

SaferJourno

RECURSOS DE SEGURIDAD DIGITAL
PARA CAPACITADORES DE MEDIOS
DE COMUNICACIÓN



Internews
Local voices. Global change.

Agradecimientos

En primer lugar, queremos expresar nuestro más profundo agradecimiento a **Manisha Aryal** y **Dylan Jones** por la creación, redacción y organización de estos materiales de aprendizaje, que conforman una guía coherente y práctica para capacitadores y alumnos faltos de tiempo. La elaboración y el diseño de estos materiales dan cuenta del compromiso de Manisha Aryal y Dylan Jones con la seguridad en los medios de comunicación y con el trabajo colaborativo.

También nos gustaría expresar nuestro agradecimiento por sus inestimables sugerencias a todos los especialistas en materia de seguridad digital, periodismo y defensa de buenas prácticas que revisaron este proyecto: **Jesse Friedman** (Google), **Dr. Richard R. Brooks** (Clemson University, Carolina del Sur), **Jillian C. York** (Electronic Frontier Foundation), **Chris Doten** (National Democratic Institute), **Shahzad Ahmad** y su equipo (Bytes4All), **Carol Waters** (LevelUp/Internews), y **Brian J. Conley** (Small World News).

La guía *SaferJourno* se puso a prueba en el terreno en un taller para capacitadores que tuvo lugar en Nairobi (Kenya) en diciembre de 2013. Gracias, **Ida Jooste**, directora de Internews en Nairobi, por el apoyo brindado a *SaferJourno*; gracias, **Sandra Ndonge** y **Eva Constantaras**, por la organización del taller de capacitación; y gracias, **Samuel Musila**, por atender, y sobrepasar, nuestras expectativas con respecto a todas y cada una de nuestras peticiones antes, durante y después de la capacitación. Gracias también a todos los capacitadores en materia de periodismo que participaron en el taller de Kenya, cuyas recomendaciones contribuyeron indudablemente a mejorar esta guía.

En el proceso de investigación, los autores de esta guía estuvieron en contacto con los capacitadores en medios de comunicación de Internews y con nuestras organizaciones asociadas que se dedican a la capacitación y la seguridad en los medios de comunicación en Afganistán, Bosnia, Dadaab, Jordania, Kazajistán, Líbano, Pakistán, Palestina, Sudán del Sur y Túnez. Queremos extender nuestro agradecimiento a cada uno de ellos por la generosidad con la que compartieron con nosotros su tiempo y conocimiento.

Internews le agradece a **Gary Garriott** su liderazgo en este proyecto. A los miembros de Internews, que tanto contribuyeron a perfeccionar este proyecto, **Anthony Bouch**, **Jon Camfield**, **Mark Jardina**, **Nicolas Ebnother**, **Oleg Gant**, **Sam de Silva** y **Thomas Chanussot**, muchas gracias por sus aportaciones en el proceso de revisión. Finalmente, nos gustaría darles las gracias especialmente a **Megan DeBlois**, **Tere Hicks** y a todo el equipo del departamento de Iniciativas de Internet de Internews por el apoyo brindado desde el primer momento.

La elaboración de esta guía ha sido posible gracias al apoyo financiero de la Oficina de Democracia, Derechos Humanos y Trabajo del Departamento de Estado de los Estados Unidos, de la Fundación John D. y Catherine T. MacArthur, y de Google Inc.

Creación, redacción y producción: **Manisha Aryal** y **Dylan Jones**

Revisión: **Charlotte Stichter**

Diseño gráfico: **Ashley Low**

Diseño y maquetación: **Kirsten Ankers**

Internews, 2014

Prólogo

En Internews, tenemos la gran suerte de contar con la colaboración de algunos de los mejores periodistas, tecnólogos y profesionales del mundo en los ámbitos de la comunicación y el desarrollo. Los logros más destacados que hemos alcanzado colectivamente radican en materia de educación y de apoyo directo a nuevas generaciones de narradores de historias.

Sin embargo, a la existencia de más oportunidades de investigar e informar gracias a las nuevas tecnologías, se suman nuevos retos. Los riesgos jamás habían sido tales, ni tan complejos y cambiantes como hoy. En este contexto, comprometerse con el aprendizaje continuo es esencial para entender y sacar partido de forma segura del poder de la tecnología y, de esta manera, estar mejor preparados como periodistas.

Este currículo ha sido diseñado y elaborado por dos de los mejores periodistas y profesionales del ámbito de la comunicación, los cuales aportan un amplio conocimiento y vasta experiencia en dicho ámbito y han colaborado con Internews en varios países, que van desde Afganistán hasta Zimbabwe. Estamos muy agradecidos con Manisha Aryal y Dylan Jones por su extraordinario trabajo y liderazgo en esta iniciativa. Juntos han sabido responder a las peticiones de amigos y colegas de todo el mundo en cuanto a la importancia de contar con este currículo para dar respuesta a sus necesidades.

Nos complace presentar esta guía para capacitadores, docentes y periodistas que están haciendo frente a los desafíos de aprender (y enseñar a los demás) cómo protegerse y estar más seguros en Internet en una época de cambios y amenazas para el periodismo.

Kathleen Reen, vicepresidenta del Departamento de Políticas y Programas TIC

Marzo de 2014



Los capacitadores siempre deben asegurarse de que la información incluida en cualquier guía de seguridad está actualizada, ya que a diario surgen novedades tecnológicas, así como nuevas amenazas. Esta guía, publicada en marzo de 2014, ha sido concebida como material de apoyo para capacitadores de medios de comunicación, quienes, por lo general, no tienen acceso a recursos de seguridad o desconocen su existencia. Cabe notar asimismo que la presente guía no sustituye a una capacitación especializada en materia de seguridad impartida por un capacitador calificado.



Índice

USO DE ESTA GUÍA PARA CAPACITADORES	3
1. EVALUACIÓN DE RIESGOS	15
2. MALWARE Y PROTECCIÓN BÁSICA	36
3. PROTECCIÓN DE DATOS	54
4. INVESTIGAR DE MANERA SEGURA	68
5. PROTECCIÓN DE SU CORREO ELECTRÓNICO	84
6. SEGURIDAD PARA TELÉFONOS CELULARES.....	108
GUÍA DE INICIO RÁPIDO: consejos para garantizar la seguridad de teléfonos inteligentes	124
GUÍA DE INICIO RÁPIDO: consejos para garantizar la seguridad de computadoras y cuentas en línea	125

SaferJourno: recursos de seguridad digital para capacitadores de medios de comunicación



CÓMO UTILIZAR LA GUÍA PARA CAPACITADORES

Los seis módulos de *SaferJourno: recursos de seguridad digital para capacitadores de medios de comunicación* están pensados para ayudar a dichos capacitadores a integrar temas relacionados con la seguridad digital y en línea en sus cursos de capacitación. Los módulos no parten de la premisa de que el capacitador tiene conocimientos especializados en la materia.

Si bien elaboramos esta guía pensando en capacitadores en periodismo, creemos que estos mismos módulos también pueden aplicarse a capacitaciones destinadas a todo tipo de comunicadores (ya sean blogueros, reporteros ciudadanos o activistas en derechos humanos que trabajen en el ámbito de la información) que utilicen teléfonos inteligentes e Internet para comunicarse. Es más, la producción de contenidos periodísticos suele ir a cargo de un equipo, formado por fixers, redactores, videógrafos y fotógrafos, quienes también pueden sacar partido de las capacitaciones que integran los recursos de esta guía.

Concretamente, los capacitadores pueden utilizar esta guía de cuatro formas distintas:

- Como material de base para complementar cursos de temáticas periodísticas (por ejemplo, el módulo sobre comunicación segura podría incorporarse a un taller sobre técnicas de entrevistas periodísticas, mientras que el módulo sobre elusión de medidas tecnológicas y el uso de anonimizadores podría formar parte de una capacitación sobre técnicas de investigación, etc.);
- Como material de base de una capacitación de tres días sobre seguridad digital, en la cual se utilizarán todos los materiales que conforman esta guía;
- Como parte del currículo de una capacitación para emergencias (es decir, como respuesta a peticiones o incidentes específicos en el entorno local);
- Como parte de un programa mayor y de mayor duración en materia de capacitación periodística.

Los módulos están pensados para una duración de aproximadamente tres horas cada uno y para poder adaptarse para su aplicación en los cuatro contextos mencionados anteriormente. Sin embargo, recomendamos a los capacitadores que empiecen por el módulo Evaluación de riesgos, independientemente de si se va a impartir el curso en tres días consecutivos o módulo por módulo en el transcurso de varias semanas. Este primer módulo permitirá a capacitadores y a sus alumnos entender los riesgos digitales y físicos presentes en su entorno de trabajo, así como contextualizar el resto de los módulos.

Si bien no esperamos que los capacitadores sean expertos en materia de seguridad digital, sí esperamos que tengan un profundo conocimiento de los medios de comunicación y de Internet de su país o región y que se muestren verdaderamente interesados en temas como la higiene electrónica y la seguridad móvil y en línea.

Estos materiales están concebidos para capacitar a adultos, quienes deberían ser seleccionados para las capacitaciones de las dos formas siguientes: un concurso abierto al público (se difunde información sobre la inscripción al curso y se lleva a cabo un proceso de selección) o un proceso no abierto al público (los organizadores eligen a los participantes después de ponerse en contacto con organizaciones en el ámbito de los medios de comunicación). En ambos casos, tras la selección de los participantes y antes del inicio de la capacitación, los capacitadores deberán empezar a prepararse, teniendo siempre en cuenta las necesidades de estos alumnos adultos.

1. PLAN DE LA CAPACITACIÓN

Malcolm S. Knowles, cuya investigación contribuyó a definir los enfoques modernos sobre el aprendizaje en adultos, escribió en su obra *The Modern Practice of Adult Education: From Pedagogy to Andragogy* [Práctica moderna de la educación para adultos: de la pedagogía a la andragogía], que los adultos aprenden más cuando se responsabilizan de su propio aprendizaje. La andragogía, que proviene del griego *andros* (que hace referencia a “hombre” o “adulto”) y *gogía* (que significa “guía”), es una disciplina distinta a la pedagogía corriente (*paidos* significa “niño”). La andragogía es un modelo de aprendizaje dirigido por el adulto y centrado en el adulto. La teoría de Knowles puede resumirse en cinco principios:

1. Los adultos tienen que entender y aceptar la razón por la cual necesitan adquirir una competencia determinada.
2. La experiencia (también la que deriva del error) constituye la base de las actividades de aprendizaje.
3. Los adultos tienen que participar activamente en la planificación y la evaluación de su aprendizaje.
4. El aprendizaje adulto se basa en la resolución de problemas, en vez de basarse en el contenido.
5. La mayoría de los adultos tienen interés por aprender aquello que tiene una pertinencia inmediata en su vida profesional y social.

SaferJourno: recursos de seguridad digital para capacitadores de medios de comunicación parte de un modelo de aprendizaje basado en la secuencia actividad-debate-información-profundización-síntesis (ADIPS).

Este enfoque andragógico ha demostrado ser muy eficaz en campañas de sensibilización y capacitación sobre asuntos relacionados con los derechos humanos, y hemos constatado que es muy útil para ayudar a alumnos con conocimientos técnicos limitados a entender conceptos tan complejos como la seguridad digital y en línea. A los capacitadores, por su parte, les brinda un útil marco teórico para crear su plan de clase.

El principio rector del enfoque ADIPS radica en que, en adultos, el aprendizaje es más eficaz si la información se presenta en varias fases y distintos formatos (actividades de grupo, estudios de caso, presentaciones audiovisuales y de diapositivas, debates dirigidos, trabajo en equipo, ejercicios prácticos y reflexión). Este enfoque aporta un entorno de aprendizaje integral y tiene en cuenta las necesidades de los alumnos que aprenden kinestéticamente (los que necesitan realizar una acción física para comprender el contenido), visualmente (los que requieren el uso de imágenes, diagramas y videos) o auditivamente (los que aprenden con la ayuda de materiales auditivos, como presentaciones orales).

El enfoque ADIPS

Actividad (familiarización con el tema). Cada módulo empieza con una actividad que ilustra el material que se empleará a continuación. Recomendamos a los capacitadores que empiecen con una actividad de grupo, que tiene la función de romper el hielo entre los participantes y estimula su reflexión sobre un tema que tal vez les es nuevo.

Debate (contextualización del tema). Después de cada actividad, se abre una sesión de debate. Estas sesiones están pensadas para ayudar a los capacitadores a entablar una conversación con los participantes sobre el tema en cuestión y sobre la actividad anterior. Hemos incluido una lista de preguntas y temas de conversación para ayudar a los capacitadores a moderar el debate. Aconsejamos a los capacitadores que adapten estas recomendaciones según su criterio.

Información (sesión interactiva). A pesar de que muchos capacitadores suelen empezar la jornada con una presentación o exposición, aconsejamos que antes de pasar a una presentación de PowerPoint se realicen las dos sesiones previas mencionadas (actividad y debate). Los temas complejos requieren preparación y, gracias a las dos primeras sesiones, los participantes estarán preparados para continuar. Una sesión informativa eficaz debe incluir una gran variedad de materiales, como casos de estudio, que motiven a participantes y capacitadores a compartir conocimientos.

Profundización (actividades prácticas). En capacitaciones en periodismo y seguridad en línea, esta sesión suele incluir la instalación de programas informáticos y la realización de actividades prácticas para aprender a utilizarlos. Esta es, tal vez, la sesión más importante del curso, puesto que los participantes adquieren nuevas competencias al ponerlas en práctica. Sin embargo, tiene que ir precedida de las tres fases anteriores para que los participantes entiendan por qué necesitan adquirir una competencia determinada.

Síntesis (reflexión). Una lección es mucho más útil si se complementa con la práctica y el repaso de lo aprendido. El aprendizaje queda reforzado si se reflexiona sobre los conocimientos adquiridos. En esta sesión, los capacitadores pueden resumir los conocimientos y competencias que se han abordado. Aconsejamos que esta sesión sirva para aclarar dudas y como conclusión. Los capacitadores deben animar a los alumnos a hacer preguntas, aclarar dudas y entender cuáles son los siguientes pasos que tendrán que seguir.

Estamos convencidos de que la secuencia de sesiones descrita permitirá a los participantes convertir lo aprendido en hábito. Los capacitadores pueden servirse de las siguientes preguntas para planificar la capacitación:

- ¿Con qué competencias básicas llegarán los participantes?
- ¿Qué lagunas de aprendizaje tendrán?
- ¿Qué competencias adquirirán los participantes durante la capacitación?
- ¿Cuáles son los objetivos pedagógicos de cada sesión? (es decir, ¿qué se cubrirá en cada sesión?)
- ¿Servirán las sesiones para complementar las competencias que los participantes ya tenían? ¿Estarán relacionadas con su contexto de trabajo?
- ¿Están bien integrados los temas y los subtemas?
- ¿Qué actividades podrían servir para presentar los temas o los subtemas a los participantes?
- ¿Qué ejercicios interactivos y colaborativos pueden ilustrar los puntos principales de cada sesión?
- ¿Qué preguntas pueden ayudar al capacitador a suscitar un debate constructivo?
- ¿Cómo relacionarán los participantes las actividades con los temas principales de la sesión?
- ¿Cómo pueden los participantes profundizar su conocimiento en la materia?
- ¿Incluyen las sesiones ejemplos reales para ilustrar la utilidad de una competencia determinada?
- ¿Qué recursos van a emplearse? ¿Exposiciones? ¿Presentaciones de PowerPoint? ¿Videos?
- ¿Qué pasos se seguirán en los ejercicios prácticos? ¿Cuánto tiempo va a reservarse para estos ejercicios?
- ¿Cuál es la mejor forma de evaluar qué han aprendido los participantes? ¿Tal vez pruebas?
- ¿Cómo podemos aprovechar lo aprendido en una sesión de clase para mejorar otras sesiones posteriores?
- ¿Qué competencias habrán adquirido los participantes al final de la capacitación?
- ¿Cambiarán sus hábitos después de la capacitación?
- ¿Cómo pueden los participantes completar lo aprendido por su cuenta?

2. CARACTERÍSTICAS DE LOS MÓDULOS

A efectos de esta guía, llamamos a cada conjunto de materiales que versan sobre una misma materia *módulo*. Creamos un total de seis módulos que reflejan los problemas a los que más a menudo hacen frente los periodistas. Es probable que publiquemos módulos nuevos, y esperamos que los capacitadores compartan sus propios materiales y plan de clase mediante proyectos de iniciativa comunitaria como [LevelUp](#).

En los casos en los que se imparta la capacitación completa, aconsejamos que los capacitadores sigan el orden establecido de los módulos y empiecen por Evaluación de riesgos. De este modo, los participantes podrán priorizar y aplicar lo aprendido en los módulos siguientes. Como ya hemos mencionado, cada módulo consta de cinco sesiones (Actividad, Debate, Información, Profundización y Síntesis). A fin de sacar el máximo partido de este enfoque, recomendamos a los capacitadores que sigan las sesiones en el orden establecido.

Todos los módulos empiezan con una actividad de grupo (Actividad) a modo de presentación de un concepto clave o para ilustrar una vulnerabilidad de seguridad a los participantes. La segunda sesión del módulo (Debate) tiene como objeto hacer que los participantes debatan sobre el concepto del módulo o la vulnerabilidad en cuestión, específicamente en relación con su trabajo. Estos dos pasos son necesarios para preparar a los participantes para la siguiente sesión (Información), que consiste en una exposición o una presentación audiovisual interactivas.

Una vez que los participantes hayan entendido qué riesgos tienen que tener en cuenta y que hayan adquirido un conocimiento mínimo sobre las estrategias de reducción de riesgos, estarán preparados para aprender las competencias con las que van a garantizar su seguridad (Profundización). Finalmente, la sesión final (Síntesis) resume lo que se ha aprendido en todas las sesiones del módulo. Aunque esta última sesión es de suma importancia, muchas veces hay que prescindir de ella por falta de tiempo. Sin embargo, aconsejamos a los capacitadores incluir esta sesión, puesto que brinda a los participantes una última oportunidad de confirmar lo aprendido con los capacitadores y de reflexionar sobre ello. Además, sirve a modo de conclusión de cada módulo.

Cada módulo incluye los siguientes materiales de apoyo que los capacitadores pueden repartir a los participantes:

- Apuntes de clase (aspectos destacados abordados en clase);
- Glosario (recopilación de vocabulario y términos utilizados en las sesiones);
- Lecturas adicionales (materiales a los que los participantes podrán recurrir para profundizar su aprendizaje).

