicos

2.1 Descripción

Para cumplir con su misión, la Subsecretaría de Defensa provee a todos sus usuarios de aquellos equipos electrónicos institucionales que se considere necesarios. El activo más importante de toda organización, sin embargo, no son estos equipos sino las personas y la información que manejan. Es necesario, por tanto, fijar algunas normas para proteger tanto a nuestros usuarios como a la información que manejamos. Un uso inadecuado de los equipos institucionales nos expone entre otras cosas a infecciones por virus, ataques informáticos y filtración de información secreta o reservada.

La versión actualizada de este documento puede encontrarse en `http://www.ssdefensa.cl/media/2018/01/manualseguridad.pdf`.

2.2 Objetivo

El objetivo de esta política es fijar las normas de uso aceptable de equipos electrónicos institucionales en la Subsecretaría de Defensa.

2.3 Alcance

Esta política es aplicable a todos los usuarios que reciben un equipo electrónico institucional, independientemente de si se trata de funcionarios de planta, contrata, o personal a honorarios; o de si se trata de funcionarios en comisión de servicio o en calidad de delegados de otras instituciones trabajando en dependencias de la Subsecretaría de Defensa.

2.4 Normas

2.4.1 Normas generales

1. Los equipos provistos por la subsecretaría a cada usuario son de propiedad de la Subsecretaría de Defensa. La Subsecretaría de Defensa es titular de toda la información que se almacena en los equipos de la Subsecretaría de Defensa. La Subsecretaría de Defensa mantendrá un registro de cada una de las personas a las que le son asignados uno o más equipos electrónicos.
2. Cada usuario es responsable de proteger físicamente tanto los equipos que se le asignen como la información que en ellos se almacene, en la medida que esta protección no ponga en riesgo su integridad física (por ejemplo, en caso de robo con intimidación o con violencia).
3. Cada usuario es responsable de proteger el acceso a cada equipo que se le asigne a través de un password, de acuerdo con lo establecido en la política **Uso de Passwords** (pág. 23).
4. Cada usuario puede acceder, utilizar o compartir la información de la Subsecretaría de Defensa sólo en la medida que sea necesario para realizar su trabajo.
5. Cada usuario tiene la responsabilidad de ejercer el sentido común respecto al uso de los equipos institucionales para actividades personales. En caso de duda, un usuario debe preguntar a su jefe directo, o en su ausencia, al Encargado de Seguridad.
6. Por razones de seguridad, el personal del área informática podrá monitorear remotamente las actividades realizadas por cada usuario a través de los equipos institucionales que le fueron asignados. Este monitoreo en ningún caso tiene por objetivo vigilar las acciones de un usuario, sino detectar software malicioso que pudiera poner en riesgo la información de la Subsecretaría o la identidad de los usuarios de la Subsecretaría.

2.4.2 En caso de robo, hurto o pérdida de equipos

1. En caso de robo, hurto o pérdida de un equipo institucional, el usuario a quien fue entregado el equipo debe reportar el evento dentro de las 12 horas siguientes a que se produzca, o de que se advierta por primera vez su ausencia, incluso si el evento se produce durante horario inhábil.
2. Todo robo, hurto o pérdida debe ser reportada a través de una de las siguientes opciones:
   a) A través de la URL `http://172.20.5.20/plataforma/soporte/`,
   b) Al correo electrónico `incidente@ssdefensa.cl`,
   c) A través de una llamada al número +569 7976 9705.
3. En caso de reportar un robo, hurto o pérdida a través de correo electrónico o de una llamada telefónica, se debe reportar lo siguiente:
   a) Nombre del usuario que realiza el reporte o su username,
   b) En caso de robo, debe reportarse fecha, hora y lugar del evento. En caso de hurto o pérdida, fecha y hora del momento en que se advirtió por primera vez la falta del equipo, y la fecha y hora estimada del último uso del equipo.
   c) Circunstancias en que se produjo el robo o pérdida.
4. En caso de robo o hurto de un equipo, es responsabilidad del usuario el reportar dicho robo a la comisaría más cercana.

2.4.3 Normas específicas sobre uso de teléfonos móviles

Las normas contenidas en esta sección son aplicables a aquellos usuarios a los que les hayan sido asignados teléfonos móviles (smartphones), y deben ser cumplidas en adición a las normas y prohibiciones en el resto de esta política.

1. Los teléfonos móviles (smartphones) asignados por la Subsecretaría de Defensa a algunos usuarios tienen el propósito exclusivo de mantener una línea dedicada de comunicación tanto de voz como de datos con dichos usuarios.
2. Antes de recibir un teléfono móvil, cada usuario deberá firmar un documento donde dice que conoce tanto la política **Uso aceptable de equipos electrónicos** (esta política, pág. 15) como la política **Uso aceptable de correo electrónico y redes** (pág. 19).
3. Las siguientes aplicaciones de comunicaciones serán instaladas en cada teléfono móvil asignado a usuarios de la Subsecretaría de Defensa:
   a) **WhatsApp**, desarrollada por *WhatsApp Inc.* (`https://www.whatsapp.com/`): para mensajes no confidenciales.
   b) **Signal Private Messenger**, desarrollada por *Open Whisper Systems* (`https://whispersystems.org/`): para mensajes confidenciales.
   c) **iPGMail**, desarrollada por *Wyllys Ingersoll* (`https://ipgmail.com/`): para envío de correo electrónico institucional, ya sea cifrado, firmado, o ambos.
   d) **SonicWall**, desarrollada por *SonicWALL Inc.* (`https://www.sonicwall.com/es/`): para conexión a una red virtual privada (VPN).
4. Si un usuario necesita utilizar una aplicación distinta de las indicadas en el punto anterior, podrá solicitar por escrito al Encargado de Seguridad que se instale dicha aplicación en su teléfono, justificando la necesidad. El Encargado de Seguridad podrá autorizar o no la instalación de la aplicación, basado exclusivamente en criterios de seguridad informática. Dicha autorización deberá ser por escrito.
5. Los usuarios que tengan acceso a un correo electrónico a través del teléfono móvil que se les asigne deben seguir estrictamente la política **Uso aceptable de correo electrónico y redes** (pág. 19) para el uso de dicho correo electrónico.
6. Los usuarios que se conecten a través de su teléfono móvil a cualquier sitio web o servicio en línea desde el extranjero, deben hacerlo a través de la aplicación VPN instalada para ello.
7. Los usuarios que reciban un teléfono de de la Subsecretaría de Defensa no deben:
   a) Instalar aplicaciones en el teléfono.
   b) Desinstalar o modificar aplicaciones ya instaladas en el teléfono.
   c) Modificar de cualquier manera la configuración del teléfono.
   d) Agregar contactos personales al teléfono, tanto en las aplicaciones identificadas anteriormente, como en la aplicación de contactos nativa del teléfono.
   e) Utilizar la cámara del teléfono.
   f) Permitir que cualquier otra persona utilice el teléfono, incluyendo familiares y amigos.
   g) Reinstalar el sistema operativo del teléfono con privilegios elevados (*rooting* o *jailbreaking*), o pedirle a otra persona que lo haga, independientemente de si esta actividad es o no pagada.

2.4.4 Prohibiciones

Las actividades en la lista a continuación están en general prohibidas a todos los usuarios de la Subsecretaría de Defensa. Esta lista no pretende ser exhaustiva, sino entregar lineamientos sobre aquellas actividades que son consideradas inadecuadas. Toda excepción debe ser autorizada expresamente por el Encargado de Seguridad.

Las siguientes actividades están prohibidas para todos los usuarios de la Subsecretaría de Defensa:

1. Bajar o instalar software, plug-ins, add-ons o cualquier otra aplicación propietaria en un equipo electrónico institucional, si el usuario o la Subsecretaría no cuenta con la licencia correspondiente.

2. Bajar, instalar, almacenar o reenviar software malicioso, como virus, gusanos, troyanos, bombas de correo electrónico, etc.
3. Conectar cualquier equipo electrónico personal a la red institucional; en específico, está estrictamente prohibido conectar un router inalámbrico personal o un switch personal a cualquier punto de red de la Subsecretaría. En casos justificados, un usuario podrá conectar su computador personal a la red institucional, si cuenta con una autorización previa del Encargado de Seguridad. Para pedir autorización para conectar un equipo electrónico personal a la red institucional, debe pedir autorización a través de la siguiente URL: `http://172.20.5.20/plataforma/soporte/`.
4. Instalar o ejecutar scripts o programas cuya intención sea interferir con, desactivar o impedir la operación normal de las redes institucionales, o de los equipos institucionales de otros usuarios.
5. Ejecutar cualquier clase de monitoreo de la red institucional que no haya sido autorizada expresa y previamente por el Encargado de Seguridad, a menos que este monitoreo sea parte de las labores habituales del usuario.
6. Instalar cualquier clase de software o aplicación que permita eludir o anular el ingreso de passwords para acceder a un equipo institucional. La única excepción a esta norma serán las aplicaciones descritas en la **Guía de creación de passwords** (pág. 45).

3. Uso aceptable de correo electrónico y redes

3.1 Descripción

Esta política describe qué constituye un uso aceptable del correo electrónico institucional y de las redes sociales a través de las redes institucionales; describe también qué constituye un uso aceptable de las redes institucionales y del ancho de banda.

La versión actualizada de este documento puede encontrarse en `http://www.ssdefensa.cl/media/2018/01/manualseguridad.pdf`.

3.2 Objetivo

El objetivo de esta política es fijar las normas de uso aceptable del correo electrónico institucional y de las redes institucionales, operadas o contratadas por la Subsecretaría de Defensa.

3.3 Alcance

Esta política es aplicable a todos los usuarios que hacen uso de las redes de la Subsecretaría de Defensa, o que hacen uso del correo electrónico institucional, independientemente de si lo hacen a través de equipos electrónicos institucionales o a través de equipos personales, e independientemente de si se trata de funcionarios de planta, contrata, o personal a honorarios.

3.4 Normas

3.4.1 Uso de correo electrónico institucional

1. El correo electrónico institucional es provisto a un usuario exclusivamente para comunicarse con el resto de los usuarios, y con personas externas a la Subsecretaría cuando su labor así lo requiera. El correo electrónico institucional no debe ser usado para crear cuentas en redes sociales, sitios

de comercio electrónico, tiendas de comercio, o en general cualquier clase de servicio provisto en línea, excepto si este servicio está directamente relacionado con la labor del usuario.

2. Por razones de seguridad, el correo electrónico institucional es revisado por programas automáticos para filtrar virus, malware, spam, y otros tipos de amenazas que se esparcen a través del correo electrónico. A pesar de que el correo electrónico institucional no será leído o revisado por seres humanos, los mensajes de los usuarios pueden ser revisados por filtros automáticos y ser marcados para ser revisados posteriormente por personal del área informática en caso de que el contenido del mensaje calce con criterios predefinidos de riesgo.

3.4.2 Uso de Internet y redes sociales

1. Un usuario puede navegar normalmente por Internet a través de las redes institucionales, ejerciendo su buen juicio para decidir qué sitios visita, y siendo austero en términos del ancho de banda que utiliza. En este sentido, se recomienda lo siguiente:
   a) Está permitido escuchar música a través de Internet, siempre y cuando se detenga la reproducción cuando el usuario se ausente de su lugar de trabajo.
   b) Evitar reproducir películas a través de Internet; por ejemplo, a través de servicios como Netflix o YouTube.
2. Por razones de seguridad, todos los sitios que un usuario visita podrían ser monitoreados por filtros automáticos, y algunos sitios pueden ser marcados por filtros automáticos para ser revisados por personal del área informática.
3. El área informática puede bloquear parcial o completamente sitios web o direcciones en Internet cuando:
   a) Estas direcciones se encuentren en listas negras de cualquier tipo. El área informática podrá publicar una lista de aquellas listas negras que utiliza para bloquear sitios web.
   b) Estas direcciones contengan pornografía, o contenido difamatorio o denigrante para cualquier persona; o contenido racista o discriminador de cualquier especie.
   c) El Subsecretario de Defensa u otra autoridad así lo solicite bajo razones fundadas.
4. Un usuario puede hacer uso de sus cuentas personales de redes sociales o de su correo electrónico personal a través de las redes institucionales, siempre y cuando:
   a) Este uso no lo distraiga de sus labores habituales,
   b) No revele información relacionada con su trabajo o el trabajo realizado por otros usuarios de la Subsecretaría de Defensa,
   c) Sus mensajes no sean difamatorios, denigrantes, racistas, o discriminadores para con cualquier otro usuario de la Subsecretaría, o para personas externas a la Subsecretaría de Defensa.
   d) No haga uso excesivo del ancho de banda puesto a disposición de los usuarios de la Subsecretaría. El qué constituye un uso excesivo será analizado caso a caso por el área informática; en caso de duda, un usuario debe preguntar al Encargado de Seguridad.
5. El uso y administración de las cuentas de redes sociales oficiales de la Subsecretaría de Defensa estará reservado exclusivamente a usuarios autorizados por el Subsecretario de Defensa, a través de una resolución exenta.

3.4.3 Representación de la Subsecretaría de Defensa

1. Todo mensaje de un usuario de la Subsecretaría de Defensa a través de redes sociales es de su exclusiva responsabilidad, y no compromete de manera alguna la posición o parecer de la

Subsecretaría, ni de sus autoridades. La única excepción a esta norma la constituyen los mensajes de las más altas autoridades (Ministros y Subsecretarios).

2. Ningún usuario está autorizado para enviar mensajes a través de redes sociales en nombre de la Subsecretaría de Defensa, a excepción de las más altas autoridades (Ministros y Subsecretarios) y quienes ellas autoricen expresamente.

3.4.4 Prohibiciones

Las siguientes actividades están prohibidas para todos los usuarios de la Subsecretaría de Defensa. Toda excepción debe ser autorizada expresamente por el Encargado de Seguridad.

Está estrictamente prohibido:

1. Utilizar el correo electrónico institucional para crear cuentas en servicios de apuestas en línea, sitios pornográficos, sitios de citas o de búsqueda de pareja, o cualquier otro sitio cuyo uso vaya en contra de lo establecido en el artículo 61, letras g), h) e i) del Estatuto Administrativo fijado por la Ley 18.834.
2. Utilizar las redes institucionales para bajar, almacenar, distribuir, reenviar o transmitir cualquier material que infrinja la Ley 17.336 sobre Propiedad Intelectual y Derecho de Autor; por ejemplo, música, películas, series de televisión, aplicaciones, libros, imágenes, fotografías, etc.
3. Utilizar las redes institucionales para bajar, almacenar, distribuir o reenviar cualquier tipo de material pornográfico, ya sea a través de imágenes, audio, o video,
4. Utilizar el correo electrónico institucional o las redes institucionales para vender productos u ofrecer servicios de cualquier naturaleza,
5. Utilizar el correo electrónico institucional para enviar correo electrónico no solicitado (spam),
6. Utilizar el correo electrónico institucional o las redes institucionales para enviar mensajes para acosar o molestar sexualmente a otras personas, pertenezcan éstas o no a la institución.