NOTA: Para los materiales de clase que tratan sobre dispositivos Mac OS X e iOS, cada módulo incluye un apartado adicional con aplicaciones y ejercicios pertinentes. Encontrará estos apartados sobre Mac OS X al final de cada sesión ADIPS de los módulos 2 al 6.

También hemos incluido las siguientes dos guías de inicio rápido (hojas de resumen) sobre seguridad para teléfonos celulares y PC:

- Guía de inicio rápido: *consejos para garantizar la seguridad de teléfonos inteligentes;*
- Guía de inicio rápido: *consejos para garantizar la seguridad de computadoras y cuentas en línea.*

Si bien estas guías de inicio rápido pueden aplicarse a todos los módulos, recomendamos que se repartan a los alumnos para que las consulten después de clase.

3. CONSEJOS PARA CAPACITADORES

Algunos de los consejos que presentamos a continuación se han extraído de [LevelUp](#), un programa de iniciativa comunitaria y liderado por Internews dedicado a capacitadores en el ámbito de la seguridad. Estas recomendaciones serán de gran utilidad para capacitadores en periodismo tanto durante la fase de preparación como durante la impartición de capacitaciones.

Gestión de expectativas

Como capacitador, es importante asegurarse de que los organizadores (la administración o la organización contratante) tienen claro lo que esperan de la capacitación. ¿Podrán obtenerse los resultados esperados? ¿Son los recursos reservados para la capacitación suficientes? ¿Es el número de participantes suficiente? ¿Serán suficientes los días asignados para cubrir todo el temario que se espera que se enseñe? Es muy importante hacerse todas estas preguntas antes del inicio de la capacitación. Hemos preparado un modelo de [Cuestionario previo a la capacitación para los organizadores](#), que los capacitadores pueden modificar y adaptar.

En condiciones óptimas, para que la capacitación se desenvuelva correctamente, los capacitadores deberían contar con la colaboración de un miembro del personal técnico (como el responsable informático, el coordinador técnico u otra persona que entienda de dispositivos electrónicos y software).

A menudo, los participantes llegan con expectativas poco realistas sobre lo que aprenderán en tres días. Una vez que se cierre la lista definitiva de participantes, aconsejamos a los capacitadores que se pongan en contacto con los participantes y les envíen lo siguiente:

- Un mensaje de bienvenida con información sobre la capacitación;
- Un cuestionario que deberán llenar y enviar a los capacitadores antes de que empiece la capacitación, para que estos últimos puedan hacerse una idea del nivel de los participantes y sus expectativas. *(Hemos preparado un modelo de [Cuestionario previo a la capacitación para los participantes](#), que los capacitadores pueden modificar y adaptar.)*
- Lecturas (de una página, como máximo) sobre dos o tres de los temas que se van a tratar en la capacitación. Las lecturas no deben ser artículos extensos, sino más bien documentos de lectura rápida que susciten el interés de los participantes.

(A la fecha de redactar esta guía, proponemos dos artículos, en inglés, de la revista Wired, “[How Apple and Amazon Security Flaws Led to My Epic Hacking](#)” y “[How I Resurrected My Digital Life After an Epic Hacking](#)”, además de un [video de la CNN](#), también en inglés.)

Debemos insistir en la importancia de que capacitadores, participantes y organizaciones tengan presente que para entender y abordar aspectos relacionados con la seguridad digital es necesario actualizarse continuamente. En este sentido, los presentes materiales no presentan conclusiones definitivas:

- Las soluciones en materia de seguridad en Internet nunca son definitivas o permanentes. Los programas y servicios de Internet pueden cambiar sus políticas de privacidad y configuración de seguridad sin previo aviso y, consiguientemente, suponer riesgos potenciales para el usuario.
- Cada día surgen nuevas actualizaciones de seguridad, pero también nuevos virus y malware. Lo que ayer era seguro, puede que hoy sea vulnerable a un ataque. Es necesario permanecer alerta y estar siempre informado y dispuesto a actuar.
- Los capacitadores solo pueden ayudar a los participantes a dar el primer paso, lo cual es fundamental para concientizarse; el resto dependerá de los participantes. Aconsejamos a los capacitadores que insistan en el hecho de que, si bien es cierto que los tres días de la capacitación van a servir para que los participantes se concienticen sobre los peligros digitales y en línea y adquieran nociones básicas sobre las medidas vigentes en materia de reducción de riesgos, a la larga, tendrán que empezar a responsabilizarse de su propia integridad y seguridad digitales.

Preparación de la capacitación

Tamaño de la clase: recomendamos un máximo de 12 participantes y, si es posible, contar con un cocapitador o capacitador auxiliar que ayude a los participantes durante los ejercicios, los simulacros y la instalación de programas informáticos (es decir, 6 alumnos por capacitador). Si se piensa impartir los seis módulos seguidos, aconsejamos que dos capacitadores a tiempo completo se turnen las tareas de capacitador principal y cocapitador para que la energía no decaiga, y que se cubra todo el material en un periodo de tres días. Prolongar la capacitación sería contraproducente: la atención de capacitadores y participantes menguaría, y la eficacia de la capacitación se vería comprometida.

Espacio: las capacitaciones en seguridad digital deben llevarse a cabo en un espacio seguro. Si bien los organizadores son quienes mejor pueden elegir el lugar idóneo, este tipo de capacitaciones exige que los capacitadores estén al corriente de la elección de la sala y, especialmente, de las características de la conexión a Internet. La lista que presentamos a continuación será de gran utilidad para seleccionar el espacio de la capacitación:

- **Equipo:** ¿Dispondré del equipo necesario para la capacitación? Por *equipo* entendemos computadora, equipo audiovisual, proyector, dispositivos multimedia, etc. Si la sala no dispone de estos recursos, ¿Se pueden traer? ¿Habrán suficientes tomas eléctricas para cargar computadoras portátiles?
- **Sala:** ¿Se trata de una sala adecuada para exposiciones, actividades de grupo y demostraciones prácticas? ¿Dónde van a sentarse los participantes? ¿Es flexible la disposición de los asientos? ¿Se podrían cambiar las sillas de lugar? ¿Se podrían incorporar o sacar mesas, en caso de que fuera necesario?
- **Conectividad:** ¿El edificio cuenta con una red Wi-Fi segura? ¿Se podría instalar una red virtual privada, en caso de que fuera necesario? ¿El enrutador inalámbrico es industrial y permite que entre 12 y 15 personas se conecten a Internet simultáneamente? ¿El ancho de banda es de al menos 6 MB / 1.5 MB y permite que varias personas accedan a la Web y consulten su correo electrónico gracias a un enrutador potente? ¿Habrán un encargado de informática, con acceso de administrador, para resolver los problemas de equipo informático, software y conectividad que puedan surgir durante la capacitación?
- **Finalmente, ¡la intuición cuenta!** Si un capacitador no se siente cómodo en una sala y pueden considerarse otras alternativas, recomendamos que dichas alternativas se exploren.

Materiales más frecuentes utilizados en la capacitación

Para la mayoría de las capacitaciones, los organizadores deberían proporcionar los materiales siguientes:

- Proyector LCD y pantalla;
- Marcadores y rotafolios con hojas grandes de papel;
- Pizarrón blanco, marcadores no permanentes y borrador;
- Blocs de notas y plumas;
- Computadoras portátiles o de escritorio;
- Conectividad a Internet con un ancho de banda suficiente para el número de participantes.

Si se decide alquilar el equipo, antes de la capacitación, deberían seguirse los siguientes pasos:

- Comprobar que el software de las computadoras sea legítimo y esté actualizado;
- Comprobar que las computadoras no tengan virus y otras formas de malware;
- Comprobar que el punto de acceso a la red Wi-Fi esté protegido por un cifrado WPA2 y contraseña seguros, y que la contraseña predeterminada del punto de acceso se haya cambiado. (Este paso es muy importante, y tendría que hacerlo el capacitador o el personal de apoyo informático de la entidad organizadora.)

Los capacitadores (y los organizadores) deberían preparar los materiales siguientes:

- Carpetas en línea que contengan el horario, el programa, la metodología a seguir, las lecturas y los documentos impresos que se van a repartir, hojas de ejercicios, los formularios de evaluación de la capacitación, breves semblanzas biográficas de capacitadores y participantes, y un documento con los datos de contacto de organizadores, capacitadores y participantes. Los dos últimos elementos de la lista son opcionales, ya que algunos participantes no querrán dejar constancia de su información personal por motivos de seguridad. Dropbox y Google Drive parecen ser las herramientas más utilizadas.
- Ejemplares impresos de guías más recientes sobre seguridad digital. Recomendaciones:
 - *Manual de Seguridad para Periodistas* del Committee to Protect Journalists (Comité para la Protección de los Periodistas);
 - *SpeakSafe*, de Internews;
 - *Threatsaurus*, de Sophos. Incluye Security in-a-box, de Tactical Technology Collective y Front Line Defenders. (link = <https://securityinabox.org>).
- Memorias USB (una para cada participante) con software, programas y lecturas, así como un documento que exponga brevemente el contenido de la memoria USB. (Si los capacitadores prefieren distribuir los programas informáticos en un único dispositivo, que los participantes tendrán que ir pasándose, recomendamos el uso de un CD, porque no es vulnerable a infecciones de virus.)

Los participantes pueden traer los siguientes materiales:

- Computadoras personales (opcional);
- Celulares o tabletas que utilicen para trabajar.

Seguridad de los participantes

Los capacitadores tendrán que realizar su propia evaluación de riesgos cuando impartan capacitaciones a participantes que vivan en contextos de alto riesgo, donde se monitorea constantemente a periodistas y profesionales de la comunicación. En estas circunstancias, es importante establecer protocolos de comunicación con los organizadores y los participantes antes, durante y después de la capacitación. Esto podría requerir que se llevaran a cabo algunos de los siguientes pasos (o todos ellos):

- Designar a una persona de la organización para que se encargue de comunicarse con los participantes;
- No difundir la lista de participantes ni los nombres de capacitadores y organizadores en línea;
- Garantizar que la información personal de los participantes (número de pasaporte, dirección, etc.) no se guarde en línea y se archive de forma segura;
- No poner en contacto entre sí a los participantes sin previo consentimiento expreso;
- Evitar el uso de direcciones de correo electrónico pertenecientes a una organización.

Formalización de un contrato

En el contexto del aprendizaje en adultos en general, y en el de esta capacitación en concreto, la relación entre capacitador y alumno tiene que basarse en la colaboración, donde la confianza y el respeto mutuos son factores clave. Las dos partes son adultos y cuentan con un gran bagaje de experiencias, competencias, conocimientos y motivaciones. La capacitación en materia de seguridad digital aborda temáticas y problemáticas delicadas y podría suponer riesgos para participantes, organizadores, capacitadores y donantes.

En el marco de la capacitación también se tienen que establecer ciertas pautas de conducta aceptable. Tras llegar a un consenso, dichas pautas pueden colgarse en la sala de la capacitación y distribuirse a los participantes (pueden incluirse en sus carpetas). Estas pautas deberían incluir los siguientes aspectos (se trata de una lista no exhaustiva):

- **Horario:** Acuerdo sobre la duración de las sesiones, hora de inicio y de fin. Deberían incluirse los descansos y la hora del almuerzo. El horario puede ser flexible y puede variar de un día a otro, pero una vez que se llegue a un acuerdo, hay que respetarlo.
- **Asistencia:** Los participantes tienen que asistir física y mentalmente a todas las sesiones. Esto significa que no pueden estar navegando por Internet, consultando correos electrónicos o publicando entradas en redes sociales durante las sesiones. Los participantes pueden tener los celulares en silencio durante la capacitación para que les lleguen llamadas y mensajes, que podrán responder en otro momento.
- **Publicación del contenido de la capacitación:** Los talleres de seguridad digital para profesionales y activistas de comunicación no suelen ser oficiales. Sin embargo, si la capacitación no supone ningún riesgo para organizadores, participantes y capacitadores, puede aplicarse la [regla de Chatham House](#) [en inglés], que estipula lo siguiente: “Cuando una reunión, o parte de ella, se lleva a cabo en virtud de la regla de Chatham House, los participantes son libres de utilizar la información recibida, pero no pueden revelar la identidad ni la afiliación de los oradores ni de ningún otro participante”. En relación con las redes sociales,

la regla estipula que se puede publicar o tuitear lo que se dijo en un evento sin identificar al orador o a cualquier otro participante.

- **Seguridad:** La seguridad de todas las personas que participen en el taller (alumnos, capacitadores, organizadores y donantes) es muy importante. Los participantes tienen que comprometerse a no hacer nada que pueda suponer riesgos o vulnerabilidades para otros participantes, organizadores, capacitadores y donantes.
- **Descargas:** Los participantes no pueden monopolizar el ancho de banda de la clase. Por lo tanto, tendrán que desactivar cualquier programa torrent y, en tanto que no formen parte del contenido de la clase, aplicaciones como Dropbox, Google Drive o OneDrive, ya que generan mucho tráfico. También tendrán que cerrar las aplicaciones de redes sociales como Facebook, Twitter y Skype, ya que reciben alertas y otras fuentes de distracción de forma constante.
- **Respeto:** Tratar a los demás con respeto y asumir que la responsabilidad de aprender recae sobre uno mismo son dos normas intocables que deben aceptarse antes de empezar la capacitación. Es importante que los participantes lleguen a un acuerdo sobre qué consideran una conducta adecuada y concreten los detalles de las dos normas mencionadas, lo que fomentará el interés de los participantes por la capacitación y por su propio proceso de aprendizaje.

El conjunto de pautas consensuadas por todos conformará un contrato que tanto participantes como capacitadores utilizarán antes, durante y después de la capacitación.

Horario

Los módulos que presentamos a continuación están pensados para sesiones de entre tres y tres horas y media, con un descanso de 15 o 20 minutos para estirar las piernas, ir al baño o comer algo. Aconsejamos a los capacitadores que les recuerden a los participantes que también pueden dedicar estos minutos a consultar el correo electrónico, con el fin de evitar que lo hagan durante el tiempo de clase.

Como ya hemos señalado, los módulos se basan en el enfoque ADIPS y siguen el siguiente formato:

Sesión 0: Bienvenida, cuestiones de organización y reglas del curso

De 00:00 a 00:30	Presentación y expectativas
De 00:30 a 01:30	Normas del curso (debate y consenso)

Sesiones 1 a 6: Enfoque ADIPS aplicado a la seguridad digital

De 00:00 a 00:15	Actividad (15 minutos)
De 00:15 a 00:30	Debate (15 minutos)
De 00:30 a 01:00	Información, presentación interactiva, preguntas y respuestas (30 minutos)
De 01:00 a 01:15	Descanso (15 minutos)
De 01:15 a 02:45	Profundización (90 minutos)
De 2:45 a 03:00	Síntesis (15 minutos)

Sesión 7: Conclusión

De 00:00 a 00:30	Sesión de retroalimentación con preguntas abiertas, en círculo cerrado
De 00:30 a 01:30	Evaluación de la capacitación, debate sobre los siguientes pasos a seguir

4. MEJORES PRÁCTICAS

A continuación, presentamos algunos principios en materia de capacitación que creemos que contribuirán a que las sesiones sean más eficaces. Puede leer los comentarios, consejos y recomendaciones de otros capacitadores sobre temas relacionados con la seguridad digital en la página web de seguridad comunitaria [LevelUp](#) [en inglés], de donde hemos extraído algunos materiales.

Compromiso de continuar aprendiendo

¡Las herramientas tecnológicas cambian constantemente! Esta guía complementa las iniciativas de Internews [SpeakSafe](#) y [LevelUp](#), y se redactó en diciembre de 2013.

Dado que el surgimiento de nuevas herramientas tecnológicas va acompañado inevitablemente de nuevas amenazas y vulnerabilidades, los capacitadores no pueden limitarse únicamente a esta guía, sino que deben actualizarse continuamente. Una serie de colectivos, entre los cuales se encuentran el [Tactical Technology Collective](#), el [Comité para la Protección de los Periodistas](#), [Reporteros Sin Fronteras](#) y la [Medill School of Journalism](#), de la [Northwestern University](#), han elaborado guías sobre seguridad digital para periodistas. Es recomendable guardar sus páginas web como favoritas y consultarlas periódicamente.

A diferencia de los capacitadores de periodistas del siglo pasado, que iban a sus talleres sobre medios de comunicación impresos con una serie de apuntes bien estudiados y ejemplos bien conocidos, los capacitadores de hoy en día tienen que conocer el contexto técnico y los medios de comunicación con los que trabajan sus alumnos y comprometerse a estar al día en materia de nuevas herramientas e innovaciones pertinentes. A continuación, encontrará fuentes magníficas (en inglés) para estar al día sobre las libertades relativas a los medios de comunicación:

- Dos informes de la Freedom House (que se actualizan anualmente): [Freedom on the Net](#) [Libertad en la red] y [Freedom of the Press](#) [Libertad de prensa];
- [Índice de libertad de prensa](#), de Reporteros Sin Fronteras;
- [Índice de impunidad](#), del Comité para la Protección de los Periodistas.

Aconsejamos que los capacitadores lean blogs especializados, sigan a los líderes de la industria en Twitter, hagan aportaciones en foros en línea y se unan a grupos de Facebook para estar al corriente de noticias, tendencias y novedades. Una buena forma de estar al día es mediante [Liberationtech Listserv](#), del [Centro para la Democracia, el Desarrollo y el Estado de Derecho](#) (Center on Democracy, Development and the Rule of Law), de la [Universidad de Stanford](#). Listserv es un foro destinado a personas e instituciones que trabajan en iniciativas de Internet como plataforma abierta (*open Internet*). Los debates de este foro versan sobre los puntos fuertes y las vulnerabilidades de las herramientas digitales. Dichos debates se almacenan en los [Archivos de Liberationtech](#).

Otros recursos (en inglés) recomendados para capacitadores:

- [ArsTechnica Security](#);
- [Página de resumen de noticias del SANS Institute](#);
- [The Krebs on Security](#), página web de Brian Krebs, experiodista del [Washington Post](#).

Finalmente, recomendamos a los capacitadores que dediquen tiempo periódicamente a expandir su conocimiento. Estar al día requiere asumir un compromiso.

Utilización de software de código abierto

La guía [SaferJourno](#) apuesta, en la medida de lo posible, por el uso de software, programas y herramientas de código abierto. Las herramientas de código abierto son fáciles de descargar y permiten el acceso a sus códigos fuente a todo aquel que desee verlos, copiarlos, modificarlos o compartirlos. Además, suelen ser gratuitas. Las aplicaciones de código abierto pueden ser modificadas por el público y hacen posible que usuarios y desarrolladores de software las prueben, detecten y corrijan errores, y detecten vulnerabilidades.