4. Uso de passwords

4.1 Descripción

La selección y uso de buenos passwords constituye una parte importante de la seguridad de una institución. Un "buen password" es aquel que es fácil de recordar por su titular, difícil de adivinar por otras personas, y difícil de averiguar a través de medios automáticos. Un mal password puede ser adivinado por otras personas, y puede permitir a esas personas tener acceso a recursos a los que no debería tener acceso. Todos los usuarios somos responsables de escoger buenos passwords para los recursos digitales institucionales a los que se nos provee acceso.

La versión actualizada de este documento puede encontrarse en `http://www.ssdefensa.cl/media/2018/01/manualseguridad.pdf`.

4.2 Objetivo

El objetivo de esta política es fijar las normas de uso aceptable de passwords en la Subsecretaría de Defensa.

4.3 Alcance

Esta política es aplicable a todos los usuarios que tienen acceso a recursos digitales institucionales, independientemente de si se trata de funcionarios de planta, contrata, o personal a honorarios.

4.4 Normas

4.4.1 Creación de passwords

1. Todos los recursos digitales institucionales deberán ser protegidos a través de un password. Todo password debe ser creado siguiendo lo establecido en la **Guía de uso de passwords** (pág. 45).

2. A veces, por razones de buen servicio, a un usuario se le asigna un password provisional que es comunicado verbalmente o que es entregado por escrito en una hoja de papel. Todo usuario al que se le asigna un password provisional deberá cambiar este password la primera vez que ingrese al recurso digital correspondiente.

4.4.2 Protección de passwords

1. Un password siempre es de uso personal. Un usuario no debe revelar ni compartir ninguno de sus passwords con otros usuarios, incluyendo asistentes, secretarios, administradores, y familiares del usuario. Esto es aplicable especialmente cuando un equipo electrónico institucional sea usado en el hogar del usuario, o cuando el usuario está de vacaciones, con permiso o fuera de su puesto de trabajo.
2. Un password no debe ser compartido ni revelado bajo ninguna circunstancia a personas externas a la Subsecretaría de Defensa, incluyendo familiares del usuario o personas que vivan bajo el mismo techo que el usuario.
3. Un password debe ser único; es decir, no debe ser reutilizado en ningún otro recurso institucional digital.
4. Un password no debe ser almacenado en medios físicos o digitales, tales como archivos de texto sin encriptar, pendrives USB, discos duros externos, CDs o DVDs. En particular, un usuario no debe utilizar la funcionalidad de almacenamiento de passwords ofrecida por los browsers.
5. Un password no debe ser enviado ni comunicado oralmente, a través del teléfono, correo físico, memorándums, oficios, circulares, correo electrónico, mensajes de texto (SMS), fotos, imágenes, o cualquier otro medio físico o digital.
6. Un password no debe ser escrito ni guardado en ninguna parte de la oficina de un funcionario. La única excepción a esta norma son las tarjetas de passwords, descritas en el documento **Guía de creación de passwords** (pág. 45).
7. Periódicamente, el área informática intentará adivinar de manera automática los passwords utilizados en los recursos institucionales digitales. En caso de que un password sea adivinado, se le informará al usuario para que modifique su password de acuerdo con lo establecido en la **Guía de creación de passwords** (pag. 45).
8. El que una persona averigüe el password de un usuario a través de cualquier método constituye un acceso no autorizado a los recursos digitales institucionales. Todo usuario que sospeche que uno de sus passwords pueda haber sido averiguado o espiado por otras personas deberá:
   a) cambiar inmediatamente su password, y
   b) reportar el incidente inmediatamente al Encargado de Seguridad. Para reportar el incidente, el usuario debe seguir el procedimiento establecido en la política **Respuesta a Incidentes de Seguridad Digital** (pág. 25).

4.4.3 Delegación de identidad

1. En caso de que un funcionario/a, por la naturaleza de su cargo, deba delegar parte de la administración de su identidad a otros funcionarios/as, deberá solicitar apoyo al área informática para poder realizar estas acciones sin que tenga que revelar su password a otras personas.

5. Respuesta a incidentes de seguridad digital

5.1 Descripción

Cualquier persona dentro de una institución puede hoy sufrir un incidente de seguridad digital. La mayor parte de las políticas y guías de buenas prácticas de la Subsecretaría de Defensa están dedicadas a prevenir la ocurrencia de incidentes de seguridad digital. Sin embargo, es fundamental que en caso de que ocurra un incidente, la o las personas que sepan del incidente sean capaces de reconocerlo y reportarlo, para que entre todos seamos capaces de remediar las consecuencias del incidente.

5.2 Objetivo

El objetivo de esta política es establecer un procedimiento a seguir por todo usuario, una vez que se ha reconocido un ataque digital a equipos electrónicos institucionales, recursos digitales institucionales, a funcionarios de la institución, o a información secreta o reservada de la institución.

5.3 Alcance

Esta política es aplicable a todos los usuarios que tienen acceso a recursos digitales institucionales o a equipos electrónicos institucionales, independientemente de si se trata de funcionarios de planta, contrata, o personal a honorarios.

5.4 Normas

5.4.1 Prevenir incidentes

Todo usuario debe conocer y practicar lo contenido en la **Guía de Higiene Digital** (pág. 29), con el objetivo de prevenir ataques digitales sobre los equipos electrónicos que le son asignados y sobre los recursos digitales institucionales a los que tiene acceso.

5.4.2 Identificar incidentes

Todo usuario debe conocer lo contenido en la **Guía de Identificación de Incidentes de Seguridad**, con el objetivo de saber identificar los incidentes de seguridad allí descritos.

5.4.3 Remediar incidentes

Todo usuario que ha identificado un incidente de seguridad en un equipo electrónico a su cargo debe seguir el siguiente procedimiento:

- Si se trata de un teléfono móvil:
  1. Apague inmediatamente el teléfono y no vuelva a encenderlo.
  2. De ser posible, retire la batería y la tarjeta SIM.
  3. Si tiene acceso inmediato a Internet a través de otro equipo distinto del teléfono, abra la siguiente URL y siga las instrucciones que allí se indican para reportar el incidente:`http://172.20.5.20/plataforma/soporte/`.
  4. Si no tiene acceso inmediato a Internet pero tiene acceso a otro teléfono, comuníquese inmediatamente con el Encargado de Seguridad al teléfono +569 7976 9705 para reportar el incidente.
  5. Entregue físicamente el teléfono, la batería y la tarjeta SIM a la brevedad posible al Encargado de Seguridad.
- Si se trata de un computador de escritorio o computador portátil:
  1. Si el computador está conectado a la red, desenchufe inmediatamente el cable de red. No apague el computador.
  2. Si tiene acceso inmediato a Internet a través de otro computador, abra la siguiente URL y siga las instrucciones que allí se indican para reportar el incidente: `http://172.20.5.20/plataforma/soporte/`.
  3. Si no tiene acceso inmediato a Internet, comuníquese inmediatamente con el Encargado de Seguridad al teléfono +569 7976 9705 para reportar el incidente.
  4. Si no tiene acceso inmediato ni a Internet ni acceso a un teléfono, consiga un computador con conexión a Internet o un teléfono lo más pronto posible para reportar el incidente.

II Guías de Seguridad Digital

6 Higiene Digital 29

6.1 Introducción
6.2 Higiene digital personal
6.3 Higiene con dispositivos digitales
6.4 Higiene en redes digitales

7 Guía de creación de passwords 45

7.1 Introducción
7.2 Método 1: Usa passphrases
7.3 Método 2: Usa un administrador de passwords
7.4 Método 3: Usa una tarjeta de passwords
7.5 Tipos de ataques

Referencias 61

6. Higiene Digital

6.1 Introducción

La higiene, en términos generales, es el conjunto de técnicas y procedimientos que se utiliza para controlar aquellos factores que perjudican la salud[1]. La higiene digital personal[2] tiene que ver con proteger tanto las identidades digitales que uno posee, como los datos que están asociados a ellas.

Este capítulo presenta 21 recomendaciones de higiene digital personal. Estas recomendaciones van dirigidas a los funcionarios de la administración pública, que deben tener especial cuidado en proteger su información y la información de las instituciones donde trabajan. Sin embargo, este capítulo debería ser útil para todas las personas que quieran tomar medidas básicas de higiene digital.

Las recomendaciones en este capítulo están divididas en tres grupos: higiene digital personal (sección 6.2); higiene con dispositivos digitales (sección 6.3); e higiene en redes digitales (sección 6.4). El resto de esta sección introduce algunos conceptos básicos para comprender el resto del capítulo.

6.1.1 Identidades de una persona

La identidad, en el contexto de la seguridad digital, es el conjunto de datos que están asociados indisolublemente a una persona, y que permiten distinguirla de manera única dentro de un grupo (potencialmente grande) de personas.

Todas las personas tienen múltiples identidades, en el sentido de la información que manejan diariamente. Imaginemos por ejemplo una persona (Fulano Sutano) que trabaja en la Subsecretaría de Defensa. En este rol, posee múltiples deberes y responsabilidades. Posee un correo electrónico

[1] `https://es.wikipedia.org/wiki/Higiene`. Consultado el 28/abril/2017. Curiosamente, el código sanitario chileno (`http://bcn.cl/1uv0j`), que fija y ordena todas aquellas materias relacionadas con el "fomento, protección y recuperación" de la salud pública, menciona 13 veces el término "higiene", sin definirlo.

[2] El término es arbitrario, y no es utilizado formalmente en la literatura sobre seguridad informática. En este texto, es utilizado sólo como una metáfora conveniente.

institucional (`fsutano@ssdefensa.gob.cl`), que debe usar responsablemente, sólo para labores de su trabajo. Posee una credencial (una tarjeta contact-less), que debe ser usada para entrar y salir de las dependencias del Ministerio de Defensa, pero que no es válida para ingresar a ninguna otra dependencia del sector público. Posee un username y un password para entrar a su correo electrónico, otro username y password para entrar a la Intranet institucional, y otro username y password para ingresar al Sistema de Documentación Electrónica de la institución, a través del cual recibe los documentos que llegan oficialmente a su área.

En su vida personal, esta persona tiene una familia y amigos personales. Posee un email personal (`fulano.sutano@gmail.com`), que utiliza para comunicarse con sus amigos y familia, y para recibir correos de cuentas por pagar. Posee una cuenta corriente, e ingresa a ella con su RUN y un password. Posee cuentas en múltiples tiendas de retail, y paga sus compras en línea, en los sitios web de cada tienda, a los que ingresa a través de su username (`fulano.sutano@gmail.com`) y password correspondientes. Tiene también una cuenta en Facebook (a la que ingresa con su número de teléfono y un password), en Twitter (`@fulanosutano`, para el que requiere otro password), y en LinkedIn (para mantener contactos profesionales). Tiene también el correo electrónico de la Universidad donde estudió (`fsutanom@dcc.uchile.cl`), que mantiene para intercambiar email con antiguos colegas con los que no quiere perder el contacto.

En el ejemplo ficticio anterior, la misma persona posee al menos dos identidades bien definidas. Una es profesional, y la otra personal. Ambas se utilizan para propósitos distintos, en lugares distintos, e involucran usualmente a grupos de personas distintas. Muchas personas manejan sus identidades de forma separada, y no envían (por ejemplo) emails personales desde su cuenta personal, ni viceversa.

6.1.2 ¿Qué es una identidad digital personal?

Una *identidad digital personal* (o "cuenta digital") es la representación única de una persona[3] que realiza una transacción en línea [9, p.15]. Una identidad digital personal puede estar o no asociada a una organización. Por ejemplo, cada uno de nosotros tiene al menos una identidad relacionada con el trabajo que realiza y otra personal (como en el ejemplo en la sección anterior). Con la identidad de trabajo nos comunicamos con nuestros colegas, hacemos solicitudes, compramos cosas, enviamos y recibimos documentos, realizamos revisiones, etc. Con nuestra identidad personal nos comunicamos con nuestros amigos, pagamos cuentas, enviamos y recibimos fotos y videos personales a través de redes sociales, organizamos cumpleaños familiares, etc.

Una identidad digital personal está siempre asociada a un y sólo un *identificador*. Un *identificador* es una palabra o texto corto, usualmente sin espacios, que identifica de manera única a una persona dentro de un contexto determinado. Por ejemplo, la dirección de correo electrónico `fulano.sutano@gmail.com` puede ser utilizada para identificar a una única persona de entre todos los usuarios del servicio de correo electrónico provisto por Gmail.

Un identificador puede o no ser anónimo. Por ejemplo, el identificador `fulano.sutano@gmail.com` sugiere la existencia de una persona real, mientras que `r9823799423@gmail.com` no lo sugiere. El que un identificador sea o no anónimo depende de si existe o no una forma de vincular, a través de datos públicos, un identificador con una persona específica.

El proceso mediante el cual una persona prueba o confirma que posee control de un identificador se llama autenticación. Por ejemplo, para abrir una cuenta de correo electrónico una persona tiene que

[3] En rigor una identidad puede estar asociada a cualquier entidad (un servicio público, un cargo político, un club de fútbol, etc.) u objeto (un documento, una aplicación, etc.). En este documento desarrollamos sólo el concepto de identidad personal, es decir, asociada a personas.

escoger un identificador (p.ej., `fulano.sutano@gmail.com`). El identificador tiene que ser único en el contexto de los usuarios del mismo servicio de correo. Si alguien más (por un alcance de nombre) ya posee esa cuenta de correo, no podremos escoger exactamente el mismo identificador. Una vez que una persona ha creado una cuenta de correo electrónico, es necesario que cree una clave o *password* que le permita autenticarse frente al servicio de correo electrónico. Así, cada vez que la persona ingresa a su correo electrónico, el servicio de correo le pide que ingrese su identificador (para saber quién es) y su *password* (para probar que la persona es efectivamente quien dice ser). Para lograr lo anterior, es imprescindible para la persona mantener de forma secreta el password asociado al identificador.

6.1.3 Protegiendo tus datos personales

Cada persona tiene una vida privada que generalmente desea mantener de esa forma. Existe mucha información que por lo general no deseamos hacer pública; y eso es perfectamente legítimo. Lamentablemente, hoy es más fácil que nunca antes para personas e instituciones que desean conocer nuestra vida privada el "minar" información sobre nosotros: cada vez que hacemos click sobre un link, o colocamos *"Me gusta"* en un artículo, o publicamos un post en Facebook, o hacemos las compras de la semana en el supermercado, estamos entregando información a empresas y organizaciones con la que pueden crear un "perfil" de cada persona. Hoy existen algoritmos que permiten a empresas como Facebook, por ejemplo, comparar el perfil de una persona con el de millones de otras personas, y deducir cosas muy privadas, como la orientación sexual de la persona[10].

Aun más, existen empresas digitales que se dedican a rastrear masivamente y de forma automática a las personas cuando navegan a través de Internet, y a entender sus hábitos de navegación y de compra en línea. Muchas de las organizaciones que se dedican a construir perfiles personales digitales se encuentran fuera de Chile, lo que hace en la práctica imposible el poder entablar una demanda contra ellas en el caso hipotético (aunque poco probable) de que pasaran a llevar nuestros derechos respecto de nuestra vida privada.