En el ámbito de los recursos de seguridad digital y en línea, las herramientas de código abierto ocupan un lugar cada vez más importante, dado que las desarrollan personas e instituciones que desean que la comunidad de usuarios prueben los códigos en distintos contextos de seguridad. Actualmente, muchos desarrolladores de software apuestan por el código abierto, y, gracias a su empeño, hoy es posible contar con alternativas de código abierto a cualquier herramienta de código cerrado o patentado, desde sistemas operativos hasta plataformas en línea, pasando por todo tipo de aplicaciones.

Este proceso de desarrollo de herramientas de código abierto, liderado por los propios usuarios y basado en iniciativas comunitarias, constituye una razón de peso para utilizarlas. Ciertamente, la escritura de códigos es una labor llevada a cabo por un grupo relativamente reducido de personas. Sin embargo, gracias a la inteligencia colectiva de muchos usuarios que comparten su experiencia personal y dedican tiempo a mejorar las herramientas de código abierto al probarlas en distintos contextos, introducir enmiendas, modificar pequeños detalles y eliminar errores, la industria

del código abierto brinda oportunidades prometedoras en el ámbito de la comunicación. Para más información, vea el video *What is Open Source?* [¿Qué es el código abierto?] o lea el artículo “Benefits of Open Source Software” [Los beneficios del software de código abierto]. Si le interesa obtener más información sobre los puntos fuertes y débiles en materia de seguridad del software de código abierto, le recomendamos la entrada de Wikipedia (una enciclopedia de código abierto) “Open-source Software Security” [Seguridad del software de código abierto].

Mitigación de riesgos

Presentar los peligros del mundo de Internet es un gran reto, puesto que los riesgos son virtuales y, por lo tanto, no son tangibles. Es por eso por lo que la mayoría de los participantes solo llegan a concebirlos cuando han sido víctimas de un ataque, y es esta la razón por la cual muchos capacitadores especialistas en seguridad empiezan la jornada pirateando la cuenta del sistema o de la red social de alguien. Esta estrategia permite estimular la reflexión sobre los riesgos y los peligros de manera mucho más eficaz que mediante una exposición. Otra forma de suscitar el interés de los participantes consiste en contar anécdotas o exponer casos de estudio en los cuales reporteros o activistas han corrido riesgos por culpa de prácticas inseguras en Internet.

Sin embargo, todo capacitador debe saber cuándo parar: sembrar el pánico suele generar un sentimiento de impotencia entre los participantes. Si sienten que la problemática que se les presenta está fuera de su alcance, es posible que se paralicen y no puedan concentrarse en las soluciones. El objetivo de las capacitaciones en seguridad digital es sensibilizar a los participantes sobre los riesgos para que los tengan siempre presentes a la hora de utilizar Internet. Por regla general, los capacitadores deben recordar que por cada peligro presentado habrá que equipar a los participantes con, al menos, una solución o una estrategia técnica. Hay que tener en cuenta que aunque no siempre exista una solución para un riesgo dado, siempre habrá estrategias y tácticas que los participantes podrán aplicar para mitigar los riesgos que enfrentan.

Simplificación de la jerga

Una jerga es un idioma secreto compartido por un grupo de expertos en una materia determinada. Es un código que permite abreviar conceptos complejos y expresarlos en una sola palabra o enunciado. En una capacitación técnica se manejarán términos y conceptos específicos que los participantes desconocerán. El trabajo del capacitador es utilizar la jerga (y no evitarla), pero acompañándola de una explicación e ilustrándola con metáforas e historias.

Por ejemplo, cuando se expliquen los usos de la privacidad bastante buena (*pretty good privacy*) o de otros tipos de cifrado de protección de cuentas de correo electrónico, se puede describir el proceso estableciendo un paralelismo con objetos cotidianos (como meter un carta en una caja cerrada con llave), antes de presentar la explicación técnica.

Cómo estimular la participación

Hasta cierto punto, no se puede evitar que una capacitación incluya exposiciones (es decir, formas de comunicación unidireccional en las que el capacitador habla sobre un tema específico que conoce y luego responde las preguntas de los participantes). Es importante que los capacitadores tengan en cuenta que no pueden estructurar la exposición en forma de monólogo. A continuación presentamos algunos consejos para que las presentaciones no se conviertan precisamente en monólogos:

- **Planee en qué puntos va a detenerse antes de empezar.** Una exposición con pausas (momentos en los que el capacitador deja de hablar y atiende a preguntas de los participantes) fomentará la interacción.
- **Preste atención al nivel de energía de los participantes.** Algunos indicadores de cansancio:
 - **Los participantes asienten con la cabeza.** Este gesto no siempre significa que los participantes están de acuerdo con todo lo que dice el capacitador, sino que también puede ser indicio de que han dejado de prestar atención y simplemente asienten con la cabeza porque no quieren que se note. (Para comprobarlo, el capacitador puede hacer preguntas a quienes hagan este gesto repetidamente. Si se muestran confundidos, es probable que no hayan estado escuchando con atención.)
 - **Signos de distracción.** Dar golpecitos en el suelo con los pies, jugar con la pluma o el cabello o mirarse las uñas son gestos que pueden señalar pérdida de interés.
- **Al detectar indicios de cansancio, el capacitador debe dejar de hablar y empezar a hacer preguntas.** Si el nivel de energía del grupo es bajo y los participantes no están prestando atención, un breve descanso o una actividad estimulante pueden ser el remedio.

Preparación de las presentaciones

Muchos capacitadores tienen la costumbre de utilizar presentaciones en todas las capacitaciones. La ventaja de utilizar PowerPoint, Prezi u otros programas similares en una capacitación es innegable: una presentación visual puede servir para abordar diferencias del lenguaje utilizado y para ayudar a los participantes a ubicarse. Sin embargo, las presentaciones también pueden ser una herramienta de enseñanza ineficaz por su naturaleza poco interactiva. En los casos en los que sea oportuno utilizar una presentación visual, esta tiene que incorporar espacios de debate para que los participantes puedan hacer preguntas.

- En una sesión de 90 minutos, la presentación no puede exceder los 10 minutos ni las 7 diapositivas.
- No lea la presentación, ya que esta tiene la función de apoyar lo que está presentando. No es recomendable llenar las diapositivas de texto.
- Diseñe las diapositivas con una o varias preguntas finales que le ayuden a dejar de hablar. Las presentaciones PowerPoint deben tener el objetivo de suscitar debates.

El valor del aprendizaje práctico

Las actividades prácticas constituyen la base de toda capacitación técnica. Se aprende mucho más cuando uno hace algo (en este caso, instalar y utilizar nuevos programas informáticos que protegerán la seguridad de los participantes). Tal vez algunos participantes no se defiendan con la computadora tanto como otros. En estos casos, los capacitadores deberán evitar a toda costa agarrar el mouse del alumno para demostrarle qué tiene que hacer. Si se priva a los participantes de aprender ellos mismos experimentando, la actividad pasa a ser un obstáculo de aprendizaje. La mejor forma de ayudar a estos participantes es que el capacitador se sitúe detrás de ellos durante la actividad práctica y los vaya orientando, en vez de apoderarse del mouse.

- **Las actividades prácticas que mejor funcionan se llevan a cabo con un equipo de capacitadores.** La estructura ideal consiste en tener a un capacitador delante de la clase que demuestre los pasos del ejercicio (lo que tiene en su computadora puede proyectarse en otra pantalla) y uno o varios capacitadores (o capacitadores auxiliares) que se paseen por la sala y ayuden a los participantes mientras van completando los pasos.
- **No explique el ejercicio, demuestre cómo se hace.** El capacitador debe demostrar cómo hacer el ejercicio primero y después pedir a los participantes que instalen o desinstalen un programa dado. Finalmente, el capacitador tiene que revisar el trabajo de los participantes. Puede colocarse un proyector para que todos los participantes vean la pantalla del capacitador. Es recomendable contar con varios capacitadores auxiliares que les ayuden a completar los pasos y que les pregunten si están siguiendo el ejercicio. Preguntas como “¿Ves esto en tu pantalla?” o “¿Pasa esto cuando activas esta casilla?” es una buena manera de saber quién está siguiendo la demostración y quién se ha perdido.

¡A divertirse!

Finalmente, el objetivo de compartir conocimientos es ayudar a los demás. Cada persona puede aprender en formatos y estilos muy distintos, pero el deseo de divertirse es universal. Si los participantes se van con la sensación de haber asistido a un taller divertido, donde han aprendido cosas nuevas, el capacitador habrá cumplido su cometido.

Manisha Aryal y Dylan Jones

SaferJourno: recursos de seguridad digital para capacitadores de medios de comunicación es un proyecto de Internews que complementa el trabajo hecho en [SpeakSafe](#) y [LevelUp](#). Creado y compartido bajo [licencia Creative Commons Attribution-NonCommercial 3.0 Unported \(CC BY-NC 3.0\)](#).

CUESTIONARIO PREVIO A LA CAPACITACIÓN PARA LOS ORGANIZADORES

Recomendamos a los capacitadores que adapten las siguientes preguntas en función de los objetivos de la capacitación. No todas las preguntas serán pertinentes o necesarias para todas las capacitaciones, y algunas capacitaciones requerirán preguntas adicionales.

NOTA: Recomendamos que se reparta el cuestionario en persona para evitar el uso de métodos menos seguros.

1. ¿Han asistido los participantes a alguna capacitación en materia de seguridad digital anteriormente?
2. ¿Tienen los participantes acceso a un técnico que les pueda ayudar a utilizar herramientas de seguridad digital fuera de clase?
3. ¿A algún miembro de su organización le han robado o confiscado algún dispositivo electrónico?
¿Algún miembro ha perdido un dispositivo electrónico con información delicada?
4. ¿Ha sido su organización víctima de un ciberataque (virus, pérdida de datos, interceptación de comunicación, pirateo de una cuenta de correo electrónico o de una red social o bloqueo de una página web)? En caso afirmativo, describa brevemente el ciberataque experimentado.
5. ¿Sabe si su organización ha sido vigilada en algún momento?
6. ¿Proporcionará su organización computadoras portátiles para todos los participantes?
7. En caso afirmativo, ¿comprobarán que las computadoras no tienen virus ni malware antes de la capacitación?
8. ¿Qué sistemas operativos utilizarán los participantes? ¿Se trata de sistemas operativos legítimos?
9. ¿Se ofrecerá conexión a Internet durante la capacitación?
10. En caso afirmativo, ¿se compartirá la conexión a Internet con el personal de su organización?
11. ¿Permitirá dicha conexión la emisión en *streaming* de videos de YouTube que el capacitador empleará a modo de demostración?
12. ¿Está la red Wi-Fi protegida por una contraseña?
13. En caso afirmativo, ¿está el punto de acceso a la red Wi-Fi protegido con un cifrado WPA2 que garantice la seguridad de los participantes?
14. ¿Dispondrán todos los participantes de un teléfono inteligente?
15. ¿Qué marcas de teléfono y qué tipo de red utilizarán los participantes?
16. ¿Está el uso de cifrado permitido legalmente? (¿Se prohíbe el uso de VPN o de software con cifrado de datos almacenados en la PC?)

Cuestionario que el capacitador debe hacer llegar a los ORGANIZADORES

CUESTIONARIO PREVIO AL CURSO PARA LOS PARTICIPANTES

Recomendamos a los capacitadores que adapten las siguientes preguntas en función de los objetivos de la capacitación. No todas las preguntas serán pertinentes o necesarias para todas las capacitaciones, y algunas capacitaciones requerirán preguntas adicionales.

NOTA: Recomendamos que se reparta el cuestionario en persona para evitar el uso de métodos menos seguros.

1. ¿Utiliza PC (o Mac) o dispositivos móviles en su trabajo periodístico?
2. En caso de que el celular o la tableta sea su herramienta de comunicación periodística principal, ¿qué marca, modelo y sistema operativo utiliza? (¿iOS? ¿Android?)
3. ¿Cuál es el sistema operativo de su computadora? (¿Windows? ¿Mac OS?)
4. ¿Cómo suele conectarse a Internet? (¿desde la red Wi-Fi de la oficina? ¿desde casa? ¿desde un cibercafé?)
5. ¿Qué navegador web suele utilizar?
6. ¿Qué buscador suele utilizar para buscar información en línea?
7. ¿Se pone en contacto o entrevista a sus fuentes mediante programas de chat por voz, video o texto? (En caso afirmativo, especifique qué programas suele utilizar: Skype, Google Chat, etc.)
8. ¿Sabe lo que es una conexión SSL? ¿Sabe qué diferencia hay entre un servidor HTTP y uno HTTPS?
9. ¿Ha utilizado alguna vez herramientas de privacidad como VPN o Tor?
10. ¿Está el disco duro de su computadora protegido por una contraseña?
11. ¿Utiliza a veces su cuenta de correo electrónico personal en el trabajo?
12. ¿Utiliza Facebook, Twitter u otras redes sociales? En caso afirmativo, ¿cuáles?
13. ¿Le han robado o confiscado un dispositivo electrónico alguna vez?
14. ¿Tiene acceso a especialistas técnicos cuando le surgen dudas sobre prácticas y herramientas de seguridad digital?
15. ¿Ha asistido alguna vez a una capacitación en materia de privacidad? En caso afirmativo, ¿qué temas abordó dicha capacitación?
16. ¿Qué temas le gustaría que abordara esta capacitación?
17. ¿Piensa traer su computadora portátil a la capacitación?
18. ¿Piensa traer su teléfono inteligente a la capacitación?

Cuestionario que el
capacitador debe
hacer llegar a los
PARTICIPANTES

1. Evaluación de riesgos



IMPORTANCIA DEL TEMA

Los periodistas manejan en su día a día información delicada y dispositivos que contienen dicha información. Pocos han considerado los riesgos que se corren en lo que a dicha información y dispositivos se refiere, así como las posibles consecuencias de perderlos por robo, decomiso o catástrofe natural.

La evaluación de riesgos es un proceso sistemático en el que se hace inventario de los activos físicos y digitales, se identifican los niveles de riesgo y las vulnerabilidades, y se diseña un plan para afrontarlos. El presente módulo incluirá algunas herramientas para evaluar amenazas digitales y físicas, y motivará a los participantes a tener en cuenta lo siguiente:

- La importancia de su trabajo y la información de la cual dependen para hacer su trabajo (p.ej., contactos);
- Hábitos propios que pueden poner en peligro su trabajo;
- Un nivel de seguridad y privacidad en la oficina que sea práctico.

LO QUE APRENDERÁN LOS PARTICIPANTES

Ideas: evaluación de riesgos, planes de seguridad.

Competencias: métodos básicos para evaluar riesgos comunes, digitales y físicos, relativos a datos utilizados en el entorno laboral.

OBJETIVOS

Aprender a identificar y priorizar riesgos

APLICACIONES PRÁCTICAS

Identificar y proteger datos y equipos con información delicada

CONOCIMIENTOS PREVIOS EXIGIDOS

Para el presente módulo no se requieren conocimientos técnicos previos



NOTA PARA LOS CAPACITADORES

Para encontrar soluciones a los retos relativos a la integridad digital, hay que empezar por ser conscientes de los riesgos. Por ello, recomendamos que los capacitadores piensen en comenzar por dictar este módulo antes de pasar a los demás temas. Aunque los periodistas enfrentan diferentes tipos de riesgos en su día a día, el presente módulo se limita a los riesgos para dispositivos y conexiones digitales.

ANTES DE COMENZAR

Los recursos que se enumeran a continuación podrían ayudar a los capacitadores a mejorar sus conocimientos acerca del tema del presente módulo antes de comenzar a dictarlo:

- Guía: *Proteger tu información de amenazas físicas* (Security in-a-box);
- Guía: Evaluación de amenazas y el círculo de seguridad en *Seguridad y Privacidad Digital para los Defensores de los Derechos Humanos* (Equalit.ie);
- El Proyecto SSD: *Risk Management* [Gestión de riesgos] (EFF.org).



MATERIALES

Además de los materiales de capacitación que recomendamos normalmente en la *Guía para capacitadores*, (véase el apartado “Consejos para la capacitación”), los capacitadores necesitarán lo siguiente para esta lección:

Documentos impresos a repartir

- Apuntes de clase
- Glosario
- Planilla de evaluación: [entorno físico](#)
- Planilla de evaluación: [integridad digital](#)
- Instrucciones: How to Protect Your Information from Physical Threats [Cómo proteger su información de amenazas físicas] (Security in-a-box).

Personal

- Recomendamos que los capacitadores informen al personal de apoyo informático de las organizaciones que participan en la capacitación para que estén presentes (para responder preguntas) cuando se dicte este módulo, particularmente durante la sesión de la [Actividad](#) y la sesión de [Profundización](#).



MÓDULOS RELACIONADOS

- Como se mencionó anteriormente, recomendamos que el presente módulo se dicte antes que los otros módulos de esta guía, de manera que los participantes entiendan todos los riesgos a los que hacen frente los periodistas.
- Algunos capacitadores querrán dictar este módulo junto con el módulo de [Malware y protección básica](#) puesto que, combinados, abordan una amplia gama de riesgos comunes y sus soluciones.
- Otros módulos de integridad digital pueden aportar consejos útiles para mitigar o eliminar las amenazas digitales que identifiquen los participantes durante el presente módulo.

RECORDATORIO

Si el presente módulo es el primero de un taller más amplio, sugerimos que los capacitadores dediquen los primeros 10 minutos a trabajar con el grupo para definir los lineamientos de conducta y seguridad. Para más información, véase el apartado “Formalización de un contrato” de la *Guía para capacitadores*.

PLAN DE CLASE



1. ACTIVIDAD (20 MINUTOS)

En busca de riesgos

La presente actividad invita a los participantes a explorar una sala de simulación o un espacio “arriesgado” (es decir, un lugar reservado del espacio donde se llevará a cabo la capacitación o un lugar aparte) para identificar posibles riesgos para los equipos y los datos. En esta actividad, el espacio tendrá que haberse preparado previamente y el capacitador tendrá una lista de los riesgos que se han dejado allí intencionalmente para que los encuentren los participantes.

Preparación

Antes de comenzar la clase, el capacitador prepara dicho “espacio arriesgado” con varios riesgos que se dejan a la vista intencionalmente y que pueden incluir los siguientes:

- Ventanas abiertas;
- Puerta con la llave colgando de la cerradura;
- Computadora(s) portátil(es) en un escritorio, sin cable de seguridad contra robos;
- Alambres o cables para dispositivos, esparcidos por el piso donde alguien tendría que pasar encima de ellos;
- Enchufes colgando de un contacto múltiple cerca de algún papel;
- Cajones abiertos, con un disco duro externo expuesto;
- Contraseñas escritas en una nota autoadhesiva o en un papel pegado al monitor o a la superficie del escritorio con cinta pegante;
- Un bolso abierto con un teléfono inteligente, una cámara u otro dispositivo de valor a la vista;
- Una unidad flash que hayan dejado en el puerto USB de una computadora;
- Una computadora desatendida con aplicaciones como Outlook, Gmail, Skype u otra aplicación de comunicación activa, abierta y visible;
- Computadoras(s) portátil(es) en un escritorio, sin cable de seguridad contra robos.

NOTA: Se trata tan solo de una lista de sugerencias, que se puede modificar para adaptarse a las necesidades de los participantes y a potenciales hábitos arriesgados que los capacitadores quieran resaltar.

Cómo organizar la actividad

Al inicio del ejercicio, el capacitador explicará que el objetivo del módulo es conocer formas de identificar riesgos para periodistas y sus dispositivos electrónicos. Puesto que a menudo los periodistas deben ser buenos investigadores, esta actividad será perfecta para ellos. Después, el capacitador hará lo siguiente:

- Invitará a los participantes a caminar hasta el lugar preparado o en torno al mismo (o a ver una fotografía) durante cinco minutos y tomar nota de los riesgos que identifiquen.
- Organizará a los participantes en grupos de dos o tres y les pedirá que trabajen juntos y compartan sus conclusiones y que después tomen cinco minutos para escribir sus observaciones en una hoja de papel rotafolio.
- Les recordará a los participantes que algunos riesgos serán evidentes, mientras que otros tal vez no lo sean para todos los miembros del equipo, y los animará a hablar entre sí para intercambiar sus puntos de vista.
- Cuando falten 10 minutos para concluir la actividad, les pedirá a los equipos que se turnen para presentar su lista de riesgos y explicar por qué cada elemento de la lista puede suponer un riesgo.
- Se tomara unos minutos para señalar riesgos puestos allí intencionalmente y que el grupo no haya identificado.

MATERIALES ADICIONALES

- Papel rotafolio;
- Marcadores;
- Un espacio designado como “espacio arriesgado” (es decir, un espacio que presente riesgos);
- Equipos y muebles para usarlos en dicho “espacio arriesgado”.

NOTA: No es indispensable que los muebles sean idénticos a los de los lugares de trabajo de los participantes, pero a mayor parecido con un espacio de trabajo real, más probabilidades de que se aproveche bien la actividad.

Alternativas

1. En casos en los que no haya suficiente tiempo o espacio para el “espacio arriesgado”, el capacitador podrá sustituir esta actividad por otra llamada “*Un día en la vida de*”, que puede encontrarse en el sitio web de [LevelUp](#).
2. En casos en los que los participantes pertenezcan a la misma organización de medios de comunicación y el evento se lleve a cabo en sus oficinas, los capacitadores podrán optar por dividir la clase en grupos y pedir a los participantes que evalúen su entorno laboral de siempre. Esto motivará a los participantes a ver con otros ojos un entorno que les es familiar y les aportará un beneficio práctico e inmediato a los organizadores del evento.



2. DEBATE (10 MINUTOS)

A menudo, la actividad de identificar riesgos que vimos anteriormente da lugar a un largo debate cuando los equipos se turnan para presentar sus conclusiones. Sin embargo, si sobra tiempo, los capacitadores tal vez quieran que los participantes se sienten en círculo o en medio círculo para poder dirigirse los unos a los otros. Las preguntas que presentamos a continuación pueden ser útiles para dar inicio al debate. Los capacitadores tienen plena libertad para añadir elementos a la lista o improvisar según lo estimen oportuno.

Como siempre, los capacitadores deberían animar a cada quien a expresar su punto de vista. Es probable que no todos los participantes hayan reflexionado a conciencia sobre los puntos de debate. Este ejercicio mostrará por primera vez a los participantes algunas prácticas interesantes y fomentará un fructífero debate.

- ¿Hay algún aspecto de este ejercicio que le haya recordado su oficina o espacio de trabajo? ¿Se parecía? ¿Era muy distinto? ¿En qué sentido se parecía o era distinto?
- ¿Por qué cree que son comunes los riesgos de este tipo en salas de prensa o en espacios de trabajo?
- ¿Cree usted que estos riesgos solo afectan a la persona que usa el espacio de trabajo? ¿En qué sentido?
- ¿Qué tipo de riesgos existen en espacios públicos? ¿Ha visto usted riesgos similares en cibercafés, por ejemplo?
- Conoce casos en los que:
 - ¿Se vio comprometida la seguridad personal de un periodista? ¿Sabe qué sucedió?
 - ¿Se vieron comprometidos los bienes o los datos de un periodista? ¿Cómo sucedió?
- ¿Qué clase de precauciones toma para velar por su integridad física o la integridad de su trabajo?
- ¿Alguien de este grupo ha llevado a cabo una evaluación de riesgos? En caso afirmativo, pídale a la persona que le explique cómo llevó a cabo dicha evaluación.

Los capacitadores tienen plena libertad para añadir elementos a la lista o improvisar según lo estimen oportuno.



3. INFORMACIÓN/EXPOSICIÓN (30 MINUTOS)

La siguiente sesión incluye estudios de caso recomendados, ideas clave y algunos materiales para ayudar a transmitir la idea que se está abordando.

Estudios de caso

Los estudios de caso que se mencionan a continuación analizan los riesgos a la integridad digital que no se hayan contemplado en la actividad de apertura ("En busca de riesgos") y que se incluyen para concientizar a los participantes sobre una serie más amplia de retos.

A. Compartir archivos puede poner vidas en peligro

Presentación: Como periodistas, investigamos y compartimos información constantemente. Incluso a medida que tomamos precauciones para garantizar que nuestra información está protegida, este caso nos recuerda que es igualmente importante prestar atención a quién, en el seno de la organización, tiene acceso a dicha información. Resulta particularmente importante recordar lo anterior cuando los reporteros se valen de la Nube para compartir archivos.

Historia: Una sala de prensa en Afganistán usaba Dropbox para compartir archivos. Estaban trabajando en un proyecto noticioso en colaboración y todos los que estaban trabajando en cada una de las investigaciones periodísticas tenían acceso a los archivos y carpetas, incluida la información delicada. Nadie llevaba registro de qué estaba en la carpeta compartida, quién tenía acceso a los archivos específicos y quién de los muchos miembros podía compartir o había compartido qué carpetas con otras personas no vinculadas al proyecto.

En el transcurso de la investigación para esta historia, se le pidió a uno de los miembros del equipo que abandonara la organización. Dicha persona entregó todo el hardware a su cuidado (incluido el equipo portátil, cámara y memorias USB), pero nadie se acordó de revocar su permiso de acceso a la carpeta de Dropbox.

Dicha persona se incorporó a otra organización de medios de comunicación y publicó un artículo que incluía toda la información que sus antiguos colegas habían recopilado con tanto esfuerzo. Mientras todo esto ocurría, también se divulgó la identidad de una fuente que quería permanecer anónima e información delicada que podía remontarse a la fuente.

Fue necesario sacar a la fuente del país.

B. Lenguas sueltas y dispositivos abiertos

Presentación: El primer estudio de caso fue un ejemplo de un tipo de riesgo, el de perder control de la información almacenada en línea. El caso que presentamos a continuación analiza qué ocurre cuando se pierde control de datos en un entorno físico.

Historia: Una organización internacional de formación en medios de comunicación estaba capacitando a activistas y blogueros libios en Turquía. Los organizadores hablaron abiertamente del lugar donde se estaba llevando a cabo la capacitación y del número de participantes, así como de su identidad, de los equipos que estos llevaban, de los equipos que se les entregarían a su llegada, etc.

Una vez finalizada la capacitación, cuando los participantes estaban cruzando la frontera de regreso a casa, se encontraron con que había un nuevo puesto de control con el único propósito de requisarlos. Los reporteros llevaban sus portátiles, cámaras y memorias USB con programas de cifrado, así como herramientas de elusión de medidas tecnológicas y anonimizadores. Sus vehículos fueron requisados, les confiscaron las computadoras portátiles, y tres de los participantes de la capacitación fueron detenidos por las autoridades de seguridad fronteriza.

Más adelante se liberó a un reportero, pero los otros dos murieron detenidos.

Interacción con los participantes

En cada uno de estos casos, el capacitador les preguntará a los participantes qué creen que los periodistas y las organizaciones podrían haber hecho de manera distinta.

- **Para el estudio de caso A:** ¿Qué pudo haber hecho la organización de noticias afgana de manera distinta para asegurarse de no perder control de la información y disminuir la probabilidad de daños? ¿Podría haber ayudado una política que exigiera actualizar la lista de personas con acceso a las carpetas compartidas? ¿Qué haría usted en una situación similar?

Los capacitadores tienen plena libertad para añadir más información o improvisar según lo estimen oportuno.

- **Para el estudio de caso B:** En su opinión, ¿dónde radicaban las vulnerabilidades? ¿Las personas que se vieron afectadas no debieron haber confiado en sus propios colegas? ¿Qué le sugeriría usted a la organización para cuando lleve a cabo una capacitación similar en el futuro?

A partir de los estudios de caso, los capacitadores pueden resaltar las siguientes ideas:

Específicamente para el estudio de caso A:

- Dependiendo del entorno de seguridad, cualquier archivo puede considerarse un archivo delicado.
- Es importante saber dónde se comparte y envía la información. La información no debería compartirse con ninguna persona que no tenga por qué conocer dicha información, y deberían instaurarse controles para garantizar que la gente que recibe dicha información no la comparta de manera repetida.
- Nunca está de más revisar los accesos y cambiar las contraseñas periódicamente.

Específicamente para el estudio de caso B:

- En algunos lugares, el mero hecho de tener estas tareas de configuración inicial puede ser motivo de arresto.
- La información delicada almacenada en dispositivos puede ser un blanco y un motivo para ser fichado y arrestado.
- Como dicen los refranes, las paredes tienen oídos y por la boca muere el pez.

Ideas de conversación para el capacitador

Tras la presentación de los estudios de caso, el capacitador remitirá a los participantes a los [Apuntes de clase](#).

Para esta sesión, recomendamos que los capacitadores comiencen por explicar que el objetivo de la actividad de apertura y los estudios de caso que le siguieron fue dar una idea de los diversos retos que afrontan los periodistas. En el material restante, se pretende mostrar cómo la evaluación de riesgos puede ayudar a identificar soluciones a dichos retos y orientar la concepción de un plan de seguridad.

1. El proceso de evaluación de riesgos implica lo siguiente:

- Identificar activos valiosos (p. ej., listas de contactos, datos de investigación, apuntes de entrevistas o archivos audiovisuales);
- Determinar qué supone una amenaza para dichos activos;
- Evaluar en qué momento y lugar se está expuesto a dichas amenazas;
- Sopesar las posibles consecuencias.
 - ✓ Dar respuesta a estos interrogantes no solo brinda un panorama completo de qué hardware y tipo de información está expuesto a riesgos, sino que también ayuda a los periodistas a priorizar lo más importante. Por ejemplo, ningún reportero quiere perder el trabajo que ha adelantado para un artículo que está escribiendo, pero tampoco puede adelantar ese trabajo sin su lista de contactos.

2. En el contexto de la evaluación de riesgos, puede ser útil pensar en el entorno por niveles:

- **Vecindario:**
 - ✓ ¿Comparten sus vecinos las mismas preocupaciones que usted en materia de seguridad? ¿Existen maneras de ayudarse mutuamente para hacer de sus hogares u oficinas lugares más seguros?
- **Fuera de la oficina:**
 - ✓ ¿Cualquier persona puede entrar a la oficina? ¿Podría la gente alcanzar Internet o su equipo telefónico desde la ventana? ¿Está el punto de acceso a Internet de su oficina a la vista de personas que pasen por delante?
- **Desde la entrada:**
 - ✓ ¿Puede usted identificar posibles vulnerabilidades desde la entrada de su casa u oficina? ¿Está usted compartiendo detalles acerca de su proyecto o sus ideas con visitantes o con personas que pasan por la ventana? ¿Podría alguien que está de paso tener acceso físico a sus cables de red o a una PC?
- **En su escritorio:**
 - ✓ ¿Está su PC protegida con un cable de seguro contra robo o un candado? ¿O podría alguien llevársela fácilmente? ¿Está protegida con contraseña? ¿Ha tomado precauciones para que su PC no esté expuesta al polvo, al calor en exceso o a altibajos en la corriente eléctrica? Es recomendable que mantenga limpia el área de trabajo, se asegure de que su PC cuenta con

NOTA PARA LOS CAPACITADORES

Los textos con un ✓ no figuran en los Apuntes de clase de las copias a repartir a los estudiantes.

ventilación y use un sistema de alimentación ininterrumpida (UPS, por sus siglas en inglés).

■ **Su espacio digital:**

- ✓ ¿Están todos sus dispositivos protegidos con contraseña? ¿Cuenta usted con políticas o lineamientos que deban seguirse a la hora de compartir materiales o comunicarse con otras personas?

■ **Su red humana:**

- ✓ ¿A quién conoce? ¿En quién confía? ¿Quién debería tener acceso a su información y quién no?

3. Un plan de seguridad identifica las acciones que se pueden tomar para lidiar con las amenazas.

Estas son algunas de las preguntas que le pueden ayudar a formular un plan:

- ¿Qué riesgos podrían eliminarse por completo y cómo?
- ¿Cuáles podrían mitigarse y cómo?
- En función de la probabilidad e importancia de cada riesgo, ¿cuáles deberían tratarse primero?
 - ✓ Se asume que los periodistas y sus jefes no podrán abordar todas las amenazas al mismo tiempo. Deben estar preparados para organizar el trabajo para este proyecto, como lo harían para cualquier otro.

4. Aspectos que deben tenerse en cuenta:

■ **Sea inclusivo al planear.**

- ✓ Sus propios riesgos pueden depender de los hábitos de otras personas. Es importante hablar en grupo acerca de las políticas de seguridad.

■ **Sea cauteloso con los permisos y accesos.**

- ✓ ¿Tienen todas las personas de la oficina acceso a los datos o dispositivos que se encuentran en dicha oficina? ¿Deberían tenerlo?

**NOTA PARA LOS
CAPACITADORES**

El presente módulo tiene por objeto proporcionar una base en materia de evaluación de riesgos. Sin embargo, si los capacitadores quieren saber más acerca de la priorización de riesgos y de las fórmulas que a veces se aplican para producir puntajes de riesgo detallados, el siguiente material de Equalit.ie proporciona una explicación más detallada, así como lineamientos: "Evaluación de riesgos y el círculo de seguridad".



4. PROFUNDIZACIÓN (90 MINUTOS)

La siguiente sesión se divide en ejercicios de evaluación de riesgos y de planes de seguridad. Recomendamos que **el capacitador dedique unos 60 minutos al primer ejercicio y 30 minutos al segundo**. Antes de empezar, el capacitador comunicará a los participantes que los ejercicios tienen como fin ayudarles a dar inicio a una evaluación de riesgos práctica y a un plan de acción.

Ejercicio nro. 1: Identificar los riesgos (60 minutos)

El capacitador reparte las hojas de evaluación al comienzo de la sesión:

- Planilla de evaluación: [entorno físico](#)
- Planilla de evaluación: [integridad digital](#)

Este ejercicio tiene por objeto ofrecer a los participantes un enfoque de equipo y algunas herramientas para que comiencen a evaluar los riesgos en su lugar de trabajo. El capacitador orientará a los participantes por medio de los siguientes pasos:

- Dividirá a los participantes en dos equipos, uno de los cuales se centrará en integridad física y el otro, en integridad digital.
- Explicará que se dedicarán 30 minutos a identificar riesgos y clasificarlos en orden de prioridad. Todos deberían regresar al salón de capacitación en ese momento y estar preparados para poner en común una lista de los riesgos identificados.

NOTA: *En caso de que la capacitación se esté llevando a cabo en una oficina, sería muy beneficioso contar con la presencia de una persona de apoyo en TI para el presente ejercicio. Sin embargo, si la capacitación se está llevando a cabo en un lugar distinto, como en un hotel, y cuenta con participantes de varias organizaciones, tal vez los capacitadores quieran dividir a los participantes en función de la organización a la que pertenezcan o el tipo de trabajo y hacer listas de verificación de riesgos que estén adaptadas a cada situación particular.*

- Al final de los 30 minutos, el capacitador reunirá nuevamente a los participantes y moderará un debate en el que escribirá en una hoja de papel rotafolio la lista colectiva de los riesgos que hayan identificado los participantes.
- Le pedirá a la clase que clasifique los riesgos en orden de prioridad en función de la probabilidad de cada amenaza y el impacto que puedan tener. A modo de ejemplo, un terremoto puede ser devastador independientemente de dónde ocurra (alto impacto), pero en algunas regiones hay muy pocos terremotos (baja probabilidad).

Ejercicio nro. 2: Diseño de un plan de seguridad (30 minutos en total, 10 minutos para presentar las conclusiones)

Este ejercicio complementa el ejercicio anterior. El capacitador orientará a los participantes por medio de los siguientes pasos:

- Dividirá a los participantes en dos equipos e informará a los equipos que tendrán 20 minutos para ampliar el trabajo que acaban de hacer.
- Le pedirá al grupo A que haga una lluvia de ideas en cuanto a formas de mitigación de los riesgos identificados durante el Ejercicio nro. 1. Los participantes escribirán estas ideas en una única lista en una hoja de papel rotafolio. El grupo A debería tener en cuenta lo siguiente:
 - Asumiendo que tal vez no tengan todas las respuestas, ¿quiénes son las personas clave a quienes les podrían pedir ayuda y recomendaciones?
- Le pedirá al grupo B que piense en lineamientos que deben seguirse en la oficina (en la suya o en cualquier otra) al realizar una evaluación integral de los riesgos y en el plan de seguridad (o plan de acción) para implementar dichas soluciones. El grupo B debería tener en cuenta lo siguiente:
 - ¿Quiénes son los colegas clave que tendrían que participar en una evaluación integral de riesgos? (Se pueden proporcionar cargos genéricos, tales como jefe de redacción).
 - ¿Quién tendrá que tomar decisiones cruciales para que se puedan implementar cambios relativos a la seguridad?
 - ¿Cómo luciría un cronograma razonable?
 - ¿Qué herramientas podrían utilizarse en la oficina para instruir a los colegas acerca de cambios en materia de políticas de seguridad una vez que dichos cambios se apliquen?
- Cuando queden **10 minutos**, les pedirá a los equipos que presenten sus conclusiones.