Existen algunas recomendaciones generales para proteger la información que viaja a través del navegador, tanto si navegamos en sitios chilenos como extranjeros, que entregaremos más adelante. Sin embargo, hay recomendaciones en el ámbito de sitios y organizaciones chilenas que toda persona debería conocer.

Tanto en el sector privado como en el público rige en Chile la Ley 19.628 de protección de la vida privada [6]. En algunos casos específicos, algunos organismos públicos están autorizados por ley a preguntar algunos datos privados (por ejemplo, a través del censo nacional realizado por el Instituto Nacional de Estadísticas cada 10 años). Sin embargo, en la inmensa mayoría de los casos, para que una empresa o servicio público recolecte los datos privados de personas debe pedir autorización expresa (es decir, por escrito) a cada persona. Antes de obtener autorización, la empresa o servicio público debe:

1. Informar claramente del propósito de la recolección de datos,
2. Informar si esos datos serán comunicados a otras personas u organizaciones[4].

Las organizaciones están obligadas a usar la información que recolecten sólo para el propósito para el que la recolectaron[5]. Existen dos casos especiales:

1. **Información sensible**: Las organizaciones no pueden recolectar datos sensibles (apariencia

[4]Ley 19.628, Art. 4, párrafos 1 y 2: "El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello. La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público."

[5]Ley 19.628, Art. 9: "Los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público."

física, tipo racial, opiniones políticas, creencias religiosas, estado de salud, vida sexual, etc.)[6]. La excepción es cuando esto es necesario para determinar u obtener algún beneficio de salud (por ejemplo, el Ministerio de Desarrollo Social obtiene y guarda información sobre la condición de discapacidad para poder otorgar algunos subsidios o bonos a personas).

2. **Información pública**: Las organizaciones pueden recolectar sin autorización expresa aquellos datos personales sobre información comercial o financiera que ya sea pública; independientemente de si es (por ejemplo) de naturaleza financiera, o de si son sobre nuestra profesión, dirección, educación, u otros.

Adicionalmente, según la Ley 19.880 de Procedimiento Administrativo [5], todas las personas, en su relación con las instituciones públicas, tienen derecho a no presentar documentos "que ya se encuentren en poder de la administración pública"[7].

6.1.4 Protegiendo tus dispositivos

Durante los últimos años se ha acentuado la tendencia a considerar los dispositivos (computadores, teléfonos, tablets, etc.) como de uso personal. En general, compartimos nuestro teléfono sólo a nuestras personas más cercanas (hijos, parejas), y sólo por espacios controlados. Una excepción a esto se da en el hogar, donde las personas que viven bajo el mismo techo comparten el uso de dispositivos como televisores o tablets.

A pesar de lo anterior, en general solemos tener menos cuidado del que deberíamos con nuestros dispositivos. En 2014, una encuesta realizada en Estados Unidos por Consumer Reports reportaba que el 34 % de los usuarios de smartphones no utilizaba ningún método para bloquear su teléfono, y el 36 % utilizaba un número de cuatro dígitos (la forma más básica de bloquear el teléfono) [22]. Esto incluso a sabiendas de que los teléfonos almacenan una enorme cantidad de información sobre cada persona: correo electrónico, fotos, redes sociales, etc.

Algunos de los problemas relativamente frecuentes hoy son el robo y pérdida de teléfonos, que las personas que están físicamente muy cerca nuestro (por ejemplo, en el transporte público) husmeen lo que estamos escribiendo o conversando con otras personas a través del teléfono, y que las aplicaciones que tenemos instaladas en nuestro teléfono espíen lo que estamos haciendo.

Con respecto a los computadores personales no portátiles (tanto en la oficina como en el hogar), a pesar de que el robo y la pérdida pueden constituir un problema, éste es mucho menos frecuente que con los teléfonos móviles. En cambio, el que una persona se siente frente a un computador ajeno sin la autorización ni conocimiento del dueño mientras éste está ausente es un problema potencialmente más grave (y posiblemente más frecuente).

6.1.5 Permisos de aplicaciones en tu teléfono

Los smartphones hoy son pequeños computadores con una cámara (algunos tienen más de una) y un sinnúmero de sensores. Esto, junto a la enorme variedad de aplicaciones que hacen uso de la información que proviene de estos sensores, nos permite realizar una serie de tareas que hace dos décadas parecían impensables (como tener un GPS de bolsillo). Sin embargo, estas mismas capacidades permiten a los desarrolladores de las aplicaciones tener acceso a exactamente la misma información de nosotros que obtenemos a través de las aplicaciones en nuestros teléfonos.

[6] Ley 19.628, Art. 10: "No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares."

[7] Ley 19.880, Art. 17, letra c): "Las personas, en su relación con la Administración, tienen derecho a: c) Eximirse de presentar documentos que no correspondan al procedimiento, o que ya se encuentren en poder de la Administración."

Por ejemplo, en julio de 2016, algunos usuarios notaron que cuando instalaban el juego Pokemon GO en sus iPhones, y creaban una cuenta para el juego a partir de una cuenta Google, la aplicación solicitaba acceso completo a la cuenta en Google; este acceso significaba que podían (entre otras cosas) leer y enviar correo en Gmail y obtener en todo momento la posición del usuario marcada en Google Maps[8]. Niantic Labs (los creadores de Pokemon GO) publicaron una declaración diciendo que "sólo utilizaban información básica del perfil" del usuario, y que corregirían el problema[9].

Muy pocos usuarios revisan los permisos en las aplicaciones que instalan. Un estudio en 2012 encontró que sólo el 17 % de los usuarios de Android prestaban atención a los permisos durante la instalación, y sólo 3 % del total comprendía los permisos [7]. Precisamente por la misma razón, Google y Apple restringen la forma en que las aplicaciones en nuestros teléfonos tienen acceso a nuestra información.

En Android, cada vez que se instala una aplicación el sistema operativo muestra la lista completa de permisos a los que la aplicación tendrá acceso una vez que esté instalada; las únicas dos opciones para el usuario son aceptar que la aplicación utilice todo lo que solicita, o no permitirlo (y por tanto no instalar la aplicación).

En iPhone, en cambio, cada vez que una aplicación requiere acceso a un sensor (la cámara, por ejemplo), el sistema operativo muestra un mensaje preguntando al usuario si desea permitirlo. Si no lo permite, no obtendrá alguna funcionalidad de la aplicación, pero no está obligado/a a desinstalar la aplicación si no lo desea así.

6.1.6 Protegiendo tu navegación

Hoy existen aplicaciones que permiten proteger nuestra navegación en Internet de empresas "rastreadoras" (trackers) que construyen perfiles de cada persona a partir de su navegación por Internet. Estas aplicaciones se instalan sobre el navegador en el computador o teléfono personal, e impiden a trackers obtener información de los sitios que se visitan.

La mayor parte de estas aplicaciones funcionan basadas en "listas blancas" (whitelists) y/o listas negras ("blacklists"). Una blacklist es una lista de rastreadores o anunciantes que tienen antecedentes de espiar a las personas mientras navegan. Cada vez que se visita un sitio web a través de tu navegador en el que se ha instalado una aplicación basada en una blacklist, la aplicación chequea el sitio web y bloquea todas aquellas partes del sitio que provienen de rastreadores, para evitar que estas organizaciones se enteren de qué sitios la persona está visitando. Una whitelist funciona al revés: cuando una persona visita un sitio web, éste es usualmente bloqueado excepto si está explícitamente dentro de la whitelist. Por tanto, el segundo método es más restrictivo que el primero.

6.1.7 Repositorios oficiales de aplicaciones

Hoy, Google y Apple (las compañías que están detrás de Android y iPhone, respectivamente) operan repositorios oficiales (*App Stores*) desde donde los usuarios de teléfonos inteligentes pueden bajar e instalar aplicaciones para sus teléfonos (*Google Play* y *iTunes*, respectivamente). Como ambas compañías decidieron en algún momento abrir el desarrollo de aplicaciones para sus teléfonos a desarrolladores independientes, *Google* y *Apple* (e incluso algunos fabricantes de teléfonos, como *Samsung*) se preocupan de revisar para sus clientes todas las aplicaciones antes de que éstas sean puestas a disposición del público. Ninguna aplicación puede ser publicada si no es autorizada antes

[8] Ver `https://www.theverge.com/2016/7/11/12150468/pokemon-go-privacy-full-account-access-permission`. Consultado el 8/sept/2017.

[9] Ver `https://www.theverge.com/2016/7/11/12156990/pokemon-go-security-flaw-google-account-fix`. Consultado el 8/sept/2017.

por la compañía correspondiente. Este proceso, sin embargo, no garantiza que las aplicaciones que encontramos en las *App Stores* sean seguras: sólo disminuye la probabilidad de que las aplicaciones que instalamos contengan malware.

Por ejemplo, en junio de 2017 la empresa TrendMicro reportó[10] una librería de anuncios (*Ads*) maliciosa llamada *Xavier*, que es utilizada por muchas aplicaciones en el repositorio oficial de Android que obtienen ingresos mostrando avisos comerciales a sus usuarios.

Aun así, la cantidad de teléfonos afectados por malware es muy pequeña. En marzo de 2017 *Google* reportó que la proporción de teléfonos *Android* con malware es de 0.71 % para los usuarios que bajan aplicaciones desde fuera del repositorio oficial, y de 0.05 % para los usuarios que sólo bajan aplicaciones desde el repositorio oficial [15, p.4]. Considerando que Apple es aún más restrictivo que Google con sus aplicaciones, es probable que estas cifras sean aún menores para la plataforma iPhone.

Para que una aplicación pueda provocar real daño en un teléfono, tiene que tener acceso al usuario con más privilegios en el sistema operativo. Para esto no sólo hay que instalar aplicaciones que no estén en los repositorios oficiales, sino también hay que intervenir el teléfono a través de un proceso conocido como *jailbreaking* en los iPhones, y *rooting* en los Android. Ambos procesos requieren instalar software específico en el teléfono para ejecutar programas a través del usuario administrador del sistema operativo. **Este proceso no se puede realizar por casualidad**: se requiere de una serie de pasos que deben ser ejecutados por una persona con conocimiento técnico, y que es imposible que ocurran durante la operación normal de un teléfono.

6.2 Higiene digital personal

6.2.1 Recomendaciones básicas

Recomendación 1: Nunca ingreses información en una página sin estar seguro de quién la está pidiendo.
Antes de ingresar información privada en un sitio web, siempre debes comprobar la dirección del sitio web en la barra superior de tu navegador. El nombre del sitio web que estás visitando es el que se encuentra entre el `http://` o `https://` y la siguiente barra diagonal ("/"). Por ejemplo, en la dirección `http://malware.com/www.buensitio.com/`, el nombre del sitio web es `malware.com`, no `www.buensitio.com`. ¡Nunca ingreses información privada (incluidos tus passwords) sin haber confirmado que el sitio que estás viendo concuerda con el nombre del sitio en la barra del navegador!

Recomendación 2: Nunca ingreses tus datos en un sitio que no sea seguro.
Cuando visitas una página web, la información viaja físicamente desde el computador de la institución dueña o controladora del sitio web hasta tu computador. Si la comunicación no es cifrada, entonces en teoría cualquier persona puede observar la información que recibes y la que envías desde tu computador. Antes de ingresar tus datos en un sitio web, confirma que la comunicación sea segura asegurándote de que la dirección en la barra del navegador comience con `https` y no con `http`.

[10] Ver `http://blog.trendmicro.com/trendlabs-security-intelligence/analyzing-xavier-information-stealing-ad-library-android/`. Consultado el 7/sept/2017.

Recomendación 3: Mantén tus identidades digitales personales separadas unas de otras.
No realices actividades que son propias de una identidad a través de otra identidad (como enviar un correo electrónico personal a través de un correo electrónico institucional).

Lo anterior significa no utilizar usernames ni passwords de una identidad para propósitos o actividades que son propios de otra identidad. Por ejemplo, Fulano no debería utilizar un email personal (p.ej., `fulano.sutano@gmail.com`) para recibir información relacionada con su trabajo; ni debería utilizar su email institucional (`fsutano@ssdefensa.gob.cl`) para abrir una cuenta en Instagram (o en Tinder, o en sitios de apuestas, o en casas comerciales, etc.) Fulano tampoco debería usar el mismo password que utiliza para su correo personal en su correo institucional.

La razón de esta recomendación es tanto legal como técnica y práctica.

En instituciones que manejan información que requiere de altos niveles de confidencialidad (como lo es la Subsecretaría de Defensa), es frecuente que lo anterior esté explícitamente prohibido. Al utilizar su dirección de correo institucional para abrir una cuenta en Facebook, Fulano estaría transgrediendo las normas de la institución donde trabaja, y se expone por tanto a las sanciones que la institución haya fijado.

Existe una razón más técnica y práctica. Una práctica relativamente frecuente de delincuentes digitales es robar el identificador de una persona y el password correspondiente. Una vez hecho esto, el delincuente prueba ese password en todas las cuentas que la víctima pueda tener. Si la víctima utiliza el mismo password en varios servicios distintos, corre el riesgo de que varias de sus cuentas sean hackeadas al mismo tiempo, aumentando el riesgo que esto tiene para la persona afectada (y sus familiares, amigos, etc.) Algunas de las motivaciones más frecuentes del delincuente para hacer esto son el robo, el engaño tanto a la persona como a sus contactos, y la instalación de malware en su computador.

Recomendación 4: Utiliza doble factor de autenticación en todas aquellas cuentas que te lo ofrezcan.
Utiliza doble factor de autenticación en todas las cuentas que ofrezcan el servicio. Esto disminuye la probabilidad de que un delincuente pueda tener acceso a una cuenta protegida de esta forma.

Una de las mejores formas de cuidar nuestra identidad es a través de un mecanismo llamado **autenticación de doble factor** o **doble autenticación**.

Todas las formas de acceso a un sistema o a un recurso digital se basan en tres tipos de factores:

1. Lo que una persona *sabe* (por ejemplo, un password, una dirección física, una fecha de cumpleaños, el nombre de una mascota, etc.),
2. Lo que una persona *tiene* (por ejemplo, una tarjeta de crédito, una tarjeta contact-less, un aparato OTP[11], etc.),
3. Lo que una persona *es* (por ejemplo, la huella digital, el iris del ojo, etc.).

[11] Un OTP, o *One Time Password*, es un aparato portátil que, al presionar un botón, genera un número "aleatorio" que puede ser ingresado en un sistema para obtener acceso a éste.

De los factores anteriores, el más utilizado es el primero; sin embargo, algunos sistemas utilizan dos de los factores anteriores para incrementar el nivel de seguridad en el acceso a un sistema. Esto, en la práctica, significa que para ingresar a un sistema se solicita no sólo una clave (lo que la persona *sabe*), sino también su huella digital (lo que la persona *es*) o alternativamente una clave enviada al teléfono (que correspondería al segundo factor: lo que la persona *tiene*). Por ejemplo, supongamos que una persona desea conectarse a un sitio web que implementa este último mecanismo de doble factor. Esto podría funcionar de la siguiente forma:

1. Cuando la persona se conecta al sitio web de un servicio en línea (por ejemplo, su correo electrónico) por primera vez, el sistema le pide que ingrese su username y su password.
2. Si el password es correcto, entonces el sistema envía a la persona un mensaje de texto (SMS) a su teléfono con un código o clave numérica.
3. Una vez que el mensaje llega al teléfono, la persona ingresa el código en el sitio web.
4. Si el código es correcto, el sistema da acceso al servicio (p. ej., correo electrónico).

El sistema anterior es más seguro que la forma tradicional de autenticarse, pues depende no sólo de que la persona sepa su username y password, sino también de que posea su teléfono para poder recibir el código numérico correspondiente. Posee también la desventaja de que, para poder ingresar a un servicio, la persona necesita tener su teléfono consigo en el momento en que esté ingresando al sistema. En general es poco probable que un atacante pueda tener acceso al teléfono de una persona y averigüe el password de la persona al mismo tiempo (¡y tenga tiempo para obtener acceso a una cuenta asociada a ambas cosas antes de que la persona pueda bloquear una de los dos!).

La tabla 6.1 (pág. 37) muestra una selección de servicios y redes sociales que ofrecen doble autenticación a la fecha de este documento.

Lamentablemente, en Chile muy pocos servicios en línea (banca, retail, gobierno, etc.) cuentan a la fecha de este documento con autenticación de doble factor. En este caso, es necesario compensar la falta de seguridad poniendo énfasis en el resto de las medidas contenidas en este documento.

Recomendación 5: Usa passwords distintos para cada identidad digital.
Escoge un password distinto para cada cuenta digital personal.

El password es hoy el mecanismo más utilizado para acceder a servicios de acceso restringido. A pesar de que ha habido muchas propuestas alternativas, es muy poco probable que los passwords lleguen a ser reemplazados en el futuro cercano [2].

Un buen password es aquel que es fácil de recordar para la persona que lo creó, y difícil de adivinar o averiguar para cualquier otra persona. Lamentablemente, esto es difícil de hacer porque los passwords más seguros son cadenas de caracteres escogidos aleatoriamente, y éstos son muy difíciles de recordar. Incluso cuando los escribimos, estos passwords son tan difíciles de ingresar en un teclado o la pantalla de un teléfono inteligente, que usualmente terminamos renunciando a passwords seguros y usamos passwords que en vez de eso son fáciles de recordar y de ingresar en cualquier parte (como “123456”).

Según un estudio del año 2007, las personas tenemos en promedio 25 cuentas o sitios que requieren de un password, y tenemos en promedio 6.5 passwords distintos [8]. Esto significa que, en promedio, reusamos el mismo password en alrededor de 4 sitios. Esto es problemático porque si un atacante obtiene acceso al username y password de una persona, y la persona usa el mismo password en otras cuentas de la persona, el atacante podría tener acceso a esas cuentas sin necesidad de “robar” otros passwords.

Nombre servicio	Tipo servicio	URL	Observaciones
Banco de Chile	Banca en línea	https://portalpersonas.bancochile.cl/persona	Disponible vía token por software y token por hardware.
BancoEstado	Banca en línea	https://www.bancoestado.cl/imagenes/comun2008/nuevo_paglg_pers2.html	La clave de ingreso a cuenta personal está compuesta por 4 dígitos; disponible por token no digital (tarjeta impresa de códigos).
Dropbox	Almacenamiento de documentos	https://www.dropbox.com/	Disponible a través de SMS, token por software y token por hardware.
Facebook	Red social	https://facebook.com/	Disponible vía SMS con restricciones (máximo un teléfono por cuenta).
Gmail	Correo electrónico vía web	https://gmail.com/	Disponible vía SMS, llamada telefónica, token por software y token por hardware.
Google Drive	Almacenamiento y edición de documentos	https://drive.google.com/	Disponible a través de SMS, llamada telefónica, token por software y token por hardware.
Instagram	Red social	https://www.instagram.com/	Disponible vía SMS.
LastPass	Administrador de passwords	https://lastpass.com/	Disponible vía token por software y token por hardware.
LinkedIn	Red social	https://linkedin.com/	Disponible vía SMS.
Outlook.com	Correo electrónico vía web	https://outlook.live.com/owa/	Disponible vía SMS y token por software.
Slack	Comunicación y trabajo en equipo	https://slack.com/	Disponible vía SMS y token por software.
Skype	Comunicación vía video	https://www.skype.com/en/	Disponible vía SMS y token por software sólo a través de una cuenta Microsoft. No disponible para cuentas Skype originales.
Telegram	Comunicación vía mensajes	https://telegram.org/	Disponible vía SMS y llamada telefónica.
Twitter	Red social	https://twitter.com/	Disponible vía SMS con restricciones (sólo algunos proveedores, máximo 10 cuentas por número de teléfono, máximo un número telefónico por cuenta).
WhatsApp	Comunicación vía mensajes, audio y video	https://www.whatsapp.com/	Disponible vía SMS y llamada telefónica.
Yahoo Mail	Correo electrónico vía web	https://mail.yahoo.com	Disponible vía SMS.
Zoho Mail	Correo electrónico vía web	https://www.zoho.com/mail/	Disponible vía SMS y token por software.

Tabla 6.1: Selección de servicios en línea que ofrecen doble autenticación. Adaptado de https://twofactorauth.org/. Consultado el 2/mayo/2017.

Es posible, a través de técnicas como las descritas en la "Guía de Uso de Passwords" (pág. 45), tener un password distinto para cada identidad digital que uno posee. Como cada persona posee necesidades distintas respecto de sus identidades, la recomendación es leer y utilizar las técnicas descritas en esa guía para tener passwords separados por cada identidad.

Recomendación 6: Usa passwords largos y difíciles de adivinar por otras personas.
Usa un password largo y difícil de adivinar para cada cuenta digital personal. Si no puedes tener un password distinto y largo para cada cuenta, entonces escoge passwords largos y difíciles de adivinar por lo menos para las cuentas más críticas (por ejemplo, la cuenta del banco).

En general, los passwords más largos son más seguros para la mayor parte de los propósitos cotidianos. El qué tan largo debe ser un password depende de para qué se utilizará, y de la técnica que se utilice para generarlo. Por ejemplo, si se desea tener passwords de largo arbitrario compuestos por combinaciones aleatorias de caracteres se puede utilizar un Administrador de Passwords. Si se desea crear passwords seguros que a la vez sea relativamente sencillo memorizar, se puede utilizar la técnica "diceware", junto con el "método de loci". Ambos recursos, y otros adicionales, son descritos en detalle en la "Guía de Uso de Password" (pág. 45).

Recomendación 7: Cambia tu password sólo si sospechas que fue hackeado.
No cambies tu password con frecuencia. Si tu organización te obliga a cambiar tu password con frecuencia, pide ayuda a la unidad informática o grupo de soporte informático para instalar una herramienta de apoyo para passwords como las descritas en la "Guía de Uso de Passwords" (pág. 45).

Al contrario de la recomendación que usualmente se hace, cambiar el password obligadamente con cierta frecuencia (p.ej., cada 3 meses) nos lleva a utilizar variaciones predecibles de nuestro password, y esto nos lleva a tener passwords menos seguros [4], [23]. Por ejemplo, una estrategia que frecuentemente usamos es agregar un signo de exclamación al final, creyendo que con eso hacemos nuestro password más seguro [23]; es, por tanto, una combinación común que puede intentar un atacante queriendo adivinar nuestro password.

Por tanto, a menos que la política de tu organización te obligue a hacerlo, no cambies tu password con frecuencia. Es mejor cambiarlo sólo si sospechas que pudo haber sido hackeado (en ese caso, cámbialo urgentemente).

6.2.2 Recomendaciones avanzadas

Recomendación 8: Entrega sólo aquella información que sea estrictamente necesaria.
Muchas veces, al crear una cuenta, al solicitar un servicio o al intentar dejar un reclamo, las organizaciones nos solicitan más datos de lo estrictamente necesario. Por ejemplo, para comprar un producto en línea una empresa podría solicitarte crear una cuenta en su

sitio web. Excepto en el caso en que la empresa deba despachar el producto que estás comprando a tu casa o a tu trabajo, usualmente la empresa no necesita ni tiene porqué conocer tu dirección particular. En caso de que te exijan conocer información privada para poder brindarte un servicio o venderte un producto, simplemente busca una tienda o proveedor alternativo.

6.3 Higiene con dispositivos digitales

6.3.1 Recomendaciones básicas

Recomendación 9: Bloquea el acceso a tu computador siempre que te ausentes por más de unos segundos.
Bloquea manualmente el acceso a tu computador cada vez que te ausentes de tu puesto de trabajo por más de unos segundos (por ejemplo, para almorzar o para asistir a una reunión); esto se realiza a través de una combinación de teclas especial que depende del sistema operativo o tipo de computador. Adicionalmente, configura tu computador para que se bloquee automáticamente si no hay actividad por más un par de minutos.

En los computadores con Microsoft Windows, se puede bloquear el computador presionando las teclas "Windows" y "L" (de "lock"); para desbloquear se utiliza la combinación CONTROL + ALT + SUPRIMIR, y luego se ingresa el password del usuario que bloqueó el computador. En los computadores con iOS (Mac) o Linux (Ubuntu, RedHat, Mint, etc.) existen mecanismos similares para bloquear el computador. En todos los casos, para desbloquear es necesario ingresar el password del usuario que bloqueó el equipo.

Esto es especialmente recomendable en el lugar de trabajo, donde otras personas pueden sentarse y tener acceso al computador propio (no sólo colegas de trabajo sino también personas que no pertenecen a la institución).

Recomendación 10: Mantén tu computador actualizado de manera automática.
Configura tu computador para que instale automáticamente las actualizaciones de seguridad del fabricante apenas estén disponibles.

Tanto en Microsoft Windows como en MacOS y Linux existen formas de configurar el sistema operativo para que revise automáticamente si existen actualizaciones de seguridad, y para que las instale de manera automática. La recomendación para usuarios no expertos es configurar el computador para que instale automáticamente las actualizaciones de seguridad que aparezcan. En ambientes laborales, esta tarea usualmente es responsabilidad del área de soporte informático.

En caso de los usuarios expertos, es posible que la instalación automática sea una molestia (por ejemplo, porque interfiere con tus labores habituales). En ese caso, cada usuario debe compatibilizar las labores habituales con el hábito de revisar con periodicidad si existen actualizaciones, e instalarlas cuando existan. Como generar hábitos es difícil, la sugerencia siempre es configurar este proceso para que se ejecute de manera automática.

Recomendación 11: Si tienes un computador con Microsoft Windows, instala un antivirus y mantenlo actualizado.
Instala un antivirus en tu computador con Microsoft Windows, y mantenlo actualizado. En un ambiente laboral, esta tarea es realizada por el área informática. En caso de que no sea así, pide una recomendación sobre qué antivirus instalar.

Esta es una de las recomendaciones más conocidas por el común de las personas, y (probablemente por la misma razón) una de las más desoídas. Hoy en día es absolutamente necesario instalar y mantener actualizado un antivirus en un computador con Microsoft Windows. Tener un antivirus instalado y no actualizado es en la práctica similar a no tenerlo: además de la rapidez con que aparecen nuevos virus, entrega una falsa sensación de protección.

A diferencia de Microsoft Windows, iOS y Linux son sistemas operativos donde, a pesar de que existe malware, éste opera de forma sustancialmente distinta del malware en Windows. Por esta forma distinta de operar, en estos sistemas no es estrictamente necesario mantener un antivirus siempre y cuando el sistema se mantenga permanentemente actualizado, según las indicaciones del fabricante o mantenedor del sistema operativo.

Recomendación 12: Bloquea el acceso a tu teléfono.
Configura tu teléfono para que cada vez que la pantalla se apague debas ingresar un *pin* (un número de por lo menos cuatro dígitos) o un patrón de puntos para poder reingresar al teléfono.

Todos los laptops, tablets, y smartphones modernos ofrecen opciones para bloquearlos y evitar que otras personas tengan acceso a nuestros aparatos. En los teléfonos iPhones, es obligatorio utilizar un mecanismo de bloqueo (el mecanismo por defecto es una clave de cuatro dígitos). En teléfonos Android no existe un mecanismo de bloqueo por defecto; sin embargo, se puede escoger entre un número de 4 o más dígitos, un password, un patrón de puntos, u otros.

A diferencia de los computadores, donde el proceso para bloquear y desbloquear el computador es siempre el mismo, para los smartphones existe una variedad de métodos. Esto se debe a que en los teléfonos el proceso de escribir o tipear una palabra o password es cualitativamente distinto porque el teclado es visual, y se presenta a través de una pantalla muy pequeña: tipear una palabra o un password toma más tiempo y se cometen más errores en comparación con un teclado "físico" [14]. Existen diferencias también en los teclados en distintas plataformas; en general, el teclado de los iPhones permite escribir más rápido y con menos errores que los teclados en otras plataformas [17].

A raíz de lo anterior, se ha desarrollado una enorme variedad de métodos visuales para desbloquear un teléfono, basados en (por ejemplo) el reconocimiento de imágenes o en unir puntos en la pantalla en un orden determinado [18]. Ningún método posee ventajas o desventajas muy grandes sobre el resto [17], [18]; lo importante es utilizar algún método para disminuir la posibilidad de que otros accedan a nuestro teléfono y a toda la información que almacenamos allí.

Recomendación 13: Mantén tu teléfono actualizado.
Configura tu teléfono para que instale automáticamente las actualizaciones de seguridad del fabricante apenas estén disponibles.

Mientras menos tiempo pase entre la publicación de actualizaciones de seguridad, y su instalación en tu teléfono, menos probable es sufrir ataques dirigidos a explotar posibles vulnerabilidades.

Mantener el computador, el teléfono y en general los dispositivos digitales que uno posee al día con las últimas actualizaciones de seguridad es una de las medidas más importantes para protegerse de las infecciones por malware.

6.3.2 Recomendaciones avanzadas

Recomendación 14: Antes de instalar una aplicación en tu teléfono, revisa los permisos que requiere y sus comentarios negativos (si los hay).
Cada vez que instales una aplicación en tu teléfono Android, revisa los permisos que requiere y los comentarios negativos de los usuarios de la aplicación. Si existen comentarios serios en contra de la aplicación, busca otra aplicación que satisfaga tu necesidad.

Si los permisos de una aplicación no coinciden con el propósito de la aplicación, no instales la aplicación y busca una alternativa. Por ejemplo, que una aplicación de fotos solicite acceso a la cámara parecería razonable a la mayor parte de las personas; en cambio, que una aplicación de linterna solicite acceso a tu ubicación fina a través de GPS probablemente no es razonable.