ALTERNATIVAS

En casos en que los participantes no tengan acceso inmediato a sus oficinas o al personal de apoyo de TI, los capacitadores podrían optar por dividir los ejercicios de profundización y que el Ejercicio nro. 1 (“Diseñar una evaluación de riesgos”) se haga de tarea, antes de llevar a cabo el Ejercicio nro. 2 al día siguiente.

Para más ideas y actividades relacionadas, véase el sitio web de [LevelUp](#).



5. SÍNTESIS (15 MINUTOS)

Sugerimos que los capacitadores se valgan de esta sesión de recapitulación para hacer preguntas informales al grupo y repasar el material visto en este módulo. Las siguientes preguntas podrían ayudar a los participantes a poner en práctica lo aprendido:

- Aparte del entorno laboral, ¿cree que la evaluación de riesgos tiene alguna utilidad práctica para usted?
- En virtud de los temas de los que hemos hablado, ¿hay algo que usted ya sabe que hace o que ve en su oficina que querría cambiar inmediatamente?
- ¿Cuál cree que será el mayor reto a la hora de hacer una evaluación de riesgos y concebir un plan de seguridad para usted o para la organización donde trabaja?
- ¿Qué retos prevé para la implementación del plan de seguridad?
- Algunos han dicho que la seguridad física, la seguridad personal (de datos) y la seguridad de la red no son cosas distintas sino interdependientes. ¿Está usted de acuerdo con tal afirmación?

SaferJourno: recursos de seguridad digital para capacitadores de medios de comunicación es un proyecto de Internews que complementa el trabajo hecho en [SpeakSafe](#) y [LevelUp](#). Creado y compartido bajo [licencia Creative Commons Attribution-NonCommercial 3.0 Unported \(CC BY-NC 3.0\)](#).



PLANILLA DE EVALUACIÓN: INTEGRIDAD DIGITAL

CAPACITACIÓN:

FECHA:

GRUPO:

PARTICIPANTES:

1. ENRUTADORES INALÁMBRICOS

Vulnerabilidad	Fuente del riesgo	Nivel de riesgo (bajo, medio, alto)	Solución posible
¿Está la conexión inalámbrica protegida con conexión cifrada? (Es decir, ¿le pide el enrutador una contraseña para conectarse?)	Ejemplo: <i>vecinos, piratas informáticos estacionados cerca de la oficina</i>	Ejemplo: <i>alto</i>	Ejemplo: <i>Activar el cifrado WPA2 en la configuración del enrutador y protegerlo con una contraseña difícil de adivinar.</i>
¿Está usando contraseñas difíciles de adivinar para sus conexiones inalámbricas? (Para consejos, véase el documento impreso <i>Crear y mantener contraseñas seguras</i> .)			
¿Usa su enrutador cifrado WPA2? (El cifrado WPA2 suele ser el más potente.)			
¿Están los enrutadores ubicados lejos de áreas públicas donde alguien podría alterarlos de manera intencional o accidental? (Las zonas de recepción, salas de espera y cocinas tienden a ser de fácil acceso para el público en general y no son seguras.)			
¿Se ha cambiado la configuración predeterminada de la contraseña del enrutador de manera que solo alguien que cuente con la debida autorización pueda cambiar la configuración del dispositivo? (Si no, el manual del usuario del enrutador contiene instrucciones para hacerlo.)			
¿Ha deshabilitado el acceso Web (también llamado administrador de WAN) en la configuración de su enrutador para que quien esté fuera de la oficina no pueda cambiar la configuración de su enrutador? (Si no, el manual del usuario del enrutador contiene instrucciones para hacerlo.)			
Otros apuntes/ideas de debate acerca de los enrutadores inalámbricos:			



2. INFRAESTRUCTURA Y MANTENIMIENTO

Vulnerabilidad	Fuente del riesgo	Nivel de riesgo (bajo, medio, alto)	Solución posible
¿Está alguien del personal a cargo de las cuestiones técnicas y puede esta persona atender las emergencias de manera inmediata (p. ej., instalar la red de la oficina o recuperar información perdida)?			
En caso negativo, ¿existe un tercero o compañía externa que usted haya contratado para las tareas de TI en su oficina, y las personas clave en su oficina conocen los datos de contacto de ese tercero?			
¿Tiene la oficina su(s) propio(s) servidor(es)? En caso afirmativo, véanse las siguientes preguntas:			
¿Está protegido el acceso en línea al servidor? 1. ¿Está habilitado el firewall o muro informático? 2. ¿Está restringido el acceso a los administradores? 3. ¿Están protegidas las cuentas con contraseñas difíciles de adivinar?			
¿Está protegido el acceso físico al (a los) servidor(es)? (¿Están todos los servidores asegurados y resguardados contra agua, exposición directa a la luz solar y lejos de las áreas públicas?)			
Si su oficina opera su(s) propio(s) servidor(es), ¿se están tomando las precauciones adecuadas para protegerlo del malware, y el sistema operativo se mantiene actualizado?			
Otros apuntes/ideas de debate acerca de la infraestructura y el mantenimiento:			



3. MIEMBROS DEL PERSONAL Y SU CONDUCTA

Vulnerabilidad	Fuente del riesgo	Nivel de riesgo (bajo, medio, alto)	Solución posible
¿Dispone todo el personal de software antivirus instalado en la PC de la oficina? En caso afirmativo, ¿se actualiza dicho antivirus de forma automática o periódicamente?			
¿Están todas las PC de la oficina configuradas para que acepten automáticamente actualizaciones del sistema operativo? Los piratas informáticos suelen aprovechar los sistemas operativos no actualizados para controlar las PC vía remota.			
¿Se está utilizando software de cifrado para proteger archivos o equipos PC en la oficina (p. ej., Bitlocker o TrueCrypt)?			
¿Se le exige a todo el personal que asigne contraseñas difíciles de adivinar para sus cuentas en el trabajo? (Para consejos, véase el documento impreso <i>Crear y mantener contraseñas seguras</i> .)			
¿Emplea el personal la misma contraseña para más de una cuenta en línea? (Esta práctica no es recomendable porque dicha contraseña podría dar acceso a más de una cuenta.)			
¿Cómo mantienen seguras las contraseñas los miembros del personal? ¿Se valen de aplicaciones de cifrado, como KeePass?			
¿Hay miembros del personal que usan software sin licencia? De ser así, indíquelo en la columna a la derecha titulada “Fuente del riesgo”, de manera que pueda buscar alternativas gratuitas y legítimas en sitios como osalt.com . Además de contravenir los derechos de autor, el software sin licencia a menudo viene acompañado de malware (virus).			
¿Se les permite a los miembros del personal usar cuentas personales de correo electrónico en el trabajo? En caso afirmativo, y si estas cuentas han sido objeto de intentos de <i>phishing</i> (correos falsos) o de ataques de piratas informáticos, ¿ha representado esto un problema para la red de la oficina, otras PC o para documentos de la oficina?			
¿Hay miembros del personal que usan sus computadoras portátiles personales en la oficina? En caso afirmativo, ¿existen requisitos mínimos para dichas computadoras portátiles antes de usarlas en la red de la oficina?			

Otros apuntes/ideas de debate acerca del personal y su conducta:

4. SERVICIOS COMPARTIDOS Y PUNTOS DE ACCESO



Vulnerabilidad	Fuente del riesgo	Nivel de riesgo (bajo, medio, alto)	Solución posible
<p>¿Usan los miembros del personal servicios para compartir archivos que la oficina no controla (Dropbox, por ejemplo)? ¿Se protegen los archivos de alguna forma o se cifran? En caso afirmativo, enumere los archivos en la columna titulada “Fuente del riesgo” y especifique cómo están protegidos.</p>			
<p>¿Usan usted o sus colegas puntos de acceso públicos, como un café, por ejemplo?</p>			
<p>En caso afirmativo, sería recomendable fijar lineamientos para el uso de portátiles de la oficina en puntos de acceso públicos. (<i>Véanse los consejos para conectarse a distintos sitios de forma segura en el capítulo "Navegar por internet de manera más segura" de SpeakSafe.</i>)</p>			
<p>¿Proporciona la oficina un punto de acceso público para visitantes? En caso afirmativo, ¿dicho punto está separado de la red para el personal?</p>			
<p>Otros apuntes/ideas de debate acerca de los servicios y puntos de acceso compartidos:</p>			



5. PLANES Y PROGRAMACIÓN DE RECUPERACIÓN DE ERRORES

Vulnerabilidad	Fuente del riesgo	Nivel de riesgo (bajo, medio, alto)	Solución posible
¿Tiene su oficina un plan o política en materia de copias de seguridad que sea aplicable a todas las PC de la oficina?			
¿Existe un método uniforme para hacer copias de seguridad de la información guardada en las PC? En caso negativo, ¿cree que las tareas de copiado de seguridad serían más fiables si se adoptara dicho método?			
¿Guarda su oficina una copia de seguridad en el mismo lugar donde guarda la información original para que las copias de seguridad sean de fácil acceso en caso de emergencia?			
¿Guarda su oficina una copia de seguridad en otra ubicación fuera de la oficina para evitar que se pierdan tanto los originales como las copias de seguridad en caso de catástrofe natural o robo?			
¿Tiene todo el personal de la oficina acceso a todas las copias de seguridad? ¿O dicho acceso está permitido únicamente a ciertas personas clave?			
¿Las copias de seguridad están cifradas para protegerlas de quienes no tengan permiso para usarlas?			

Otros apuntes/ideas de debate acerca de los planes y programación de copias de seguridad:



6. SEGURIDAD PARA TELÉFONOS CELULARES

Vulnerabilidad	Fuente del riesgo	Nivel de riesgo (bajo, medio, alto)	Solución posible
¿Guarda el personal información delicada en el celular de la oficina (fotografías, grabaciones de audio de entrevistas, información importante de datos de contacto, etc.)?			
¿Sería útil para el personal repasar materiales en línea en materia de seguridad para celulares? (<i>Security in-a-box ofrece una excelente guía sobre seguridad móvil, Seguridad Móvil.</i>)			
¿Usan los miembros del personal una contraseña larga para evitar el acceso indebido a los celulares? (<i>Una contraseña larga es más segura que un PIN.</i>)			
¿Protegen los miembros del personal con una función de cifrado los datos que contienen sus celulares? (<i>Los dispositivos Android, iPhone y Blackberry permiten a los usuarios habilitar la función de cifrado en Ajustes.</i>)			
¿Comparten los miembros del personal información relacionada con el trabajo por mensajes de texto? (<i>El proveedor de telefonía móvil y quienquiera que tenga acceso a los registros del proveedor puede ver los mensajes de texto.</i>)			
¿Usan los miembros del personal una aplicación como ChatSecure (para Android) para enviarse mensajes? (<i>Este sitio web contiene información excelente acerca de ChatSecure.</i>)			
¿Usted o sus colegas hacen copias de seguridad de información "crítica" del celular, como listas de contactos, por ejemplo, y cifran dichas copias?			
Otros apuntes/ideas de debate acerca de la seguridad para teléfonos celulares:			



PLANILLA DE EVALUACIÓN: ENTORNO FÍSICO

CAPACITACIÓN:

FECHA:

GRUPO:

PARTICIPANTES:

1. FUERA DE LA OFICINA			
Vulnerabilidad	Fuente del riesgo	Nivel de riesgo (bajo, medio, alto)	Solución posible
¿Usted o sus colegas viajan con equipos portátiles y teléfonos? ¿Tienen alguna manera de velar por la seguridad física de estos dispositivos en el lugar a donde van? (¿Llevan sus dispositivos consigo todo el tiempo o tienen un candado para asegurarlos físicamente?)	Ejemplo: <i>Pérdida (olvidado)</i> <i>Robo por parte de otros viajeros o carteristas</i> <i>Decomiso por parte de las autoridades</i>	Ejemplo: <i>Medio</i>	Ejemplo: <i>Llevarse el cable de seguridad y el candado en los viajes.</i> <i>Guardar la computadora portátil en el equipaje de mano y mantener el equipaje cerca.</i> <i>Llevar siempre el celular en el bolsillo.</i>
¿Los miembros del personal se llevan a casa portátiles e información de la oficina? ¿Qué precauciones toman para reducir el riesgo de robo?			
Otros apuntes/ideas de debate acerca de la seguridad fuera de la oficina:			



2. SU EDIFICIO

Vulnerabilidad	Fuente del riesgo	Nivel de riesgo (bajo, medio, alto)	Solución posible
¿Se protegen con candado los puntos de entrada a la oficina (es decir, puertas y ventanas)?			
¿Usted o sus colegas salen fuera de la oficina y dejan las puertas abiertas (para fumar o hacer llamadas personales por celular, por ejemplo)?			
¿Las ventanas que están en la planta baja permanecen abiertas y desatendidas durante el día?			
¿La conexión telefónica y a Internet de su oficina es de fácil acceso desde una caja de fusibles situada fuera del edificio?			
Que usted sepa, ¿están vigilando su oficina desde un edificio cercano?			
¿Cómo registra su oficina a los visitantes antes de permitirles el ingreso a las instalaciones? (¿Hay una puerta de vidrio, una mirilla, cámaras de video u otra forma de controlar la entrada de visitantes?)			
¿Cuenta su oficina con protocolos de seguridad para permitir el ingreso a visitantes que tal vez no todo el personal conozca (pedir identificación, depósito de celulares, detector de metales, escáner corporal, etc.)?			
Otros apuntes/ideas de debate acerca de cómo mejorar la seguridad:			



3. EN LA OFICINA			
Vulnerabilidad	Fuente del riesgo	Nivel de riesgo (bajo, medio, alto)	Solución posible
¿Los visitantes que entran a la oficina pueden ver inmediatamente la(s) pantalla(s) de su computadora u otros sitios donde la información importante está a la vista?			
¿Las reuniones de equipo y para decidir qué historias cubrir en los medios se hacen en espacios abiertos donde los visitantes externos pueden oír la conversación?			
¿Los dispositivos de red como enrutadores, centros de conexión (hubs), o módems están en un lugar seguro para que los intrusos no tengan acceso directo a ellos?			
¿Están sus computadoras de escritorio y portátiles protegidas por un cable de seguridad con candado para evitar robos?			
Otros apuntes/ideas de debate acerca de riesgos en la oficina:			
4. RIESGOS ELÉCTRICOS COMUNES			
Vulnerabilidad	Fuente del riesgo	Nivel de riesgo (bajo, medio, alto)	Solución posible
¿Los contactos múltiples o tomas eléctricas en la pared emiten chispas cada vez que usted conecta un dispositivo, lo que conlleva peligro de incendio?			
¿Las computadoras y otros equipos sensibles están expuestos a la luz solar directa, lo que podría hacer que se recalienten?			
¿Las computadoras que se guardan en cajones cuentan con buena ventilación para que no se recalienten?			
¿Utiliza un sistema de alimentación ininterrumpida (UPS) en su oficina? <i>(Un UPS estabiliza la corriente que recibe su PC y puede servir de fuente temporal de alimentación en caso de apagón.)</i>			
¿Están sus PC y cables a la vista en pasillos, áreas de recepción y otros lugares muy transitados?			
¿Están los cables de red alejados de ventanas donde la lluvia podría dañarlos y provocar un cortocircuito?			
Otros apuntes/ideas de debate acerca de riesgos eléctricos comunes:			



5. CELULARES			
Vulnerabilidad	Fuente del riesgo	Nivel de riesgo (bajo, medio, alto)	Solución posible
¿Los miembros del personal dejan a la vista el celular cuando se reúnen en sitios públicos (en la mesa de un café, por ejemplo)?			
¿Llevan los miembros del personal el celular consigo siempre? <i>(Se recomienda que así sea durante la jornada laboral, a no ser que los periodistas no quieran transmitir su ubicación física.)</i>			
Otros apuntes/ideas de debate acerca de los celulares:			

GLOSARIO

Las definiciones de términos que se muestran a continuación se proporcionan bajo [licencia Creative Commons Attribution-Share Alike 3.0 Unported](#) e incluyen entradas creadas por Tactical Technology Collective, Front Line Defenders e Internews.

El vocabulario relacionado con este módulo es el siguiente:

Bluetooth. Estándar físico de las comunicaciones inalámbricas para el intercambio de datos a través de distancias cortas desde dispositivos móviles y fijos. Bluetooth usa transmisiones de radio de onda corta.

amenaza física. En este contexto, amenaza que atenta contra la información delicada de un usuario como consecuencia del acceso físico y directo de terceros al hardware de la computadora de dicho usuario o derivada de otros riesgos físicos, tales como averías, accidentes o catástrofes naturales.

cable de seguridad. Cable con candado empleado para fijar la computadora portátil u otra pieza de hardware a la pared o al escritorio (incluidos discos duros externos y algunas computadoras de escritorio) para evitar que alguien se las lleve físicamente.

cifrado. Forma de usar las matemáticas para *cifrar* información, o codificarla, de manera que solo pueda *descifrarla* y leerla quien tenga una pieza específica de información, como una contraseña, o clave o llave de cifrado.

dirección de protocolo de Internet (dirección IP). Identificador único asignado a una computadora cuando está conectada a Internet.

enrutador. Equipo de red por medio del cual las computadoras pueden conectarse a sus redes locales y mediante el cual varias redes locales acceden a Internet. Los interruptores, las puertas de enlace y los hubs llevan a cabo tareas similares, al igual que los puntos de acceso remotos en el caso de las computadoras que están equipadas para utilizarlos.

firewall. Herramienta que protege la computadora de conexiones no seguras a redes locales e Internet.

malware. Término general para referirse a todo software malicioso, incluidos los virus, el spyware, los caballos de Troya y a otras amenazas de este tipo.

phishing (ciberestafa). Crear sitios web o correos electrónicos falsos que parecen ser legítimos, para lograr que los usuarios de Internet caigan en la estafa e interactúen con los contenidos. Se usa a menudo para captar contraseñas e información financiera.

pirata informático (hacker). En este contexto, delincuente informático malintencionado que intenta acceder a información delicada o tomar control de la computadora del usuario vía remota.

política de seguridad. Documento escrito que describe la mejor manera de proteger una organización de amenazas diversas, lo que incluye una lista de pasos a seguir en caso de que se produzcan ciertos percances en materia de seguridad.

proveedor de servicios. Compañía privada o pública que presta a sus clientes servicios de telefonía móvil o servicios de Internet.

proveedor de servicios de Internet (Internet service provider; ISP, por sus siglas en inglés). Compañía u organización que provee la conexión inicial a Internet. Los Gobiernos de muchos países ejercen control de Internet con métodos tales como el filtrado y la vigilancia a través de los ISP que operan en esos países.

punto de acceso. Punto en el que un dispositivo se conecta a Internet, normalmente un punto de acceso inalámbrico (Wi-Fi).

software gratuito de código abierto (free and open-source software; FOSS, por sus siglas en inglés). Esta familia de software se consigue sin costo alguno y no tiene restricciones legales que impidan a los usuarios probar el software, compartirlo o modificarlo.

servidor. Computadora que permanece encendida y conectada a Internet para proporcionar algún servicio a otra computadora, como, por ejemplo, alojar un sitio web o enviar y recibir correos electrónicos.

2. MALWARE Y PROTECCIÓN BÁSICA



<http://www...?>

IMPORTANCIA DEL TEMA

Cuando una PC se infecta con un virus u otro malware, los periodistas pueden perder control de sus equipos, cuentas de correo electrónico y otros datos que son esenciales para su trabajo. Una infección desagradable causada por un “gusano” se propaga fácilmente por toda la oficina, y las consecuencias para terceros también pueden ser graves. Una PC infectada puede darle a un pirata informático acceso a información delicada, a los resultados de su investigación y a otros archivos.

LO QUE APRENDERÁN LOS PARTICIPANTES

Ideas: virus informáticos fruto de nuestras acciones (y del software).

Competencias: utilizar la aplicación antivirus Avast! y mantener actualizados los sistemas operativos y el software.

OBJETIVOS

Aprender acerca de los métodos de ataque más comunes y de las aplicaciones antivirus

APLICACIONES PRÁCTICAS

Prevenir infecciones en una PC, detectar correos electrónicos falsos

CONOCIMIENTOS PREVIOS EXIGIDOS

El presente módulo parte de la base de que los participantes saben hacer lo siguiente:

- Identificar sistemas operativos;
- Instalar aplicaciones;
- Guardar y ubicar archivos en sus computadoras.

ANTES DE COMENZAR

Los recursos que se enumeran a continuación podrían ayudar a los capacitadores a mejorar sus conocimientos acerca del tema del presente módulo antes de comenzar a dictarlo:

- “Malware FAQ” [Preguntas frecuentes acerca del malware] (SANS Institute);
- “A List of Computer Viruses” [Una lista de virus que atacan la computadora] (Wikipedia);
- “Proteger su computadora de software malicioso y piratas informáticos” (Security in-a-box).



MATERIALES

Además de los materiales de capacitación que recomendamos normalmente en la [Guía para capacitadores](#) (véase el apartado “[Consejos para la capacitación](#)”), los capacitadores necesitarán lo siguiente para esta unidad didáctica:

Software e instalación

- Avast!
 - Guía
- ClamWin
 - Guía.

Documentos impresos a repartir

- Apuntes de clase
- Glosario
- “Proteger su computadora de software malicioso y piratas informáticos” (Security in-a-box).

NOTA: Los capacitadores que necesiten información acerca de los dispositivos Apple pueden consultar los [Apuntes de la capacitación de “Mac OS X”](#) que se encuentran justo después de la sesión de Síntesis de este módulo.



MÓDULOS RELACIONADOS

Mientras que aprender a proteger una PC del malware es aplicable a todos los módulos que integran este curso, los siguientes módulos están muy relacionados entre sí, puesto que tratan sobre el envío y la recepción de correo electrónico y sobre visitar sitios web con los que el usuario puede no estar familiarizado:

- Investigar de manera segura
- Protección de su correo electrónico.

PLAN DE CLASE



1. ACTIVIDAD (20 MINUTOS)

Los cazavirus

Esta actividad tiene como objeto poner de relieve una forma común en que las PC se infectan de virus informáticos: a través de correos falsos (lo que se conoce como *phishing*) y los virus presentes en archivos adjuntos. Se trata de mostrar a los participantes que pueden evitar muchas infecciones si simplemente prestan atención a lo que está en su bandeja de entrada.

Preparación

Antes de la clase, los capacitadores deberían repasar el siguiente artículo, disponible en el sitio web de la Electronic Frontier Foundation (EFF): “[Vietnamese Malware Gets Very Personal](#)” [El malware vietnamita se mete en asuntos muy personales]. También recomendamos que los capacitadores marquen las hojas como favoritas con capturas de pantalla o las descarguen antes de la clase para proyectarlas en un muro o imprimirlas para repartirlas.

Cómo organizar la actividad

El capacitador les preguntará a los participantes si han oído hablar de los virus informáticos, y después les preguntará si saben cuáles son las formas de contagio más comunes para las PC. Si los participantes mencionan el correo electrónico como vía de contagio, el capacitador podrá pasar directamente al siguiente paso de la actividad. Si no es así, es recomendable que el capacitador explique que el correo electrónico es una de las herramientas más usadas por los hackers o piratas informáticos para infectar una PC. Como los participantes verán a continuación, los piratas se sirven de varias estrategias para lograr su objetivo.

El capacitador procederá a proyectar la primera captura de pantalla del artículo de la EFF, que muestra el correo electrónico que recibieron esta organización y un periodista de la Associated Press.

El capacitador dirá lo siguiente: “Hay algo en este correo electrónico que no acaba de convencerme, pero no sé qué es. ¿Pueden ayudarme a averiguarlo?”

A partir de esta pregunta, el capacitador empezará desde el principio del correo e irá comentando todos los problemas. A los participantes se les deberá permitir identificar los problemas primero, pero si se les dificulta, el capacitador podrá servirse de las siguientes preguntas:

- ¿Cómo lucen las oraciones de este correo electrónico? El texto del correo tiene varios errores tipográficos. Por ejemplo, las oraciones no terminan con punto, y el lenguaje podría parecerle forzado a un nativo.
- ¿Y qué hay de la dirección de correo electrónico de quien envía el mensaje? Parece ser andrew.oxfam@gmail.com. ¿Hay algo de esa dirección que le llame la atención? ¿No sería de esperar que Oxfam tuviese su propio dominio de correo electrónico, como “oxfam.org”, por ejemplo?
- Este correo electrónico le pide a quien lo recibe que haga clic en ciertos vínculos para obtener información acerca de una invitación. Dichos vínculos son largas cadenas (azules) compuestas de letras y números que se encuentran casi al final del correo. ¿Hay algo de esos vínculos que le llame la atención? Los vínculos parecen llevar a www.oxfam.org (observe que hay una diferencia entre la dirección del sitio web y la dirección electrónica de la persona que envía el correo). Sin embargo, al examinar en detalle los vínculos, se puede ver que en realidad llevan a otro lugar, un archivo compartido en la carpeta Google Drive de alguien.

El capacitador les preguntará a los participantes qué creen que podría suceder si alguien hiciera clic en alguno de los vínculos o en uno de los archivos adjuntos al correo electrónico. Respuesta: La EFF determinó que los vínculos harían que la PC instalara un virus.

RECORDATORIO

Si el presente módulo es el primero de un taller más amplio, sugerimos que los capacitadores dediquen los primeros 10 minutos a trabajar con el grupo para definir los lineamientos de conducta y seguridad. Para más información, véase el apartado “Formalización de un contrato” de la *Guía para capacitadores*.

El capacitador escribirá dos palabras en el rotafolio:

- *malware*
- *phishing*.

El capacitador escribe las palabras *malware* y *phishing* en el rotafolio y explica cómo se definen:

- *Malware* es lo que infecta una PC. Esta palabra, en inglés, es una combinación de las palabras *malicioso* y *software*, y se refiere a virus de todo tipo.
- *Phishing* es el equivalente de un fraude electrónico. Se refiere al acto de engañar a un usuario para que haga clic en un vínculo malicioso o exponga información privada, como una contraseña, al presentarle un correo electrónico, mensaje instantáneo o sitio web falsos que parezcan legítimos. Esta es una de las formas más comunes en las que se infectan las PC.

NOTA: Los capacitadores que deseen llevar a cabo versiones más ambiciosas de la presente actividad pueden repasar el apartado “Analysing a Potentially Harmful Email” [Análisis de un email potencialmente dañino] en el sitio web de [LevelUp](#).



2. DEBATE (15 MINUTOS)

Una vez que la actividad haya concluido, los capacitadores les pedirán a los participantes que se sienten en círculo o en medio círculo para que puedan dirigirse los unos a los otros. Las siguientes preguntas pueden ser útiles para dar inicio al debate:

- ¿Alguna vez se le ha infectado la PC a alguien del grupo? ¿Cuáles fueron las consecuencias?
- ¿Cómo puede un virus infectar una PC?
 - A causa de un hardware infectado (tales como las memorias USB);
 - A causa de un software sin licencia o pirata (p. ej., sitios de descargas falsificadas);
 - Al hacer clic en vínculos maliciosos que llevan a descargar virus (p. ej., anuncios publicitarios falsos);
 - Al descargarlo por medio de archivos maliciosos adjuntos a correos electrónicos;
 - Con ataques basados en ingeniería social (es decir, uso indebido de un nombre);
 - Al descargarlo por estafas en sitios de redes sociales.
- ¿Cómo se lleva a cabo el phishing?
 - Mediante correos electrónicos que le piden al usuario que inicie sesión en su cuenta de banca en línea;
 - Mediante correos electrónicos que le piden al usuario que inicie sesión en sus cuentas de redes sociales (p. ej., “tvwitter.com” en vez de “twitter.com”);
 - Mediante mensajes privados en Twitter con vínculos abreviados que remiten al usuario a pantallas falsas de inicio de sesión;
 - Mediante mensajes en el muro de Facebook y vínculos que remiten al usuario a pantallas falsas de inicio de sesión.
- ¿Qué haría usted si recibiera el correo electrónico que acabamos de ver? (¿Qué le diría a un amigo que debe hacer?)

Recomendamos las siguiente opciones:

 - Elimine el correo electrónico;
 - Enséñele el correo electrónico a un compañero de trabajo o amigo con conocimientos avanzados de informática para ver si puede determinar la procedencia del correo. ¿Proviene de otro país o proviene de su ciudad, lo que podría indicar que usted es un blanco de ataque?
- ¿Sabe de aplicaciones o extensiones (*add-ons*) del explorador que podrían servirle?
- ¿Cuántas personas del grupo tienen una aplicación antivirus instalada en su PC? ¿Qué aplicación antivirus utilizan? ¿Cómo eligieron la aplicación antivirus que utilizan?
- ¿Cuántas personas del grupo actualizan su sistema operativo? ¿Podrían decirnos por qué lo actualizan?
- Los que no actualizan su sistema operativo, ¿podrían decirnos por qué no? (¿Les preocupa una visita de las autoridades encargadas de combatir la piratería?)
- ¿Alguien del grupo tiene una aplicación antivirus instalada en su teléfono inteligente?
- Repasemos las palabras que escribimos en el rotafolio, *phishing* y *malware*. ¿Qué significan?

Los capacitadores tienen plena libertad para añadir elementos a la lista o improvisar según lo estimen oportuno.



3. INFORMACIÓN/EXPOSICIÓN (30 MINUTOS)

La presente sesión incluye un estudio de caso recomendado, ideas clave y algunos materiales para ayudar a transmitir la idea que se está abordando.

Estudio de caso

FinFisher en Bahrein

Presentación: Casi todo el malware tiene que ver con organizaciones criminales cuyo fin es robar dinero. Como periodistas, no tenemos dinero, pero sí tenemos algo de valor para terceros: información.

Historia: En julio de 2012, el Citizen Lab y un centro de investigación interdisciplinaria de la [Munk School of Global Affairs](#), de la [Universidad de Toronto](#), analizaron el software malicioso que recibieron activistas bahreínes de una cuenta vinculada a la reportera de Al Jazeera Melissa Chang. Los investigadores analizaron los correos electrónicos que recibieron los activistas prodemocracia y los identificaron como infectados con [FinFisher](#) (también llamado *FinSpy*), un software de vigilancia que vende la organización británica [Gamma Group](#).

En Bahrein hay tensiones desde que el Gobierno tomó medidas represivas contra las manifestaciones en masa de quienes se oponían a que una minoría musulmana suní gobernara a la mayoría chiita. Las pruebas realizadas en el Citizen Lab mostraron que si un receptor hacía clic en los archivos adjuntos, normalmente fotografías o documentos de violaciones a los derechos humanos, el spyware se instalaba clandestinamente. El software malicioso pasó entonces por un complejo proceso en el que se escondía, revisaba y evadía los programas antivirus y establecía una conexión con el servidor en Manama al que enviaba su información.

Un spyware como FinFisher es muy intrusivo: se mete en los dispositivos digitales de los usuarios y lleva a cabo una vigilancia encubierta. El spyware y el resto del malware pueden llegar a penetrar hasta en los espacios más privados y, clandestinamente, tomar control de la computadora vía remota, copiar archivos, interceptar llamadas de Skype, encender cámaras web y grabar pulsaciones de teclado.

Aunque un directivo del Gamma Group dijo supuestamente en un correo electrónico de 2012 que “FinFisher es una herramienta para seguirle el rastro a los delincuentes y, con el fin de mitigar el riesgo de un uso indebido de sus productos, la compañía solo vende FinFisher a Gobiernos”, lo cierto es que los blancos de ataque eran activistas a favor de la democracia que jamás habían hecho frente a denuncias por delitos.

Los investigadores observaron el comportamiento del malware y concluyeron que se comportaba como lo hace lo que se conoce como un *caballo de Troya*, es decir, un tipo de software malicioso cuyo nombre hace alusión al caballo que construyeron los guerreros griegos para adentrarse en la antigua ciudad de Troya antes de destruirla. Los investigadores del Citizen Lab descubrieron que las máquinas comprometidas enviaban informes a una computadora en Bahrein. Sin embargo, cuando Bloomberg se puso en contacto con el Gobierno bahreí al respecto, Luma Bashmi, la portavoz de la Comisión para asuntos en materia de información (Information Affairs Authority), dijo en una declaración enviada por correo electrónico que los activistas políticos no son blanco de la tecnología de vigilancia que usa el Gobierno bahreí.

FinFisher es solo una de las muchas herramientas de vigilancia disponibles en el mercado, se desarrolló en Occidente y se vende a Gobiernos de todo el mundo que estén dispuestos a pagar por ella. Mientras que los métodos tradicionales de pirateo incluían interceptar teléfonos, correos electrónicos y mensajes de texto, algo que los Gobiernos lograban al interceptar las redes nacionales de comunicación, FinFisher les permite trascender fronteras políticas. También hace posible que los Gobiernos que tal vez no tengan cómo diseñar sus propias armas cibernéticas puedan comprar software de vigilancia más avanzado.

“Cuando FinSpy [FinFisher] se instala en el sistema de una computadora, esta puede ser controlada por vía remota y se tiene acceso a ella cuando está conectada a una red/Internet, independientemente de en qué parte del mundo se encuentre el sistema de destino”, dice un [folleto](#) en inglés de Gamma Group publicado por WikiLeaks.

Los capacitadores tienen plena libertad para añadir más información o improvisar según lo estimen oportuno.

Fuentes:

- **Citizen Lab:** “From Bahrain With Love: FinFisher’s Spy Kit Exposed?” [Desde Bahrein, con amor: ¿Se destapa el aparato de espionaje de FinFisher?];
- **Bloomberg:** “Cyber Attacks on Activists Traced to FinFisher Spyware of Gamma.” [Ciberataques contra activistas se remontan al spyware FinFisher de Gamma].

Materiales útiles:

- **Video:** *FinFisher Products and Services* [Productos y servicios de FinFisher];
- **Video:** *FinSpy Surveillance Tool Takes Over Computers* [La herramienta de vigilancia FinSpy se apodera de las computadoras (Bloomberg)].

Interacción con los participantes

A partir de los ejemplos mencionados anteriormente, los capacitadores pueden ayudar a los participantes a reflexionar acerca de prácticas propias que puede que estén poniendo en peligro a sus fuentes. Las siguientes preguntas podrían serles de utilidad:

- ¿Hace clic en todos los archivos adjuntos que llegan a su bandeja de entrada?
 - De ser así, ¿por qué? ¿Ha hecho esto que su computadora vaya más lenta, se bloquee o haya perdido información?
 - De no ser así, ¿por qué se ha detenido antes de hacer clic?
- ¿Alguna vez lo han preocupado las infecciones por malware? ¿Por qué? ¿Guarda información que podría exponerlo a tales infecciones?
- Si ha tenido alguna experiencia con el malware, ¿cómo le llegó? ¿Como archivo adjunto? ¿Como actualización de software? Compártalo con el grupo.
- ¿Si una fuente que está entrevistando se muestra particularmente difícil, estaría tentado a usar spyware o malware para piratear la computadora de dicha fuente?
 - ¿Por qué?
 - ¿Por qué no?
- ¿Cree que puede protegerse? ¿Cómo exactamente? Compártalo con el grupo.

Ideas de conversación para el capacitador

Después de presentar el estudio de caso, el capacitador remitirá a los participantes a los [Apuntes de clase](#).

- ✓ Los desarrolladores de aplicaciones antivirus informan que la mayoría de las PC se infectan con caballos de Troya, que son virus que se hacen pasar por algo inocuo e incluso deseable. (¿Alguna vez le ha salido una ventana emergente inesperada, de una compañía de la que jamás había oído hablar, que le dice que su PC ha sido infectada y que, con que usted haga clic en un simple vínculo, se la pueden limpiar?) Pandasecurity.com afirma que [tres de cada cuatro infecciones se producen así](#). Esto era precisamente lo que se quería mostrar con la actividad.

1. Los virus son un GRAN problema

- [Se han registrado decenas de miles de virus informáticos](#). Las PC que no están protegidas tienen un “[tiempo de superveniencia](#)” ¡de apenas unos seis minutos!
- ✓ “**PC sin protección**” se refiere a lo siguiente:
 - ✓ Una PC Windows
 - ✓ Sin un firewall activado,
 - ✓ Sin una aplicación antivirus instalada,
 - ✓ Que esté conectada a Internet.
- ✓ Lo bueno es que, desde el lanzamiento de Windows 7, Microsoft activó de forma predeterminada un firewall integrado. Sin embargo, este dato de los seis minutos sigue siendo una muestra patente de lo agresivo que se ha vuelto cierto tipo de malware (sobre todo los llamados *gusanos*).