Cuando muchos usuarios instalan y prueban una aplicación y quedan insatisfechos con ella, es usual que algunos usuarios escriban recomendaciones negativas sobre las aplicaciones para ayudar a otros usuarios. Al revés de las recomendaciones positivas (que pueden ser manipuladas), las recomendaciones negativas son frecuentemente honestas (aunque algunas veces pueden estar motivadas simplemente por frustración o rabia). En cualquier caso, antes de instalar una aplicación es muy útil revisar las recomendaciones negativas: si existen comentarios informados y serios advirtiendo sobre aspectos negativos de la aplicación, es mejor no instalarla.

6.4 Higiene en redes digitales

6.4.1 Recomendaciones básicas

Recomendación 15: No abras correo electrónico de personas o instituciones que no conoces.
Configura tu cuenta de correo para borrar automáticamente (o para mover a una carpeta de basura) los correos de personas que no conozcas.

El correo electrónico es (y seguirá siendo durante algún tiempo) una herramienta de comunicación importante dentro de las instituciones. Uno de los problemas más importantes con esta herramienta es que acciones como hacerse pasar por otra persona, enviar correos masivos con el propósito de engañar, o infectar computadores con malware (a través de archivos adjuntos), no requiere de mucho conocimiento.

En general es un muy buen hábito el no responder (y simplemente eliminar) los correos de personas o instituciones que no conocemos. ¿Cómo hacemos para recibir correos de personas que conocemos pero de las cuales no hemos recibido correo antes? Para eso, siempre deberíamos primero chequear físicamente con la persona su correo electrónico.

A veces es incluso posible ser engañado a través de las casillas de correo electrónico de nuestros amigos o parientes; frente a correos con peticiones inusuales lo mejor es siempre corroborar con la persona a través de una llamada telefónica o algún otro medio (distinto del correo electrónico). Por ejemplo, ¿cuán probable es que a nuestro mejor amigo, al que no vemos hace un par de meses, le hayan robado todo mientras paseaba por Ucrania, que haya perdido su pasaporte y su dinero, y necesite que le prestes $2.100 euros para pagar la cuenta del hotel? La respuesta es: depende de si es o no razonable que la persona en cuestión esté viajando por Ucrania. Este es un engaño tradicional a través de correo electrónico[12], y lo más probable es que algún hacker haya tomado el control de la cuenta de correo electrónico de nuestro amigo, y esté enviando correos pidiendo dinero a toda la lista de contactos de nuestro amigo. En cualquier caso, lo mejor que uno puede hacer es sencillamente llamar a la persona por teléfono, o ubicarla de alguna otra forma para confirmar la veracidad del problema.

Recomendación 16: Antes de conectarte a una red inalámbrica, confirma con alguna persona que pertenezca a la institución cuál es el nombre de la red.
Si estás en un ambiente laboral, pregunta al área informática cuál es el nombre de la red y su password. Si estás en un negocio o restaurant, pregunta a algún empleado del local por el nombre de la red. Si estás en casa de amigos o parientes, pregúntales por el nombre de la red que ellos poseen. Si estás en una red pública, consulta alguna fuente o aviso oficial que confirme cuál es el nombre de la red a la que deseas conectarte.

Cuando te conectas a una red inalámbrica (*Wifi*), todo tu tráfico pasa a través de un pequeño computador especializado conocido como router. Este computador, además de conectarte a Internet (técnicamente, a un proveedor de servicios de Internet o ISP, como Claro, Entel, WOM, etc.), es responsable principalmente de mostrarte los sitios correctos (por ejemplo, de mostrarte el verdadero `www.facebook.com` cuando quieres visitar tu cuenta de Facebook). Este computador está siempre bajo control de alguien; y esa persona, empresa o institución pública puede decidir (si así lo desea) restringir tu navegación de casi cualquier forma imaginable:

1. Puede mostrarte otros sitios en vez de los que tú quieres visitar,
2. Puede decidir mostrarte avisos comerciales antes de llevarte al sitio que quieres visitar,
3. Puede silenciosamente censurar ciertos sitios para que no los visites, o facilitar la visita a ciertos sitios específicos,
4. Puede espiar tu tráfico y mostrarte cosas basado en ese tráfico,
5. Etc.

6.4.2 Recomendaciones avanzadas

Recomendación 17: Borra las conexiones a redes inalámbricas públicas luego de haberlas utilizado.
Luego de haberte conectado a una red inalámbrica pública (en restaurants, tiendas de retail, bares, etc.), borra la conexión de la lista de conexiones guardadas.

[12] Ver, por ejemplo, `https://www.theguardian.com/money/2013/nov/13/stranded-traveller-phishing-scam`. Consultado el 8/sept/2017.

La mayor parte de los computadores y teléfonos están configurados para recordar las conexiones inalámbricas a las que nos hemos conectado, y para conectarse automáticamente a ellas cuando la red es detectada (esto es, sin necesidad de volver a ingresar un password, y sin siquiera avisarnos de ello). Esto puede ser utilizado por un atacante para crear una red inalámbrica con el mismo nombre y password de una red pública a la que alguna vez se estuvo conectada, y tome control de nuestra conexión a Internet. Para evitar esto, es mejor borrar las redes que uno no utiliza, o (mejor aún) configurar el computador y teléfono para no conectarse automáticamente a las redes que conoce.

Recomendación 18: Instala al menos una aplicación de bloqueo de rastreadores y anuncios en tu navegador.
Para impedir que los sitios web que visitas almacenen tus datos y los vendan a empresas "rastreadoras" para construir un perfil de tu persona, instala alguna aplicación para bloquear dicho seguimiento.

Algunas de las aplicaciones disponibles para múltiples navegadores son (en orden alfabético) AdBlock Plus, Disconnect, Ghostery, Privacy Badger y NoScript. Para ver detalles sobre estas aplicaciones, consulta la tabla 6.2 más abajo.

Aplicación	Desarrollada por	Navegadores/dispositivos compatibles
AdBlock Plus	Originalmente por Wladimir Palant en 2006, quienes crearon Eyeo (`https://eyeo.com/`, USA) para sustentar el desarrollo.	Android, Chrome, Firefox, Internet Explorer, Opera, Safari
Disconnect	Disconnect Mobile: `https://disconnect.me/`	Chrome, Firefox, Opera, Safari, Samsung browser
Ghostery	Originalmente por David Cancel para Ghostery, adquirida por Evidon Inc. (USA). Hoy propiedad de Cliqz (un emprendimiento en Alemania): `https://www.ghostery.com/`	Chrome, Edge, Firefox, Internet Explorer, Opera, Safari
Privacy Badger	Electronic Frontier Foundation: `https://www.eff.org/privacybadger`	Chrome, Firefox, Opera
NoScript	Giorgio Maone, quien creó InformAction (Italia) para sustentar el desarrollo.	Firefox (sólo browsers basados en Mozilla)

Tabla 6.2: Aplicaciones para bloqueo de rastreadores y anunciantes maliciosos.

Recomendación 19: No instales aplicaciones fuera de los repositorios oficiales.
Para los usuarios de iPhones es relativamente difícil instalar aplicaciones que no estén en *iTunes*. En Android es más sencillo[13]; precisamente por esa razón, la recomendación para los usuarios de Android es entonces no activar esta opción.

[13]Para activar la instalación de aplicaciones fuera del repositorio oficial en Android, es necesario ir a la configuración, luego escoger la opción "Sistema", luego la opción "Seguridad", y luego activar la opción "Fuentes desconocidas".

Recomendación 20: No intervengas tu teléfono si no eres un usuario técnico avanzado.
Esto es, no hagas *jailbreaking* de tu iPhone, o *rooting* de tu Android, a menos que conozcas el proceso y seas capaz de tomar las medidas de seguridad adicionales necesarias para protegerte.

7. Guía de creación de passwords

7.1 Introducción

7.1.1 ¿Qué es un buen password?

Una de las formas más utilizadas hoy para tener acceso a recursos restringidos dentro de una institución es el uso de claves o passwords. Un password siempre va acompañado de un nombre de usuario o *username*. Un *username* le permite a una persona identificarse de manera única, tal como lo haría (por ejemplo) a través de un RUN; mientras que un password le permite a la persona comprobar a otros que es quien dice ser, tal como lo haría (por ejemplo) a través de una firma manuscrita.

¿Qué constituye un "buen password"? Es aquel que es fácil de recordar para la persona que lo creó, y difícil de "adivinar" para cualquier otra persona. De manera similar, una buena "firma" es aquella que es sencilla de generar para la persona que la crea, y difícil de duplicar por cualquier otra persona.

Una investigación del año 2007 [8] estudió los passwords que más de medio millón de usuarios ingresaron en su navegador durante más de 3 meses. Los investigadores llegaron a los siguientes resultados:

- Una persona tipea 8 passwords en promedio al día;
- Una persona promedio tiene 6.5 passwords distintos, y 25 cuentas o sitios que requieren de un password; en consecuencia, en promedio las personas reutilizaron cada password entre 3.9 sitios distintos;
- La mayor parte de las personas en el estudio escogieron passwords que tenían sólo letras minúsculas (excepto en aquellos casos donde fueron obligados a escoger passwords con mayúsculas, signos y letras).

Es muy difícil para una persona promedio el pensar en 25 passwords distintos para aceder a cada uno de los recursos que lo requieren; por ejemplo, el computador en su oficina, su teléfono inteligente (smartphone), su tablet, el computador en su casa, el sitio web de su banco, los sitios web de las cuentas de su casa (electricidad, agua, luz, teléfono), y un largo etcétera. Por tanto, la mayor parte de

las personas inevitablemente pensamos en unos pocos passwords y los reutilizamos en varias cuentas.

Esto no sería un problema si escogiéramos passwords difíciles de adivinar por otros. Sin embargo, las personas somos notoriamente predecibles a la hora de escoger un password [12], [13], [16], [19]. Es por eso que necesitamos algo de ayuda para crear nuestros passwords.

Este capítulo contiene una serie de criterios para ayudar a una persona a escoger un mejor método para gestionar sus passwords. Es una guía, no una norma; fue hecha para ayudar especialmente a las personas que trabajan en la Administración Pública chilena. Sin embargo, debería ser útil también para cualquier persona que quiera proteger su información a través de buenos passwords.

7.1.2 Recomendaciones generales

En la Guía de Higiene Digital (pág. 29) se entregan dos recomendaciones relacionadas con el cuidado de los passwords personales:

1. Usa passwords distintos para cada identidad digital, y
2. Usa passwords largos y difíciles de adivinar por otros.

Para poder aplicar estas recomendaciones, en esta guía entregamos tres métodos. En general, cada persona debe utilizar el o los métodos que más se acomoden a su realidad. Algunos criterios que pueden ser de ayuda para escoger son los siguientes:

1. *Si tienes buena memoria, utiliza algún método que te permita recordar passwords distintos para cada una de tus cuentas*. Los mejores métodos (y los más difíciles) para gestionar los passwords personales son aquellos que aprendemos de memoria. En este documento, presentamos dos técnicas para crear un password seguro y fácil de recordar (diceware (pág. 47) e historias PAO (pág. 47)), y dos para memorizar passwords (repetición espaciada y el método de loci (ambos en la pág. 48)).
2. *Si no tienes tan buena memoria, utiliza un administrador de passwords*. A la mayor parte de las personas nos cuesta recordar muchos passwords distintos. En este documento recomendamos el uso de tres administradores de passwords: LastPass (pág. 49), Dashlane (pág. 50) y Keepass (pág. 51). Estos administradores almacenan de forma segura todos los passwords que uno desee, y requiere de un password maestro para tener acceso a ellos.
3. *Si eres mejor cuidando tus objetos personales, utiliza una tarjeta de passwords*. En general, las personas somos muy buenas cuidando nuestros objetos personales, como carteras, relojes o billeteras. Una tarjeta de passwords (pág. 52) es una tarjeta del tamaño de una tarjeta de crédito que uno lleva permanentemente consigo, y que, con ciertos resguardos, es muy útil para usar passwords distintos recordando un mínimo de información.

7.2 Método 1: Usa passphrases

7.2.1 ¿Qué es una passphrase?

Una passphrase es un password largo, típicamente compuesto de 15 caracteres o más de largo [20, p.1], y que se crea a partir de varias palabras separadas por espacios o signos de puntuación (por ejemplo, "CORRECTO.CABALLO,BATERÍA.COHETE"). Una passphrase tiene al menos dos ventajas por sobre los passwords tradicionales.

La primera ventaja es que, en términos generales, mientras más largo un password, más seguro es frente a un ataque conocido como de "fuerza bruta", donde el atacante prueba todas las combinaciones posibles de passwords basado en un alfabeto conocido (por ejemplo, letras minúsculas y mayúsculas del alfabeto español, además de números). Puedes ver una descripción detallada de en qué consiste un

ataque de fuerza bruta en la pág. 55. Esta ventaja también se da frente a los ataques de "diccionario". Un ataque de diccionario es uno en que el atacante no prueba todas las combinaciones posibles de caracteres, sino de palabras que podrían formar parte del password. La diferencia es sutil pero importante; describimos en qué consiste este ataque en la sección 7.5.2 (pág. 57).

La segunda ventaja es que las passphrases formadas por palabras son, en general, más fáciles de recordar [19]; una desventaja es que al ser más largas es más frecuente cometer errores al tipearlos en un teclado. Como normalmente uno no puede ver cuál es el error, esto nos obliga a borrar el password y tipearlo de nuevo por completo.

7.2.2 ¿Cómo usar una passphrase?

En primer lugar es necesario crear una buena passphrase; luego, es necesario memorizarla para poder recordarla cuando sea necesario. Para ambas cosas existen herramientas y recomendaciones.

Crear una passphrase: método *diceware*

Existen varias formas de crear una passphrase. Uno de los métodos más populares (y más seguros si se utiliza correctamente) fue creado en 1995 por Arnold Reinhold[1]. El método, llamado *diceware* (que no tiene una traducción precisa desde el inglés), consiste en escoger varias palabras siguiendo el siguiente procedimiento para cada palabra:

1. Tirar un dado de 6 caras 5 veces, y anotar el resultado de cada tirada en un papel.
2. Formar un solo número con los resultados de las tiradas. Por ejemplo, si las tiradas de dados fueron 4, 2, 3, 3 y 5, entonces el número resultante es 42335.
3. En una lista de palabras especialmente fabricada para ello, se busca la palabra que corresponde al número obtenido anteriormente.

El procedimiento anterior se repite tantas veces como palabras se desee generar. Típicamente, una passphrase con 4 o 5 palabras basta para la mayor parte de los usos cotidianos. Existen varias listas de palabras propuestas para este método, en varios idiomas distintos. En la lista en español[2], por ejemplo, la palabra correspondiente al número 42335 es "jaula". Existen también adaptaciones en línea de este método. Por ejemplo, en el sitio `rempe.us`[3] es posible generar passphrases de 5 o más palabras escogidas aleatoriamente.