2. ¿Quién crea los virus?

- [Algunos piratas informáticos lo hacen por dinero: Conficker](#).
 - ✓ Conficker es un gusano informático, un tipo de virus que se replica para infectar cualquier otro

**NOTA PARA LOS
CAPACITADORES**

Los textos con un ✓ no figuran en los Apuntes de clase de las copias a repartir a los estudiantes.

dispositivo o red. Conficker, que se ha detectado en millones de PC, se creó para que los piratas informáticos pudieran apoderarse de las PC infectadas para varios fines. Cuando muchas PC (en algunos casos cientos de miles) pasan a ser controladas por piratas informáticos se les llama *botnets* o computadoras zombi (véase el [Glosario](#)).

- **A veces, es un método empleado por los servicios de inteligencia:** [Ghostnet](#).
 - ✓ Esta aplicación de spyware, que se descubrió en 2009, les dio a hackers desconocidos control remoto de computadoras PC (incluidos el micrófono y la cámara), algunas de cuales fueron usadas por el séquito del Dalai Lama y algunas por los ministerios de Hacienda de países en el bloque económico ASEAN.
- **Otras veces se lleva a cabo porque sí:** [ILoveYou](#).
 - ✓ Este virus les pedía a los usuarios que hicieran clic en un archivo adjunto que aparentemente era un simple archivo de texto. Como resultado, en la pantalla aparecía un aviso que decía “I Love You” y los archivos de imágenes de la PC se eliminaban o dañaban.

3. Mitos comunes

- **Los virus solo atacan el sistema operativo Windows.**
 - ✓ Los virus también atacan el sistema operativo de Mac y Linux, aunque Windows es el más afectado, tal vez por ser el sistema operativo más utilizado, pues se calcula que más del 80 % de las PC del mundo funcionan con Windows. Los usuarios de sistemas operativos que no sean Windows deberían contar, de todos modos, con una aplicación antivirus, para ayudar a detener la propagación de virus que podrían estar enviando a otros sin saberlo.
- **Los virus no atacan teléfonos inteligentes.**
 - ✓ Las plataformas de iPhone y Android tienen virus. Probablemente, esto se debe a que los teléfonos inteligentes cada vez tienen más funciones que antes eran exclusivas de las PC, como chatear, enviar correos electrónicos y hacer compras.
- **Un antivirus siempre limpiará una PC infectada.**
 - ✓ Las aplicaciones antivirus normalmente están mejor equipadas para prevenir el contagio de un virus que para limpiarlo después de que haya infectado una PC. Los expertos en seguridad normalmente aconsejan a los usuarios que instalen nuevamente su sistema operativo y sus aplicaciones tras confirmar que la PC ha sido infectada por un virus, puesto que a las aplicaciones antivirus se les dificulta cada vez más protegerse una vez que el sistema operativo se ha visto vulnerado.

4. Cuatro ayudas

- **Antivirus:** detiene el virus antes de que infecte la PC.
 - ✓ Ejemplos de aplicaciones antivirus gratuitas: Avast!, Avira, AVG.
- **Antispyware:** bloquea las aplicaciones que envían su información a otras personas.
 - ✓ El spyware incluye, por ejemplo, capturadores de pulsaciones de teclado (véase el [Glosario](#)) que graban lo que el usuario escribe con el teclado y envían esa información a otra persona, de manera que dicha persona no tiene que ver la pantalla del usuario para descifrar la contraseña de este último para una cuenta determinada. Algunos ejemplos de aplicaciones antispyware gratuitas son Spybot y SUPERAntiSpyware.
- **Escáner de malware:** ubica y elimina una aplicación de un virus o spyware.
 - ✓ Un ejemplo de escáner de malware gratuito es Malwarebytes Anti-Malware.
- **Firewall:** bloquea el tráfico de Internet que usted no haya solicitado. Puede evitar la instalación involuntaria de software.
 - ✓ En ocasiones, un dispositivo o sitio web infectado puede intentar instalar un malware en su PC. Un firewall puede avisarle que esto está sucediendo y permitirle impedir la instalación. En la sesión [Profundización](#), incluimos información adicional acerca de Windows Firewall.

5. Actualice todo

- Aplicaciones antivirus
- El sistema operativo (p. ej., Windows)
- Todas las demás aplicaciones

- ✓ En cuanto al último punto, algunas aplicaciones no requieren que el usuario visite los sitios web uno por uno para descargarse las actualizaciones. El antivirus Avast! cuenta con un método integrado para verificar la versión de software. Igualmente, Secunia PSI busca actualizaciones de las aplicaciones que el usuario haya instalado.

6. Proteja sus datos con dos copias de seguridad

- Una que permanezca cerca y la otra en un lugar alejado.
 - ✓ Un ejemplo de un lugar alejado (también conocido como *off-site*) puede ser la Nube o la casa de un amigo. Así el usuario puede protegerse contra catástrofes naturales o el decomiso de los equipos en una oficina.
- Regularmente (p. ej., cada semana).
 - ✓ Para minimizar las pérdidas: aunque el usuario no pueda recuperarlo todo, al menos habrá perdido únicamente el trabajo de algunos días.
- Con una contraseña.
 - ✓ De esta manera, la copia de seguridad será tan segura como la original.

7. Bloquee las instalaciones involuntarias

- En Windows, asegúrese de que se está ejecutando el control de cuentas de usuario (*user account control*; UAC, por sus siglas en inglés).
 - ✓ Esto se puede hacer simplemente con lograr simplemente haciendo clic en Inicio y escribiendo UAC. El control deslizante jamás debería indicar Nunca notificar.

8. En un dispositivo móvil

- Ubique un software antivirus gratuito para la plataforma utilizada en la tienda oficial de aplicaciones del dispositivo.
 - ✓ Todas las grandes marcas fabrican uno, incluido Avast!
- No instale aplicaciones, papel tapiz (wallpaper) ni tonos de llamada (ringtone) que no necesite.
 - ✓ Estas aplicaciones pueden contener código dañino, o tal vez tengan acceso a información delicada a la que no necesitan tener acceso (p. ej., una aplicación de despertador que solicite acceso al registro telefónico).
- Ejecute todas las actualizaciones.

9. Si todo falla y está infectado

- Copie los archivos esenciales que no se incluyeron en la copia más reciente de seguridad que guardó en una unidad externa.
 - ✓ Dicho medio podría ser un DVD u otro dispositivo externo.
- Escriba toda la información de la licencia o información de compra de las aplicaciones que haya pagado (si las hay).
 - ✓ Esto es importante, ya que instalar el sistema operativo de nuevo eliminará toda la información que contenga el dispositivo.
- Asegúrese de guardar el disco de instalación.
- Instale de nuevo el sistema operativo y las aplicaciones.
 - ✓ Esto implica iniciar el disco de instalación, lo que incomodará a muchas personas. Nuestra recomendación es que busquen en su oficina ayuda del personal de apoyo para equipos de escritorio.

Pregunta frecuente:

- Mi copia de Windows no es original. ¿Apagará Microsoft mi equipo si intento actualizarla?
No. Microsoft hace actualizaciones de seguridad, disponibles para las copias de Windows, incluidas las copias pirata, pero las copias pirata no permiten tener acceso a todas las funciones de Windows. Los usuarios de copias pirata (software pirateado o no registrado) no pueden usar la función Microsoft Security Essentials. Windows tiene que poder reconocer el software como original para que los usuarios puedan usar la función de seguridad.



4. PROFUNDIZACIÓN (90 MINUTOS)

Esta sesión consta de dos partes: aplicaciones antimalware y actualizaciones. Recomendamos que la mayor parte de esta sesión se destine a hablar de la aplicación antivirus Avast! y, a continuación, de las actualizaciones. La aplicación adicional ClamWin Portable puede abordarse si sobra tiempo, pero los temas críticos que ayudarán a prevenir la mayoría de las infecciones se abordan en la Parte I y la II.

PARTE I: Aplicaciones antivirus

NOTA: Como se mencionó en “Ideas de conversación”, existen varias aplicaciones gratuitas que pueden ayudar a proteger la PC. Puesto que el tiempo es limitado, hemos elegido aplicaciones específicas para estos ejercicios, pero los capacitadores más duchos en la materia podrían explorar otras opciones.

A. Instalación y guía paso a paso de Avast!

Normalmente, recomendamos que los participantes instalen el software antes de entrar a la clase. En este caso, sin embargo, recomendamos esperar hasta llegar a este apartado del módulo, puesto que algunos participantes ya tendrán alguna aplicación antivirus instalada.

Antes de mostrarles a los participantes cómo instalar un antivirus, los capacitadores deben saber lo siguiente:

- **Los usuarios no necesitan más de una aplicación antivirus.** Tener más de un antivirus puede causar inestabilidad. Durante los ejercicios que mostramos a continuación, los participantes tendrán que poder demostrar que saben cómo actualizar su aplicación.
- **A todos los participantes que instalen un antivirus se les pedirá que reinicien la PC al finalizar el proceso de instalación.** No deberían elegir la opción de ejecutar un análisis en el arranque (*boot-time scan*, también denominado *escaneo programado para el inicio*). Solicite a los participantes que obvien la opción de ejecutar un análisis en el arranque cuando reinicien la PC. Un análisis en el arranque escaneará todo el contenido de la PC, y, mientras se esté ejecutando, no les permitirá a los participantes tener acceso al sistema operativo de Windows. Esto significará demoras para la clase.
- **Avast! tiene un diseño nuevo.** Al igual que otras aplicaciones, el diseño de Avast! cambia periódicamente. En noviembre de 2013, se actualizó la interfaz de la versión gratuita de la aplicación. Desafortunadamente, los materiales que proporcionamos no muestran los cambios visuales. Animamos a los capacitadores a estar atentos a YouTube y otros recursos destinados al público general para conseguir material actualizado que esté disponible después de la publicación de esta guía.

Materiales útiles:

- [Video de tutoría](#) (YouTube, en inglés);
- [Guía](#) (Security in-a-box);
- [Asistencia técnica de Avast!](#).

NOTA: Los capacitadores deberán señalar que Avast! cambió su diseño desde que se publicó el video y la guía que acabamos de mencionar. Es posible que algunas capturas de pantalla e imágenes del video sean diferentes a las que figuran en las instrucciones.

Los capacitadores tal vez quieran recalcar las siguientes ideas durante la presentación del video:

- Toda aplicación antivirus debe mantenerse actualizada para que esté al día con los nuevos virus que circulan por Internet.
- La versión gratuita de Avast! se actualizará automáticamente por lo menos una vez al día, pero el usuario puede ejecutar una actualización manualmente desde la pestaña de Configuración de la aplicación.
- Después de haber instalado Avast! y de haber reiniciado la PC, el usuario podrá analizar un archivo individual en su PC al seleccionar el icono de ese archivo, hacer clic derecho una vez y luego seleccionar Analizar (en el menú), junto al icono de Avast!

SOFTWARE E INSTALACIÓN

- Avast!
 - Guía
- ClamWin Portable
 - Guía

Si el capacitador puede determinar que la aplicación antivirus de un participante es pirata (la única forma de determinarlo es preguntando), se recomienda que dicho participante desinstale la aplicación antivirus pirata y acto seguido instale Avast!

Ejercicio nro. 1: Cómo actualizar Avast!

El capacitador mostrará a los participantes cómo actualizar Avast! desde dos ubicaciones:

- Con la aplicación abierta, el capacitador seleccionará la pestaña de Configuración y hará clic en el vínculo Actualizar. De esta manera, se actualizarán las definiciones de los virus y la aplicación misma.
- Desde la bandeja del sistema, el capacitador hará clic derecho en el ícono de Avast! y seleccionará Actualizar→Definiciones de motor y virus.

Estos dos pasos permitirán mostrarles a los participantes dos formas de hacer lo mismo.

Es recomendable que, a medida que los participantes lleven a cabo estas tareas, el capacitador se pasee por el aula para cerciorarse de que aquellos que utilicen otras aplicaciones antivirus también sepan actualizarlas.

Ejercicio nro. 2: Ejecutar un análisis rápido (o quick scan)

La aplicación de análisis rápido les permite a los usuarios ejecutar un análisis rápido del sistema, o uno completo. Un análisis completo del sistema analiza todos los archivos de cada disco duro relacionado con la PC. Por limitaciones de tiempo, recomendamos que la clase ejecute un análisis rápido, que limita la búsqueda a los archivos de sistema principales del sistema operativo. Para ello, haga lo siguiente:

- Seleccione la pestaña Análisis.
- El análisis rápido ya debería estar seleccionado por defecto en el menú desplegable.
- Haga clic en Comenzar.

IMPORTANTE: *Para evitar demoras, el capacitador podría pedirles a los participantes que detengan el análisis (al hacer clic en el botón Detener) y que ejecuten un análisis completo del sistema como tarea. El capacitador podría preparar su PC así, es decir, guardar un archivo infectado en el Escritorio para mostrar qué mensajes verían los participantes si tuvieran archivos infectados.*

Ejercicio nro. 3: Cómo actualizar otras aplicaciones con Avast!

El presente ejercicio tiene por objeto ayudar a los participantes a entender que pueden actualizar las aplicaciones de la PC y que Avast! cuenta con una función que les sirve para tal fin.

- Abra la ventana principal de Avast! (interfaz del usuario).
- Seleccione Herramientas y, después, Actualizador de software.
- Repase la lista de aplicaciones que aparezca y compruebe si alguna de ellas necesita actualización.

Consejos para usar Avast!

- Verá con frecuencia anuncios de ventas que lo invitan a que active actualizaciones supuestamente automáticas. Es así como Avast! intenta que los usuarios compren la versión de pago de la aplicación. Puede hacer caso omiso de estas invitaciones.
- Si tiene una tarjeta gráfica en la PC, en especial una tarjeta gráfica Nvidia, es probable que reciba un mensaje de alerta después de finalizar un escaneo completo del sistema. Dicho mensaje dirá: “No fue posible leer algunos archivos”. Al examinar los detalles del mensaje, normalmente encontrará que lo que no se pudo leer fue el controlador, un tipo de aplicación de la tarjeta gráfica. Lo anterior es normal y los participantes no tienen por qué alarmarse.
- Es recomendable ejecutar un análisis en el arranque por lo menos una vez para tener mayor seguridad de que la PC está limpia. Un análisis en el arranque examina los archivos de la PC que no estarían disponibles si Windows se estuviera ejecutando.

NOTA: *Los capacitadores pueden asignar como tarea que los participantes lleven a cabo un análisis en el arranque en vez de un análisis completo del sistema.*

B. Instalación y demostración de ClamWin Portable (OPCIONAL)

El objeto de la presente demostración es que los participantes vean que pueden llevar consigo una aplicación antivirus portátil en una memoria USB. Si el capacitador cree que este ejercicio no les interesará a todos los asistentes, podrá obviar este apartado y, en su lugar, pedir a los participantes que ejecuten un análisis completo del sistema. Si los participantes descubren que su PC está infectada, tendrán que remitirse a los [Apuntes de clase](#) para repasar los pasos a seguir.

Videos de tutoría: [Clamwin Ver.portable](#) y [ClamWin Technical support](#). Distribuya copias de ClamWin Portable (para usuarios de Windows) y ClamXav (para usuarios de Mac), idealmente con las definiciones de los virus ya descargadas.

- Explique algunas de las particularidades de ClamWin y ClamXav:
 - Es un programa antivirus FOSS (es decir, software gratuito de código abierto).
 - Carece de ciertas funciones que son importantes para programas antivirus comerciales, como, por ejemplo, protección en Internet.
 - Tiene la ventaja de estar disponible en versión portátil (para Windows), lo que le permite al usuario ejecutarlas desde una memoria USB en computadoras donde no tiene privilegios de administrador.
 - No lleva a cabo escaneos automáticamente, sino cuando lo ejecuta el usuario.
- Indique a los participantes que abran el programa y exploren las opciones que ofrece. Al hacer clic en Herramientas y Preferencias, deben ordenarle al programa que ponga en cuarentena los archivos infectados para que durante el análisis no se pierda información que podría ser importante.

Consejos para usar ClamWin:

- Hay una versión de ClamWin para MacOS llamada *ClamXav*.
- Una de las ventajas de usar un antivirus desde un dispositivo externo es que podría ser útil si el antivirus instalado en la PC llegara a infectarse o verse comprometido. También podrían ser útiles otras aplicaciones de “rescate”, como [AVG Rescue CD](#).

Recursos para ClamWin:

- [Sitio web oficial](#)
- [ClamWin Portable](#)
- [Cómo usar ClamWin](#)

Cómo ejecutar y actualizar ClamWin

- Los participantes tienen que abrir ClamWin desde un dispositivo externo.
- En la ventana principal de la aplicación, los participantes seleccionarán la herramienta de actualización para confirmar que las definiciones de los virus están actualizadas.

NOTA: Para el presente módulo, no se les pedirá a los participantes que instalen *Spybot* o *Comodo Firewall*, si bien podrán instalarlos después del módulo para aumentar su nivel de protección.

(Fuente para las instrucciones y el material de ClamWin: [LevelUp](#))

PARTE II: Su sistema operativo

Esta parte del presente módulo se centrará en mostrar dos funciones del sistema operativo de Windows que pueden ayudar a proteger su PC:

- Actualizaciones automáticas;
- Firewall de Windows.

A. Actualizaciones automáticas

Recomendamos que los capacitadores se sirvan de las instrucciones o el video que encontrarán a continuación para que los participantes ubiquen la configuración de las actualizaciones automáticas y para cerciorarse de que la función está activada.

Ideas de conversación:

- Debe actualizar el sistema operativo para estar protegido contra nuevas vulnerabilidades de seguridad, así como su aplicación antivirus y otras aplicaciones.
- Activar las actualizaciones automáticas evita que se le olvide actualizar manualmente el sistema operativo.
- Microsoft le presta ayuda para actualizar su sistema operativo, incluso si su versión de Windows es pirata. Tener software pirata no es recomendable, pero tampoco justifica que deje de actualizar su sistema operativo (no actualizarlo puede poner en peligro las computadoras de sus colegas).

Materiales útiles:

- **Guía:** [Cómo configurar y usar las actualizaciones automáticas en Windows](#) (Microsoft);
- **Video:** [How to Enable or Disable Automatic Updates in Windows 7](#) [Cómo activar o desactivar las actualizaciones automáticas en Windows 7] (válido también para Windows 8) (YouTube: MiamiURSC).

B. El Firewall de Windows

Recomendamos que los capacitadores se sirvan de las instrucciones o el video que encontrarán a continuación para que los participantes ubiquen la configuración del Firewall de Windows y para cerciorarse de que la función está activada.