Crear una passphrase: historias PAO

Un segundo método para crear una passphrase es el de las llamadas historias PAO (Persona-Acción-Objeto)[4]. Este método es similar al anterior; en vez de escoger una palabra tirando un dado varias veces, se escogen tres (o cuatro) palabras al azar:

1. Una persona: Por ejemplo, *Bill Gates*.
2. Una acción: Por ejemplo, *comer*.
3. Un objeto: Por ejemplo, *bicicleta*.
4. Un lugar: Por ejemplo, *la Plaza de la Constitución*.

La passphrase resulta de unir las palabras en el orden indicado arriba con los conectores adecuados: "*Bill Gates come una bicicleta en la Plaza de la Constitución*". El resultado es usualmente una historia

[1] `http://world.std.com/~reinhold/diceware_en_espanolA.htm`. Consultado el 20/abril/2017.

[2] La lista original en español está en `http://world.std.com/~reinhold/diceware_espanol/DW-Espanol-1.txt`. Consultado el 20/abril/2017.

[3] `https://www.rempe.us/diceware/#spanish`. Consultado el 21/abril/2017.

[4] Este método fue propuesto por Joshua Foer en 2011 en su libro "Moonwalking with Einstein" (`http://joshuafoer.com/moonwalking-with-einstein/`, consultado el 21/abril/2017).

fácil de recordar (y segura contra ataques de "fuerza bruta" y de "diccionario" [1]) si se imagina la persona realizando la acción sobre el objeto.

Memorizar una passphrase

Para memorizar una passphrase que ha sido generada con un sistema como *diceware*, existen dos recomendaciones importantes:

1. **Escribir la passphrase repetidamente**: La primera recomendación es:
   a) Escribir la passphrase 4 ó 5 veces con lápiz y papel, y luego destruir el papel en el cual se escribió (no basta con arrugar el papel, es necesario romperlo en muchos pedazos o, mejor aún, quemarlo); es muy conveniente repetir esta acción varios días seguidos, espaciando cada vez más la acción.
   b) Tipear el password en un teclado 4 ó 5 veces, idealmente en el mismo sistema para el cual uno está creando la passphrase; también se recomienda repetir esta acción diariamente durante varios días seguidos, espaciando cada vez más la acción.
2. **Usar el método del "palacio de la memoria"**: La segunda recomendación es utilizar una técnica llamada el "método de loci"[5], conocida también como del "templo de la memoria". Consiste en imaginar un paseo por una serie de habitaciones en un lugar conocido por la persona (por ejemplo, una casa donde haya vivido), donde se "colocará" mentalmente objetos que representen las palabras de la passphrase que uno desea recordar. Cada vez que uno desea recordar la passphrase, recorre la casa imaginaria "visualizando" los objetos que uno colocó allí antes.

El principio básico sobre el que se apoya la primera recomendación se llama "repetición espaciada"[6].

¿Cuál de las dos recomendaciones deberíamos seguir? Nuestra recomendación es seguir ambas, por dos razones. En primer lugar, existe evidencia de que escribir una serie de palabras a mano genera un mayor nivel de recordación que el simplemente tipear las mismas palabras en computador [21]. En segundo lugar, existe evidencia sólida de que la repetición de palabras o conceptos a través de computadores mejora su retención y posterior recuerdo [3], en particular si se trata de passwords [1].

Revisemos por ejemplo la siguiente passphrase, que se generó a través del método diceware[7]:

■ **Ejemplo 7.1 — Passphrase sin puntuación.** 805 ZANCO SOMOS GOL VANO ■

Podemos imaginar que el número de nuestra casa es 805, que justo al lado de la puerta hay un zanco, que el televisor en el living está encendido transmitiendo un partido de fútbol, que un mensaje en el televisor dice "somos gol", y que una persona al lado del televisor dice que el gol es en "vano". Para finalizar, podemos agregar signos de puntuación que nos permitan darle más sentido a la passphrase; por ejemplo:

■ **Ejemplo 7.2 — Passphrase con puntuación.** 805.ZANCO."SOMOS-GOL!",VANO ■

7.3 Método 2: Usa un administrador de passwords

Un administrador de passwords es un programa o servicio que le permite a una persona generar passwords únicos para sus distintas cuentas o servicios. Se accede al administrador a través de un password maestro. De manera muy general, existen dos tipos: aquellos que se instalan en el computador

[5] `https://en.wikipedia.org/wiki/Method_of_loci`. Consultado el 24/abril/2017.

[6] El artículo de Wikipedia entrega una buena introducción: `https://en.wikipedia.org/wiki/Spaced_repetition`. Consultado el 21/abril/2017.

[7] Esta passphrase fue generada a través de `https://www.rempe.us/diceware/#spanish`. Consultado el 17/mayo/2017.

personal, y aquellos que son provistos a través de un sitio web. Una de las ventajas más importantes de este tipo de servicios es que permiten generar un password único y aleatorio para cada servicio, programa o sitio web que uno maneje (el que sea aleatorio significa que es poco predecible, y por tanto altamente seguro). La desventaja más evidente es la necesidad de recordar un password maestro:

1. Si el password es poco seguro, otras personas podrían adivinarlo y obtener acceso a todos los recursos protegidos por el administrador.
2. Olvidar el password maestro podría quitarle a uno acceso de manera permanente a todos los servicios protegidos por el administrador.

La funcionalidad básica de un administrador de passwords es la siguiente: una vez que uno instala el software (ya sea sobre el navegador o en el computador), el software reconoce cuando uno está ingresando un password, y le ofrece a uno "recordar" ese password. Si uno decide recordar el password en ese sitio, las próximas veces que uno visite el mismo sitio web, el software permite llenar automáticamente el username y password.

Todos los navegadores modernos (Firefox, Chome/Chromium, Safari y Opera) ofrecen alguna variación de la funcionalidad anterior. A continuación, se describen tres administradores de passwords distintos, las funcionalidades que ofrecen por sobre la funcionalidad básica, y las desventajas que pueden ser identificadas para cada uno.

7.3.1 Lastpass

Lastpass es una aplicación para el browser, que se sincroniza a través de un sitio web (`https://lastpass.com`), con plugins para Firefox, Chrome, Safari, Internet Explorer y Opera[8]. Existen aplicaciones para Android y iPhone. La aplicación está disponible en español, y tiene una versión gratuita y una pagada, que entrega mayores funcionalidades.

Funcionalidades

Las funcionalidades más importantes de este software (por sobre la funcionalidad básica) son las siguientes:

1. Una vez que uno instala el plugin en el navegador de su preferencia (e.g., Chrome), el proceso de detección de ingreso de usernames y passwords es automático. El software es capaz de reconocer cuándo uno está ingresando un password, y de ofrecerle a uno "recordar" ese password. Si uno decide recordar un password, las próximas veces que uno visite el mismo sitio web, el software llenará automáticamente el username y password. Si uno cambia el password en un sitio web, el software también lo detecta y ofrece guardar el cambio.
2. El software permite generar passwords aleatorios distintos para cada sitio, permitiendo escoger parámetros del password como su largo, el set de caracteres para componer el password, si el password debe ser "pronunciable", y otros.
3. Los passwords se guardan localmente en el computador, encriptados con un password maestro conocido sólo por el usuario, y no son transmitidos a los servidores de LastPass[9]. El sistema ofrece doble factor de autenticación para la recuperación del password maestro[10].
4. Además del almacenamiento de usernames y passwords, el servicio ofrece guardar notas seguras, en las cuales uno puede guardar cualquier clase de mensaje o información que uno considere sensible (por ejemplo, el número de tarjeta de crédito).

[8] `https://lastpass.com/features_free.php`. Consultado el 11/sept/2017.
[9] `https://www.lastpass.com/how-it-works`. Consultado el 11/sept/2017.
[10] `https://lastpass.com/multifactor-authentication/`. Consultado el 11/sept/2017.

5. El software posee una funcionalidad llamada “Security Challenge”, que permite revisar y comparar los passwords que uno utiliza, y que reporta dos cosas:
   a) En qué sitios uno está usando el mismo password,
   b) Qué passwords son fácilmente adivinables por otras personas.

Debilidades

La principal debilidad de este software no es técnica sino legal: tiene que ver con la inestabilidad de los términos de uso y política de privacidad del servicio, como consecuencia de una serie de fusiones y ventas con otras compañías.

LastPass fue adquirido en octubre de 2015 por LogMeIn Inc., un proveedor de software como servicio (SaaS) de EE.UU.[11] A su vez, LastPass se encuentra (primer trimestre de 2017) en un proceso de fusión con GetGo Inc., una compañía de inversiones en comunicaciones, información y entretenimiento[12]. Según la política de privacidad de LogMeIn (que es la aplicable a LastPass), la información de los clientes y usuarios de LastPass será compartida con “la familia de compañías LogMeIn (la que incluye GetGo), sin embargo, tus datos continuarán siendo usados sólo para los propósitos para los cuales fueron recolectados”[13]. La política de privacidad de LogMeIn ofrece un formulario para solicitar que los datos no sean transferidos a la empresa resultante, y advierte que cuando la fusión termine, habrá una política de privacidad unificada.

En la práctica, este tipo de problemas ocurre a menudo con las compañías de tecnología. Cuando se fusionan o venden, los términos de referencia y las políticas de privacidad de los servicios ofrecidos (que son un contrato entre el usuario del servicio y la compañía) dejan de tener validez cuando la empresa que ofrecía el servicio deja de existir (cuando una empresa es vendida o se fusiona con otra, la compañía original deja de existir). En general, no existe ninguna obligación ni incentivo por parte de las empresas para mantener los mismos términos de servicio que originalmente ofrecieron a sus clientes.

En síntesis, el servicio es técnicamente muy bueno, pero legalmente no existe ninguna garantía de que los datos de las personas no vayan a ser transferidos a otra empresa dentro de algunos meses o años. Por eso, recomendamos utilizar este servicio sólo para cuentas y servicios personales o privadas; en ningún caso podemos recomendar este servicio para guardar los passwords de servicios como el correo institucional del Ministerio de Defensa, o los sistemas documentales del Ministerio de Defensa.

7.3.2 Dashlane

Dashlane es una aplicación para el computador personal y para dispositivos móviles (`https://www.dashlane.com/`). Está disponible para Windows y Mac (no para Linux), y posee versiones para Android, iPhone y Windows Phone. Está disponible en español, y tiene una versión gratuita y una pagada[14].

Funcionalidades

Las funcionalidades más importantes de este software (por sobre la funcionalidad básica) son las siguientes:

1. De manera similar a LastPass, Dashlane permite la detección automática del ingreso de usernames y passwords en sitios web, y el reconocimiento del cambio de passwords en sitios web[15]. Dashlane

[11] `https://secure.logmein.com/home`. Consultado el 11/sept/2017

[12] El sitio web de GetGo (`http://www.getgocorp.com/`) está vacante (abril/2017); sin embargo, al parecer la empresa sigue existiendo según Bloomberg (`https://www.bloomberg.com/profiles/companies/GTGOF:US-getgo-inc`).

[13] `https://secure.logmein.com/home/policies/privacy`. Consultado el 11/sept/2017.

[14] `https://www.dashlane.com/plans`. Consultado el 15/mayo/2017.

[15] `https://www.dashlane.com/features/password-manager`. Consultado el 15/mayo/2017.

permite también generar passwords aleatorios con distintas variaciones y opciones, y permite cambiar passwords de manera automática en algunos sitios web[16] (preferentemente en Estados Unidos).
2. Al igual que LastPass, Dashlane guarda los passwords localmente, y no los transmite a los servidores de Dashlane[17]. La funcionalidad de autenticación de doble factor está disponible sólo para la versión pagada[18].
3. Dashlane también permite guardar notas seguras.
4. El software ofrece una "billetera virtual", que permite guardar no sólo números de tarjetas de crédito, sino también recibos o boletas de servicios[19]. El servicio incluye la asociación entre el número de la tarjeta de crédito y la dirección postal para poder llenar de manera más ágil los formularios de compra en línea.
5. Una de las funcionalidades más útiles es la generación de mensajes de alerta para el usuario cuando ocurre un incidente de seguridad en un sitio web[20].

Debilidades

La empresa que opera Dashlane (Dashlane Inc.) está ubicada en Delaware, EE.UU. Tal como muchos otros servicios en línea, el servicio de Dashlane se entrega sin ninguna garantía; la empresa que opera Dashlane no es responsable de las condiciones de servicio, y por el solo hecho de utilizar el software el usuario accede a no demandar a la empresa. A pesar de que la empresa realiza "su mejor esfuerzo" por brindar un servicio seguro, no garantiza tampoco ni la confidencialidad de la comunicación ni de la información almacenada en el computador personal, ni de la información transmitida a través de las redes, ni la seguridad de los passwords generados.

El contrato unilateral anterior es típico de los servicios en línea; al igual que en el caso de LastPass, Dashlane es una muy buena opción para todos aquellos datos que no sean altamente sensibles, o que tengan relación con la seguridad nacional.

7.3.3 Keepass

Keepass es un software libre (es decir, no sólo gratuito sino que su código fuente está disponible de manera pública) principalmente para Microsoft Windows (`http://keepass.info/`). A pesar de que puede ser instalado en Linux, Mac y otros sistemas operativos, la integración con estos sistemas operativos no funciona bien, y gran parte de la funcionalidad más útil se pierde.

A diferencia de los sistemas anteriores, este software es exclusivamente para computadores de escritorio: no existen versiones de este software para teléfonos móviles, y por tanto no se puede utilizar para ingresar a través del teléfono móvil propio. Sin embargo, posee una ventaja muy fuerte que no poseen las dos anteriores: al ser un sistema que se puede instalar en el computador, uno mantiene completo control (y jurisdicción legal) sobre la información sensible que se coloque en el computador. Está disponible en español, y es completamente gratuito.

Finalmente, este software puede instalarse en un pendrive USB, lo que permite llevarlo permanentemente y usarlo en cualquier computador con Microsoft Windows al que uno tenga acceso.

[16] `https://www.dashlane.com/password-changer`. Consultado el 15/mayo/2017.
[17] `https://www.dashlane.com/security`. Consultado el 15/mayo/2017.
[18] `https://www.dashlane.com/plans`. Consultado el 15/mayo/2017.
[19] `https://www.dashlane.com/features/digital-wallet`. Consultado el 15/mayo/2017.
[20] `https://www.dashlane.com/features/security-alerts`. Consultado el 15/mayo/2017.

Funcionalidades

Las funcionalidades más importantes de este software (por sobre la funcionalidad básica) son las siguientes:

1. El sistema permite automatizar en gran medida el ingreso de usernames y passwords, y lo complementa con casi cualquier tipo de ingreso de información.
2. Al igual que en los casos anteriores, la información sensible se guarda de manera local, se encripta con el password maestro, y nunca es enviada fuera del computador (o del pendrive USB donde está instalado).
3. De manera similar, el software permite generar passwords aleatorios, con distintas variaciones y opciones, como el largo del password, qué set de caracteres se utiliza para generarlo, etc.
4. El software protege el password maestro cambiando frecuentemente su encripción. Adicionalmente, el software protege el password maestro de otros procesos que puedan estar corriendo en el mismo computador.
5. El software es completamente "local": puede ser instalado en un pendrive USB, sin necesidad de instalarlo en el computador que se utilice. Esto permite utilizarlo en más de un computador, sin instalar archivos localmente.
6. La lista de passwords puede ser exportada a archivos externos en varios formatos de uso común (txt, html, xml, csv). También permite importar listas de passwords de un grupo reducido de otros administradores de passwords.

Debilidades

Este software no posee la desventaja de los anteriores, en el sentido de que por diseño la información nunca deja el computador (o el pendrive USB) desde donde se utiliza. Sin embargo, al ser exclusivamente para computadores de escritorio con Microsoft Windows, carece de la funcionalidad de sincronización que poseen los dos anteriores (Dashlane y LastPass).

7.4 Método 3: Usa una tarjeta de passwords

Una tarjeta de passwords es una tarjeta del tamaño de una tarjeta de crédito, con una tabla de números y letras, que puedes imprimir y llevar en tu billetera o cartera.

En muchas instituciones es parte del "folkore de seguridad" el recomendar no anotar un password en papel. Sin embargo, expertos en seguridad como Bruce Schneier han recomendado por años crear un password aleatorio en un papel y guardar el papel en la billetera[21], porque en general sabemos bien cómo cuidar nuestra billetera. En la medida que no perdamos la billetera ni anotemos nuestros usernames junto con los passwords correspondientes, esta es una mejor idea que tener passwords fáciles de adivinar, o reutilizarlos en muchos sitios distintos.

Existen varias opciones de tarjetas de passwords en Internet. A continuación describimos dos opciones.

7.4.1 Password cards

Este es un servicio gratuito ofrecido por el sitio web `https://www.passwordcard.org/es`.

Cada vez que alguien visita el sitio web, se genera una tarjeta nueva que el visitante puede bajar e imprimir. La tarjeta contiene una tabla con una serie de caracteres alfabéticos y números (ver la

[21] `https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html`. Consultado el 27/abril/2017.

figura 7.1 en la pág. 53). Las filas están numeradas del 1 al 8, y las columnas están encabezadas por un símbolo.

Figura 7.1: Ejemplo de tarjeta de passwords generada por el sitio `https://passwordcard.org/es` (no utilizar).

Cada vez que uno requiere crear un password, escoge una combinación de una símbolo (columna) y un número (fila), y utiliza los caracteres que aparecen en la intersección de la fila y columna escogidas. A partir de entonces, cada vez que uno requiera ingresar el mismo password, debe recordar el símbolo y número con que fue creado, y consultar en la tarjeta los caracteres correspondientes.

¿Cómo se utiliza esta tarjeta?

Antes de comenzar a utilizar la tarjeta, uno debe escoger un largo de password y una dirección determinada:

1. El largo de un password es fundamental para evitar que sea adivinada por un atacante. Mientras más largo sea un password, más difícil es para un oponente el intentar adivinarlo (ver sección 7.5.1 en pág. 55). El largo recomendado mínimo es de 10 caracteres para usos que no requieran un nivel alto de seguridad, y 15 para aquellos sitios más sensibles.
2. A pesar de que lo natural es escoger el sentido de izquierda a derecha, también es posible escoger leer passwords en cualquier otro sentido (de arriba hacia abajo, de derecha a izquierda o incluso en diagonal).

Una vez escogido un largo de password y un sentido, cada vez que uno necesita crear un password nuevo, escoge un número de fila (del 1 al 8) y un símbolo (de los presentes en la primera fila), y utiliza el conjunto de caracteres que se encuentran en ese punto, con el largo escogido, en la dirección escogida. En vez de tener que recordar el password completo (lo que es difícil, pues son caracteres aleatorios), uno tiene que recordar el símbolo y el número con el que "creó" el password.

Por ejemplo: supongamos que escogemos de antemano 10 caracteres de largo, y el sentido de izquierda a derecha. Supongamos que tenemos que crear un password para un sitio web de compras (por ejemplo, Amazon). Al momento de crear el password, supongamos que decidimos asociar el sitio Amazon con el símbolo peso ($) y con el número 3. En la tarjeta que aparece en la figura 7.1, encontramos el carácter que se encuentra en la fila "3", y en la columna "$" (es el dígito 4). Incluyendo ese caracter, usamos los 10 caracteres que le siguen, resultando el siguiente password: 4VRPTSC7RJ.

Cada vez que tengamos que ingresar el password en el sitio web Amazon, tenemos que recordar que ese sitio está asociado con la combinación "$3", y buscar los 10 caracteres correspondientes a partir de ese punto.

En el caso de que una tarjeta se pierda (o sea robada), es posible generar una copia de la misma

tarjeta ingresando al sitio web que ofrece el servicio, e ingresando el número de identificación de la tarjeta (que aparece en el borde inferior).

¿Qué tan segura es esta tarjeta?

El propósito de esta tarjeta es, según su autor, el ofrecer una forma de crear passwords más seguros que los usados típicamente por la mayor parte de los usuarios[22], sin ninguna garantía de ser seguros para usos más sensibles. En ese sentido, repetimos aquí las recomendaciones más relevantes que hace el autor a propósito del uso de esta tarjeta:

1. Mantén tu tarjeta contigo, en tu billetera (idealmente, junto a tu tarjeta de crédito).
2. No marques el lugar donde está tu password con el dedo, ni hagas marcas con la uña sobre la tarjeta (por supuesto, tampoco marques un password con lápiz o destacador). Una persona que esté mirando por encima de tu hombro sabrá inmediatamente cuál es tu password.
3. Luego de generar una versión de una tarjeta a través del sitio web, borra el cache y la historia del navegador.

A pesar de lo anterior, existen algunas consideraciones que es necesario tener en cuenta[23] si se desea utilizar esta tarjeta en casos más triviales que las de un sitio web:

1. La seguridad de la tarjeta se basa fuertemente en el número de identificación de la tarjeta (el que aparece en el borde inferior). El número es útil para regenerar la tarjeta en caso de que uno la pierda, pero también es útil para un atacante. Si alguien llega a conocer ese número, puede regenerar nuestra tarjeta a través del sitio.
2. En caso de que un atacante llegara a robar nuestra tarjeta y a intentar ingresar a un sistema con ella, el número total de passwords posibles que se puede escoger a partir de una tarjeta no es grande. En total, existen 29 por 8 caracteres desde los cuales es posible "comenzar" un password. Considerando que existen en teoría 8 direcciones posibles (hacia arriba, hacia abajo, hacia la izquierda, hacia la derecha, y otras cuatro direcciones en diagonal), existe un total de $29 * 8 * 8$ (1.856) combinaciones posibles para un largo determinado de passwords. Si se intentan (por ejemplo) todos los largos posibles entre 8 y 12, la cantidad no aumenta mucho: $29 * 8 * 8 * 5$ (9.280). Dado que el código fuente con el que fue construido este software está disponible públicamente[24], es relativamente sencillo generar un programa que pruebe todas las combinaciones posibles de manera automática.

7.4.2 Tarjetas Qwerty

Este es un producto ofrecido por la empresa Tream Tech Ltd., de Reino Unido[25]. Esta tarjeta es muy similar a la anterior, pero no es ofrecida a través de un sitio web: cada tarjeta es generada aleatoriamente, es impresa y luego enviada físicamente al cliente por correo.

¿Cómo se utiliza esta tarjeta?

El procedimiento sugerido para ingresar un password utilizando una tarjeta Qwerty como la que aparece en la figura 7.2 (pág. 55) es la siguiente:

1. Ingresar los caracteres que aparecen en la "barra espacio" del teclado mostrado en la tarjeta (p.ej., SH(/J3HQ).

[22] `https://security.stackexchange.com/a/34885`. Consultado el 27/abril/2017.

[23] Estas consideraciones están basadas en el análisis publicado en `stackexchange.com`, en la misma URL de la nota a pie de página anterior.

[24] `https://www.passwordcard.org/algorithm.html`. Consultado el 27/abril/2017.

[25] `https://www.qwertycards.com/`. Consultado el 17/mayo/2017.

2. Ingresar una clave propia, que será siempre la misma para todos los passwords.
3. Ingresar la correspondencia caracter a caracter del sitio web o aplicación para la cual se está generando un password. Por ejemplo, si se está creando un password para Amazon, los caracteres que corresponden a la palabra "Amazon" son .U.RQF

A diferencia del caso anterior, no existe una forma de recuperar la tarjeta si es robada o si se pierde. Como ventaja por sobre el caso anterior, estas tarjetas son generadas de manera completamente aleatoria; por tanto su nivel de seguridad es (en teoría) muy alto.

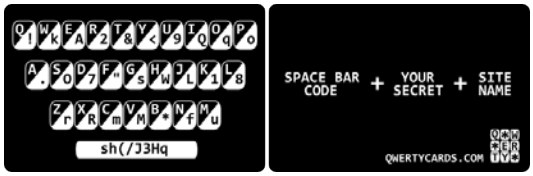

Figura 7.2: Ejemplo de tarjeta de passwords generada por la empresa Tream Tech Ltd. (no utilizar).

¿Qué tan segura es esta tarjeta?

De acuerdo con el proveedor, cada tarjeta es generada con un equipo especial: un generador de números realmente aleatorios[26]. De ser cierto, la fortaleza del password generado depende de tres partes:

1. La parte del password que se encuentra en la barra espacio. Según el proveedor, esta parte del password contiene "al menos un número, una letra minúscula, una letra mayúscula, y un caracter no alfanumérico"[27]. Al parecer, esta parte tiene un largo de 8 caracteres. Esta parte permite agregar caracteres realmente aleatorios a todos los passwords, haciendo más difícil el adivinar alguno (ver la sección 7.5.1, pág. 55).
2. La parte del password que escoge la persona, y que es igual para todos los passwords que se generan con la tarjeta. Esto hace más difícil que un atacante pueda adivinar algún password si la tarjeta se pierde o es robada.
3. La parte del password que es única respecto del sitio web o sistema para el que se desea generar un password. Esto permite hacer único cada password así generado.

7.5 Tipos de ataques

7.5.1 Ataque de "fuerza bruta"

En esta sección del documento (de lectura optativa), se explica con un poco más de detalle los tipos de ataque existentes, y la mejor forma de protegerse contra dichos ataques.

Descripción del ataque

El ataque de "fuerza bruta" consiste en probar todas las combinaciones posibles de passwords. El número total de combinaciones posibles depende de dos factores: el largo del password (es decir, el número de caracteres que tiene el password), y el tamaño del alfabeto desde donde se escogen caracteres para el password.

[26] `https://www.qwertycards.com/frequent_questions#different_codes`. Consultado el 17/mayo/2017. Los números "aleatorios" que generan los computadores en realidad son seudo-aleatorios; en realidad utilizan algoritmos que, a partir de un dato inicial conocido como "semilla", generan números que son difíciles de predecir, y que (idealmente) generan todos los números dentro de cierto rango con igual frecuencia.

[27] `https://www.qwertycards.com/frequent_questions#three_part_codes`. Consultado el 17/mayo/2017.

El largo del password determina de manera crítica la cantidad de combinaciones posibles. Mientras más largo, mayor será la cantidad de combinaciones posibles.

El tamaño del alfabeto tiene que ver con cuál es el conjunto total de caracteres (letras, números, signos de puntuación, etc.) desde el cual se escogerá un password. Por ejemplo, existen 27 letras en el alfabeto español. Como las letras minúsculas y mayúsculas son consideradas distintas para efectos de escoger un password, entonces el tamaño del alfabeto para los passwords compuestos sólo por letras es de tamaño 54 ($27 * 2$). Si uno decide tener passwords con letras y números, entonces el tamaño del alfabeto aumenta a 64 (54 más 10 dígitos). Un password sólo con números tendrá un alfabeto de tamaño 10.

La tabla 7.1 en la página 57 resume la cantidad de combinaciones posibles de passwords para distintos largos, suponiendo un alfabeto de tamaño 37 (el que resultaría de usar sólo letras minúsculas y dígitos, por ejemplo). Para dar una idea del grado de dificultad que representa para un atacante el probar todas las combinaciones posibles de passwords (para adivinar un password específico), usaremos dos atacantes ideales:

1. **Un atacante novato**: Este atacante puede usar sólo un computador, y puede probar mil passwords distintos por segundo en ese computador. En la tercera columna de la tabla 7.1 se indica el tiempo (ideal) que tomaría a este atacante probar todas las combinaciones posibles de passwords.
2. **Un atacante poderoso**: Este atacante puede usar 900.000 computadores trabajando de manera paralela (que es la cantidad estimada total de servidores que tenía Google en 2014 alrededor del mundo[28]), probando un millón de combinaciones por segundo en cada computador, y donde ningún computador se traslapa con otro (es decir, no hay dos computadores probando el mismo password). No toma en cuenta el tiempo necesario para comunicar la respuesta entre los computadores. La columna de la derecha en la tabla 7.1 muestra el tiempo que le tomaría a este atacante probar todas las combinaciones posibles de passwords. En la práctica, este "atacante" ideal es un límite superior de lo que es razonablemente posible a la fecha (agosto de 2017) para cualquier grupo de personas que no tiene acceso a los recursos de un Estado.

Aplicabilidad del ataque

Este ataque es efectivo sólo si el atacante puede "probar" passwords de manera relativamente rápida. Por ejemplo, supongamos que la Presidenta tiene un correo electrónico personal en Gmail, y que estamos decididos a averiguar el password. A pesar de que en teoría podríamos probar todas las combinaciones posibles del password en el sitio web de Gmail, esto es poco práctico, pues aunque pudiéramos probar un password por segundo, la cantidad de combinaciones posibles es tan grande que nos tomaría demasiado tiempo. Además, probablemente Google se daría cuenta de lo que estamos intentando hacer mucho antes de que pudiéramos adivinar el password de la presidenta por fuerza bruta.

En la práctica, este ataque es muy poco "eficiente", pero tiene la ventaja de que garantiza el encontrar un password determinado, aunque pueda ser en un tiempo muy largo. Una forma de hacer este ataque más eficiente es distribuyendo la tarea entre muchos computadores; sin embargo, para passwords relativamente largos sigue siendo un ataque impráctico. Por ejemplo, se estimaba en 2014 que Google tenía alrededor de 900.000 servidores alrededor del mundo[29]. Si pusiéramos a trabajar todos esos servidores en tratar de encontrar un password en paralelo, sería en teoría posible averiguar cualquier password de 8 caracteres o menos en menos de un segundo. Sin embargo, si aumentamos el largo del password a 15 caracteres, le tomaría alrededor de 104 años y 33 días a un atacante con esa enorme capacidad el averiguar el password; si aumentamos el largo del password a 20 caracteres, le

[28] `https://www.cloudyn.com/blog/10-facts-didnt-know-server-farms/`. Consultado el 7 de abril de 2017.

[29] Ver pie de página anterior.

Largo del password	*Número de passwords posibles (con un alfabeto de 37 signos)*	*Tiempo que tomaría probar todos los passwords a un atacante novato*	*Tiempo que tomaría probar todos los passwords a un atacante poderoso*
4	1.874.161	31 minutos y 15 segundos	Alrededor de 3 millonésimas de segundo.
6	2.565.726.409	29 días, 16 horas, 42 minutos y 7 segundos	Alrededor de 3 milésimas de segundo.
8	3.512.479.453.921	111 años, 138 días, 16 horas y 45 minutos	Alrededor de 4 segundos.
10	4.808.584.372.417.849	152.479 años y 77 días	Alrededor de 1 hora y media.
12	6.582.952 billones	208,7 millones de años	84 días, 15 horas y 47 minutos.
14	9.012.061.295 billones	285.770,6 millones de años (alrededor de 20 veces la edad del universo)	317 años, 190 días, 20 horas y 24 minutos.
16	12.337.511.914.217 billones	En la práctica, inalcanzable.	434.688 años y 299 días.
18	$1,69 * 10^{28}$	En la práctica, inalcanzable.	595,1 millones de años.
20	$2,31 * 10^{31}$	En la práctica, inalcanzable.	814.676,8 millones de años (alrededor de 60 veces la edad del universo)
25	$1,6 * 10^{39}$	En la práctica, inalcanzable.	En la práctica, inalcanzable.

Tabla 7.1: Número total de passwords posibles, en función del largo del password (en número de caracteres), asumiendo un alfabeto de 37 signos.

tomaría al atacante alrededor de un millón y medio de años el averiguar el password.

Protección contra el ataque

La mejor forma de protegerse contra un ataque de fuerza bruta es escogiendo un password que tenga al menos 15 caracteres, y que tenga al menos letras mayúsculas, minúsculas y números. En la práctica, y siempre que el uso no requiera de un nivel alto de seguridad, un password de 10 caracteres de largo es útil para la mayor parte de los usos cotidianos.

7.5.2 Ataque de diccionario

Descripción del ataque

Un ataque más eficiente que el de fuerza bruta es un ataque de diccionario. El atacante, en vez de probar todas las combinaciones posibles, prueba combinaciones de "palabras" que es probable que el creador del password haya utilizado (como "password", "123456", "iloveyou", y otros). Este es un mejor ataque porque es mucho más probable que utilicemos "Pedro1234" como password en vez de un password aleatorio como "dh84qgk37jf".

Las "palabras" en este tipo de ataque son tomadas de una lista (llamada "diccionario") de palabras que las personas típicamente usamos en nuestros passwords. Las palabras no tienen que estar necesariamente formadas por letras: una "palabra" típica en muchos diccionarios podría ser "123456".

Este último fue el password más común utilizado durante el 2016, según un estudio realizado por una empresa de seguridad en Estados Unidos [11].

Ahora bien; desde el punto de vista de una persona queriendo escoger un password más seguro, ¿qué tan seguro es escoger varias palabras como password en vez de un password de caracteres aleatorios? En otras palabras, ¿qué tan seguro es el método de passphrases (descrito anteriormente) frente a un ataque de diccionario?

Mientras más palabras tenga un diccionario, mayor es el número de combinaciones de (por ejemplo) cuatro palabras escogidas al azar en ese diccionario. Por ejemplo, si un diccionario contiene 1.000 palabras, y escogemos 4 de ellas al azar, existen poco más de 41 mil millones de combinaciones posibles. Como además existen 24 formas posibles de ordenar cada una de las combinaciones de 4 palabras, existen en total poco más de 994 mil millones de passphrases posibles (que le tomaría a un atacante novato alrededor de 31 años y medio probar). Por tanto, si el atacante y la víctima escogieran passwords del mismo diccionario, un password es más seguro mientras más palabras posea, y mientras más grande sea el número total de palabras en el diccionario.

Num. de palabras en	*Tiempo que tomaría probar todas las passphrases de 4 palabras a atacante novato*			*Tiempo que tomaría probar todas las passphrases de 4 palabras a atacante poderoso*		
dicc.	*4 palabras*	*5 palabras*	*6 palabras*	*4 palabras*	*5 palabras*	*6 palabras*
1.000	31 años, 189 días, 18 horas y 10 mins.	31.393 años y 293 días	31,2 millones de años	1,1 segs.	18 mins. y 20 segs.	12 días, 16 horas, 2 mins. y 19 segs.
7.776 (diceware)	115.846 años y 215 días	900,4 millones de años	6.996.695,1 millones de años (más de 500 veces la edad del universo)	1 hora, 7 mins. y 40 segs.	1 año, 3 horas y 30 mins. y 4 segs.	7.774 años y 39 días.

Tabla 7.2: Número total de passphrases posibles, en función del número de palabras en el diccionario desde donde se toman palabras al azar para escoger una passphrase, y el número de palabras al azar escogidas para un password.

Aplicabilidad del ataque

En la práctica, este es un ataque bastante práctico y efectivo. Es relativamente sencillo escoger diccionarios con palabras típicamente usadas por las personas para componer sus passwords. Existen muchos sitios web que publican diccionarios que han sido compilados de diversas formas. Por ejemplo:

1. **Passwords robados de sitios web**: Muchas veces grupos de delincuentes roban listas de passwords de sitios web muy usados (p.ej., redes sociales) y los publican directamente en Internet. Algunos sitios de seguridad republican las listas de los passwords publicados sin la información de los nombres de usuario para facilitar la investigación en seguridad. Por ejemplo, skullsecurity.org[30] publica listas de filtraciones de passwords de sitios como Facebook, RockYou, PhpBB, MySpace, Gawker, y otros.

[30] `https://wiki.skullsecurity.org/Passwords#Leaked_passwords`. Consultado el 20/abril/2017.

2. **Nombres de personas en Facebook**: Muchas personas utilizan sus propios nombres, o nombres de familiares, amigos o parejas para componer sus passwords. El sitio skullsecurity.org también publica una lista de los nombres y apellidos más comunes en Facebook[31].
3. **Palabras comunes**: Es muy frecuente también crear passwords con nombres de objetos, combinaciones de teclas en el teclado QWERTY, nombres de ciudades, citas de libros, versículos de libros religiosos como la biblia o la torah, etc. El sitio korelogic.com publicó una lista de diccionarios[32] como base para un concurso que realizó la empresa durante la conferencia DEFCON 2010.

Por otro lado existen muchas herramientas gratuitas, disponibles para (en teoría) cualquier persona, que permiten usar cualquiera de los diccionarios de arriba para intentar averiguar una passphrase. Por ejemplo, la herramienta que a la fecha (abril de 2017) es la más rápida del mundo para crackear passwords es Hashcat[33].

Protección contra el ataque

La mejor defensa posible contra este ataque es la misma que para un ataque de fuerza bruta: escogiendo passwords de caracteres aleatorios (con letras minúsculas, mayúsculas y números), de al menos 15 caracteres de largo, porque por definición un password aleatorio no va a estar contenido en un diccionario de palabras comunes.

Si uno utiliza passphrases (pág. 46) en vez de passwords, lo más seguro es escoger al menos 5 palabras verdaderamente al azar de un diccionario definido; por ejemplo, el método diceware (pág. 47) con alguna lista de palabras en español, o bien el generador en línea en el sitio `rempe.us`.

[31] `https://blog.skullsecurity.org/2010/return-of-the-facebook-snatchers`. Consultado el 20/abril/2017.

[32] `http://contest-2010.korelogic.com/wordlists.html`. Consultado el 20/abril/2017.

[33] `https://hashcat.net/hashcat/`. Consultado el 24/abril/2017. El registro de velocidad se realizó en Junio de 2016 sobre un Sagitta Bruttalis (`https://sagitta.pw/hardware/gpu-compute-nodes/brutalis/`; consultado el 24/abril/2017), una máquina con 8 GPUs que cuesta alrededor de USD$21.200.

Referencias

[1] J. Blocki, M. Blum y A. Datta, "Naturally Rehearsing Passwords", páginas 1-34, 2015. DOI: 10.1007/978-3-642-42045-0_19. arXiv: 1302.5122 (véase página 48).

[2] J. Bonneau, C. Herley, P. C. Van Oorschot y F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes", *Proceedings - IEEE Symposium on Security and Privacy*, páginas 553-567, 2012, ISSN: 10816011. DOI: 10.1109/SP.2012.44 (véase página 36).

[3] C. Caple, "The effects of spaced practice and spaced review on recall and retention using computer-assisted instruction", Doctoral dissertation, North Carolina State University, 1996, página 99 (véase página 48).

[4] A. Das, J. Bonneau, M. Caesar, N. Borisov y X. Wang, "The Tangled Web of Password Reuse", *Proceedings 2014 Network and Distributed System Security Symposium*, número February, páginas 23-26, 2014. DOI: 10.14722/ndss.2014.23357. dirección: http://www.jbonneau.com/doc/DBCBW14-NDSS-tangled%7B%5C_%7Dweb.pdf (véase página 38).

[5] Estado de Chile, *Ley 19880, establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado*, Santiago, Chile, 2008. dirección: http://bcn.cl/1uv5j (véase página 32).

[6] ——, *Ley 19628, sobre protección de la vida privada*, Santiago, Chile, 2012. dirección: http://bcn.cl/1uv2v (véase página 31).

[7] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin y D. Wagner, "Android Permissions: User Attention, Comprehension , and Behavior", *Symposium on Usable Privacy and Security (SOUPS) 2012*, 2012 (véase página 33).

[8] D. Florencio y C. Herley, “A large-scale study of web password habits”, *Proceedings of the 16th international conference on World Wide Web - WWW ’07*, página 657, 2007, ISSN: 08963207. DOI: 10.1145/1242572.1242661 (véanse páginas 36, 45).

[9] P. A. Grassi, M. E. Garcia y J. L. Fenton, “NIST 800-63-3: Digital Identity Guidelines”, informe técnico, 2017, página 68. DOI: 10.6028/NIST.SP.800-63-3. dirección: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf (véase página 30).

[10] C. Jernigan y B. F. T. Mistree, “Gaydar: Facebook friendships expose sexual orientation”, *First Monday*, volumen 14, número 10, 2009. dirección: http://firstmonday.org/ojs/index.php/fm/article/viewArticle/2611/2302 (véase página 31).

[11] Keeper, *The Most Common Passwords of 2016*, 2016. dirección: https://keepersecurity.com/public/Most-Common-Passwords-of-2016-Keeper-Security-Study.pdf (visitado 18-05-2017) (véase página 58).

[12] P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor y J. López, “Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms”, *Proceedings - IEEE Symposium on Security and Privacy*, páginas 523-537, 2012, ISSN: 10816011. DOI: 10.1109/SP.2012.38 (véase página 46).

[13] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor y S. Egelman, “Of Passwords and People: Measuring the Effect of Password-Composition Policies”, *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI ’11*, página 2595, 2011, ISSN: 00010782. DOI: 10.1145/1978942.1979321. dirección: http://www.ece.cmu.edu/%7B~%7Dlbauer/papers/2011/chi2011-passwords.pdf (véase página 46).

[14] S. Lee y S. Zhai, “The Performance of Touch Screen Soft Buttons”, *Methodology*, páginas 309-318, 2009. DOI: 10.1145/1518701.1518750 (véase página 40).

[15] A. Ludwig, “Android Security 2016 Year in Review”, informe técnico March, 2016, página 71. dirección: https://source.android.com/security/reports/Google%7B%5C_%7DAndroid%7B%5C_%7DSecurity%7B%5C_%7D2016%7B%5C_%7DReport%7B%5C_%7DFinal.pdf (véase página 34).

[16] M. L. Mazurek, S. Komanduri, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, P. G. Kelley, R. Shay y B. Ur, “Measuring password guessability for an entire university”, *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security - CCS ’13*, páginas 173-186, 2013, ISSN: 15437221. DOI: 10.1145/2508859.2516726. dirección: http://dl.acm.org/citation.cfm?doid=2508859.2516726 (véase página 46).

[17] F. Schaub, R. Deyhle y M. Weber, “Password entry usability and shoulder surfing susceptibility on different smartphone platforms”, *Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia - MUM ’12*, número December, página 1, 2012. DOI: 10.1145/2406367.2406384. dirección: http://dl.acm.org/citation.cfm?doid=2406367.2406384 (véase página 40).

[18] F. Schaub, M. Walch, B. Könings y M. Weber, “Exploring the design space of graphical passwords on smartphones”, *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS ’13*, página 1, 2013. DOI: 10.1145/2501604.2501615. dirección: http://dl.acm.org/citation.cfm?doid=2501604.2501615 (véase página 40).

[19] R. Shay, L. F. Cranor, S. Komanduri, A. L. Durity, P. (Huh, M. L. Mazurek, S. M. Segreti, B. Ur, L. Bauer y N. Christin, "Can long passwords be secure and usable?", *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14*, páginas 2927-2936, 2014. DOI: 10.1145/2556288.2557377. dirección: http://dl.acm.org/citation.cfm?doid=2556288.2557377 (véanse páginas 46, 47).

[20] R. Shay, P. G. Kelley, S. Komanduri, M. L. Mazurek, B. Ur, T. Vidas, L. Bauer, N. Christin y L. F. Cranor, "Correct Horse Battery Staple: Exploring the usability of system-assigned passphrases", páginas 1-20, 2012. DOI: 10.1145/2335356.2335366. dirección: http://dl.acm.org/citation.cfm?doid=2335356.2335366 (véase página 46).

[21] T. J. Smoker, C. E. Murphy y A. K. Rockwell, "Comparing Memory for Handwriting versus Typing", *Proceedings of the Human Factors and Ergonomics Society 53rd Annual Meeting*, volumen 1979, número February 1979, páginas 1744-1747, 2009 (véase página 48).

[22] D. Tapellini, *Smart phone thefts rose to 3.1 million in 2013*, 2014. dirección: https://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm (visitado 05-09-2017) (véase página 32).

[23] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin y L. F. Cranor, ""I Added '!' at the End to Make It Secure": Observing Password Creation in the Lab", en *Proceedings of the eleventh Symposium On Usable Privacy and Security*, 2015, páginas 123-140, ISBN: 978-1-931971-249 (véase página 38).

El equipo de informática de la Subsecretaría de Defensa está integrado por (en orden alfabético): Sebastián Araya, Encargado de Redes y Datacenter; Alejandro Hernández, Encargado de Soporte Computacional; Rodrigo Méndez, Encargado de Desarrollo y Explotación de Sistemas; y Carlos Montoya, Jefe de Informática. Nuestros agradecimientos al Sr. Marcos Robledo Hoecker, Subsecretario de Defensa, al Sr. Daniel Álvarez, Asesor en Ciberseguridad y Ciberdefensa, y al Sr. Eugenio Cruz, Jefe de la Unidad de Coordinación Administrativa.

El Manual de Seguridad Digital fue escrito y compilado por Cristian Bravo Lillo (cristian@bravolillo.xyz), Ph.D., Asesor en Ciberseguridad y Ciberdefensa.