Ideas de conversación:

- Todo firewall protegerá su PC de las conexiones de red que usted no haya solicitado.
- En concreto, esto ayuda a protegerse de infecciones por gusanos/virus que intentan propagarse automáticamente en cualquier PC con la que entran en contacto.
- Los firewalls no impiden que su PC acabe conectándose a la computadora de un pirata informático si su PC ya está infectada o si usted hace clic en un vínculo que lo conecte con la PC de dicho pirata.
- Se considera que el Firewall de Windows es un muro informático bastante básico. Si le interesa instalar un firewall más seguro que cuente con funciones adicionales (por ejemplo, que le muestre qué aplicaciones de su PC están enviando información a Internet), Comodo Firewall es una buena alternativa.

Materiales útiles:

- **Video:** [Turn On Windows Firewall Protection \(On/Off\)](#) [Active la protección del Firewall de Windows (On/Off)] (YouTube: TheMarketingMan);
- **Guía:** [Turn Windows Firewall On or Off](#) [Encienda/Apague Firewall de Windows] (Microsoft Support).

Para más ideas y actividades relacionadas, véase el sitio web de LevelUp.



5. SÍNTESIS (10 MINUTOS)

Sugerimos que los capacitadores se sirvan de esta sesión de recapitulación para hacer preguntas informales y repasar el material visto en este módulo. Las siguientes preguntas podrían ayudar a los participantes a poner en práctica lo aprendido:

- ¿Cuenta su oficina con un sistema para lidiar con los virus? ¿Las PC tienen instalados programas antivirus?
- ¿Aprendió algo que en su opinión deberían saber sus colegas? ¿Cómo podría decírselo?
- Si es usuario de computadoras públicas, como en cibercafés, ¿sospecha que puedan estar infectadas?
- ¿Qué palabras aprendió al comienzo del módulo?
- ¿Sobre qué conductas más seguras aprendió en este módulo, o acerca de cuáles está reflexionando?
- ¿Cuenta con un método para hacer copias de seguridad de sus archivos que estén “limpias” (es decir, que no estén infectadas con virus)?

SaferJourn: recursos de seguridad digital para capacitadores de medios de comunicación es un proyecto de Internews que complementa el trabajo hecho en [SpeakSafe](#) y [LevelUp](#). Creado y compartido bajo [licencia Creative Commons Attribution-NonCommercial 3.0 Unported \(CC BY-NC 3.0\)](#).



MAC OS X: MALWARE Y PROTECCIÓN BÁSICA

El material que presentamos a continuación incluye aplicaciones y ejercicios útiles para los participantes que tengan Mac OS X y dispositivos iOS. Los capacitadores que estén trabajando en parejas podrían repartirse las tareas durante los ejercicios de profundización. De esta manera, un capacitador puede trabajar con los usuarios de Windows o Android y el otro con los usuarios de OS X o iOS.

Software e instalación

- Aplicación antivirus [ClamXav](#)
 - [Guía](#).

Profundización

PARTE I: Aplicaciones antivirus

Ejercicios nro. 1 y nro. 2: Instalación y guía paso a paso de ClamXav

- Guía: [instalación](#)
- Guía: [cómo actualizar](#)
- Guía: [cómo ejecutar el primer análisis](#).

Materiales útiles:

- Video: [información general](#).

Ejercicio nro. 3: (No aplica)

Ejercicio nro. 4: Cómo actualizar aplicaciones

- Guía: [cómo actualizar](#).

Materiales útiles:

- Video: [How to Turn On Mac Auto Software Updates](#) [Cómo activar las actualizaciones de software automáticas para MAC].

PARTE II: Su sistema operativo

- Actualizaciones automáticas
 - Guía: [cómo actualizar](#)
- Firewall de OS X

Ideas de conversación:

- Apple vende sus dispositivos con los firewall deshabilitados por defecto, lo cual supone riesgos a menos que el usuario use el dispositivo con un enrutador que cuente con un buen firewall, y en ningún otro lugar.
- Vaya a Preferencias del sistema → Seguridad y privacidad → Firewall, para habilitar el firewall si está desactivado. Para llevar a cabo el paso anterior, tal vez tendrá que hacer clic en el candado que se encuentra en la esquina inferior izquierda de la pantalla y escribir la contraseña de administrador.
- Para programas validados que necesitan permisos para establecer conexiones salientes a través del firewall (mensajería instantánea, VoIP, etc.), el usuario tendrá que hacer una de estas dos cosas: o bien autorizar cada aplicación manualmente a medida que se van usando después de activar el firewall, o bien hacer clic en Opciones de firewall para permitir o para bloquear las conexiones entrantes para una aplicación dada. Recomendamos encarecidamente que bloquee las conexiones entrantes para todas las aplicaciones, a excepción de aquellas que estén validadas y que los usuarios sí usen. De lo contrario, este es un puerto de entrada común para el malware.
- En la página de Opciones de firewall, también se encuentra la opción Activar el modo silencioso. Recomendamos activarlo, pues ayuda a evitar que la computadora responda a solicitudes de información y datos que podrían ser hostiles.

MATERIALES ÚTILES:

- Guía: Opciones de firewall de Mavericks;
- Guía: Evitar conexiones no deseadas con un firewall;
- Guía: Cómo configurar las opciones de firewall para servicios y aplicaciones;
- Video: [How to enable the built-in firewall in your Mac OS X](#) [Cómo activar el firewall integrado en su Mac OS X].



APUNTES

Los virus son un GRAN problema

- Se han registrado decenas de miles de virus informáticos.
- El tiempo de supervivencia para una PC que no esté protegida es muy corto.

¿Quién crea los virus?

- Algunos piratas informáticos lo hacen por dinero (p. ej., [Conficker](#)).
- A veces, es un método empleado por los servicios de inteligencia: [Ghostnet](#).
- Otras veces... se crean porque sí: [ILoveYou](#).

Mitos más extendidos:

- Los virus solo atacan el sistema operativo Windows.
- Los virus no atacan los teléfonos inteligentes.
- Un antivirus siempre limpiará una PC infectada.

Tres ayudas:

- **Antivirus:** detiene el virus antes de que infecte la PC;
- **Antispyware:** bloquea las aplicaciones que envían su información a otras personas;
- **Escáner de malware:** ubica y elimina una aplicación de un virus o spyware;
- **Firewall:** bloquea el tráfico de Internet que usted no haya solicitado. Puede evitar la instalación involuntaria de software.
- **Actualice todo:**
 - las aplicaciones antivirus;
 - el sistema operativo (p. ej., Windows);
 - todas las demás aplicaciones.
- **Haga dos copias de seguridad:**
 - una que permanezca cerca y la otra en un lugar alejado;
 - regularmente (p. ej., cada semana).
- **Bloquee las instalaciones involuntarias:**
 - En Windows, asegúrese de que se está ejecutando el control de cuentas de usuario (*user account control*; UAC, por sus siglas en inglés).
- **En un dispositivo móvil:**
 - Ubique un software antivirus gratuito para la plataforma utilizada en la tienda oficial de aplicaciones del dispositivo.
 - No instale aplicaciones, wallpaper ni ringtones innecesarios.
 - Ejecute todas las actualizaciones.
- **Si todo falla y está infectado, haga lo siguiente:**
 - Copie los archivos esenciales que no se incluyeron en la copia más reciente de seguridad que guardó en un medio externo.
 - Escriba toda la información de la licencia o información de compra de las aplicaciones que haya pagado (si las hay).
 - Asegúrese de guardar el disco de instalación.
 - Instale de nuevo el sistema operativo y las aplicaciones.



GLOSARIO

Las siguientes definiciones de términos se proporcionan bajo [licencia Creative Commons Attribution-Share Alike 3.0 Unported](#) e incluyen entradas creadas por Tactical Technology Collective, Front Line Defenders e Internews.

El vocabulario relacionado con este módulo es el siguiente:

Avast! Herramienta antivirus gratuita.

inicialización o arranque (*booting*). Acto de inicializar una computadora.

computadora zombi (*botnet*). Conjunto de computadoras, normalmente infectadas por malware, que son controladas por piratas informáticos para varios fines, entre los que se encuentran los ataques cibernéticos que pueden deshabilitar sitios web o el envío en masa de correo basura.

aplicaciones portátiles. Programas que se ejecutan desde un dispositivo portátil, como puede ser una memoria USB o una tarjeta de memoria y que no es necesario instalar en el sistema operativo de la PC.

capturador de pulsaciones del teclado (*keylogger*). Tipo de spyware que graba lo que el usuario escribe con el teclado y envía esta información a terceros. Los capturadores de pulsaciones del teclado suelen utilizarse para robar contraseñas de cuentas de correo electrónico y otro tipo de contraseñas.

CCleaner. Herramienta freeware (es decir, software gratuito) que elimina del disco duro archivos temporales y rastros de información potencialmente delicada que han dejado tanto programas que el usuario acaba de utilizar como el propio sistema operativo de Windows.

ClamAV. Programa antivirus de código abierto para PC de escritorio y portátiles.

ClamWin. Interfaz gráfica del usuario (*graphical user interface*; GUI, por sus siglas en inglés) para Windows que permite a los usuarios tener acceso al antivirus ClamAv. Es posible ejecutar la versión portátil ClamWin desde una memoria USB.

ClamXav. Interfaz gráfica del usuario (GUI) para Mac OS que permite a los usuarios tener acceso al antivirus ClamAv.

copia de seguridad Cobian. Herramienta FOSS para hacer copias de seguridad. La versión más reciente de Cobian es un freeware de código cerrado, aunque las versiones anteriores se lanzaron como FOSS.

Firefox. Navegador FOSS muy conocido que proporciona una alternativa al navegador Internet Explorer de Microsoft.

firewall. Herramienta que protege la computadora de conexiones no seguras a redes locales e Internet.

Firewall Comodo. Herramienta firewall de freeware.

freeware. Software gratuito. Incluye software sin costo pero sujeto a restricciones legales o técnicas que no les permiten a los usuarios tener acceso al código utilizado para crear dicho software.

malware. Término general para referirse a todo el software malicioso, incluidos los virus, el spyware, los caballos de Troya y otras amenazas de este tipo.

nombre de dominio. Dirección, en palabras, de un sitio web o servicio de Internet (por ejemplo, [speaksafe.internews.org](#)).

NoScript. Complemento de seguridad del navegador Firefox que protege contra programas maliciosos que podrían estar presentes en sitios web desconocidos.

phishing (*ciberestafa*). Crear sitios web o correos electrónicos falsos que parecen ser legítimos para lograr que los usuarios de Internet caigan en la estafa e interactúen con los contenidos. Se usa a menudo para captar contraseñas e información financiera.

phishing con arpón. Tipo de ciberestafa que consiste en adaptar un sitio web falso o un correo electrónico falso para que parezca pertenecer legítimamente a un individuo o grupo específico.

pirata informático (*hacker*). En este contexto, delincuente informático malintencionado que intenta acceder a información delicada o tomar control vía remota de la computadora del usuario.

proveedor de servicios. Compañía privada o pública que presta a sus clientes servicios de telefonía móvil o servicios de Internet.

software gratuito de código abierto (*free and open-source software*; FOSS, por sus siglas en inglés). Familia de software que se consigue sin costo alguno y que no tiene restricciones legales que impidan a los usuarios probar el software, compartirlo o modificarlo.

Spybot. Herramienta freeware antimalware que analiza la computadora en busca de spyware para eliminarlo y protegerla del mismo.

spyware. Aplicación que, clandestinamente, lleva registro de las actividades y los datos del usuario de una PC y envía la información registrada a una computadora remota.

3. PROTECCIÓN DE DATOS



IMPORTANCIA DEL TEMA

Los periodistas, en particular quienes trabajan en zonas de alto riesgo, manejan información delicada, entre la que se encuentran listas de contactos, resultados de investigación para escribir artículos, fotografías y entrevistas. Puesto que almacenan mucha de esta información en dispositivos móviles, computadoras y en la Nube (p. ej. Dropbox), es importante que aprendan acerca de dos prácticas útiles:

- **Hacer copias de seguridad** para evitar pérdidas;
- **Cifrar los archivos** para evitar que se usen mal o para fines ilícitos.

Las copias de seguridad impiden que la información digital desaparezca, mientras que el cifrado evita que se tenga acceso no autorizado a la información.

LO QUE APRENDERÁN LOS PARTICIPANTES

Ideas: cifrado para PC y almacenamiento en la Nube.

Competencias: uso de TrueCrypt para cifrar información.

OBJETIVOS

Aprender acerca de la función de cifrado y cómo usarla

APLICACIONES PRÁCTICAS

Hacer copias de seguridad de la información delicada, proteger dicha información, transmitir datos de forma segura

CONOCIMIENTOS PREVIOS EXIGIDOS

El presente módulo parte de la base de que los participantes pueden instalar aplicaciones, así como ubicar archivos y guardarlos en su computadora.



NOTA PARA LOS CAPACITADORES: El presente módulo incluye la distribución y demostración de software cuyo uso tal vez no esté permitido por la ley en algunos países. Recomendamos que, antes de dictar este módulo, los capacitadores hagan una investigación básica acerca de la normativa local relativa al acceso a Internet de cada país donde se esté dictando la capacitación. En algunos lugares, por ejemplo, la ley no permite el uso del cifrado (incluidas las redes virtuales privadas, VPN por sus siglas en inglés, que se mencionan en nuestro estudio de caso).

ANTES DE COMENZAR

Los recursos que se enumeran a continuación podrían ayudar a los capacitadores a mejorar sus conocimientos acerca del tema del presente módulo antes de comenzar a dictarlo:

- Video: *Art of the Problem* [El arte del problema];
- Recurso general: “Journey Into Cryptography” [Viaje a la criptografía] (Khan Academy);
- Artículo: “The Spy Who Came in from the Code” [El espía que surgió del código] (Columbia Journalism Review).



MATERIALES

Además de los materiales de capacitación que recomendamos normalmente en la *Guía para capacitadores*, (véase el apartado “Consejos para la capacitación”), los capacitadores necesitarán lo siguiente para esta unidad didáctica:

Software e instalación

- TrueCrypt. (El paquete de idiomas en Español se encuentra [aquí](#))
 - Guía.

Documentos impresos a repartir

- Apuntes de clase
- Glosario
- Artículo: “The Hackers of Damascus” (Business Week)
- Guía: *Cómo instalar TrueCrypt y crear volúmenes comunes* (Security in-a-box)
- Guía: *Proteger los archivos sensibles en su computadora* (Security in-a-box).

NOTA: Los capacitadores que necesiten información acerca de los dispositivos Apple pueden consultar los [Apuntes de la capacitación de “Mac OS X”](#) que se encuentran justo después de la sesión de Síntesis de este módulo.



MÓDULOS RELACIONADOS

- Evaluación de riesgos
- Protección de su correo electrónico
- Seguridad para teléfonos celulares.

PLAN DE CLASE



1. ACTIVIDAD (15 MINUTOS)

Espectrograma

Esta actividad presenta afirmaciones en relación con el tema y les pregunta a los participantes si están “de acuerdo”, “en desacuerdo” o “ni sí ni no”. Lo que se pretende es trazar un espectro de opiniones en el salón, así como ayudar a los participantes a explorar varios puntos de vista.

Preparación

- El capacitador tendrá que hacer una lista de afirmaciones (véanse las sugerencias que presentamos a continuación) que pueden escribirse en una hoja de papel rotafolio con una raya vertical debajo de cada una, con la oración “Totalmente en desacuerdo” a un lado de la raya y “Totalmente de acuerdo” al otro. En caso de que no haya papel, las preguntas pueden leerse en voz alta.
- Materiales de grupo:
 - Cinta adhesiva protectora y tiza (o gis) de color;
 - Papel rotafolio y marcadores.
- Asegúrese de que haya suficiente espacio para que los asistentes puedan caminar (en algunos casos, tal vez sea útil trabajar en un lote de estacionamiento).

Sugerencias (deben ser afirmaciones cortas, directas y fáciles de entender):

- “A menor cantidad de información compartida, mayor seguridad”.
- “La información extraída de mi investigación para reportajes no es información delicada”.
- “Si alguien ha accedido a ser una de mis fuentes, no es necesario proteger su identidad”.
- “Es probable que en algún momento me roben o requisen la computadora o el teléfono”.
- “Mis datos están a salvo porque mi computadora está protegida con contraseña”.

Cómo organizar la actividad

1. El capacitador les pedirá a los participantes que se organicen en línea curva (en forma de la letra c). Si la actividad se lleva a cabo en lugares que no estén al aire libre, se recomienda una tiza (o gis) de color o cinta adhesiva protectora para usar en el suelo.
2. Después se indicará que una punta de la curva representa la afirmación “Totalmente de acuerdo” y la otra punta, “Totalmente en desacuerdo”.
3. Una vez que los participantes hayan entendido lo anterior, el capacitador leerá una de las sugerencias que se han aportado y les pedirá a los participantes que se ubiquen en algún punto del espectrograma compuesto por el espacio entre “Totalmente de acuerdo” y “Totalmente en desacuerdo”. Es posible que algunos participantes necesiten tiempo para pensar y probar varios puntos de la curva antes de tomar una decisión final.
4. El capacitador proseguirá y elegirá participantes al azar, a quienes les preguntará por qué se ubicaron en un punto determinado. ¿Han tenido alguna experiencia similar, o tal vez la haya tenido un amigo o colega?
5. Después de escuchar las respuestas de uno o dos participantes, es posible que otros asistentes quieran cambiar de ubicación. Se permite que los participantes cambien de posición.
6. Cuando todos hayan encontrado su lugar, el capacitador, en función de la ubicación de cada participante, escribirá signos grandes de *más* “+” y de *menos* “-” justo debajo de cada afirmación, e introducirá el puntaje calculado al sumar el total de signos de + y de -.
7. El capacitador pasará a la siguiente afirmación y repetirá los pasos del tres al seis para cada afirmación.
8. Al final del ejercicio, el capacitador pedirá a los participantes que lo ayuden a anotar las afirmaciones y los números en la pared.

(La presente actividad, “*Espectrograma*”, ha sido extraída de [LevelUp](#), y de las descripciones que figuran en [Aspiration Facilitation wiki](#) y [P2PU](#).)

RECORDATORIO

Si el presente módulo es el primero de un taller más amplio, sugerimos que los capacitadores dediquen los primeros 10 minutos a trabajar con el grupo para definir los lineamientos de conducta y seguridad. Para más información, véase el apartado “*Formalización de un contrato*” de la *Guía para capacitadores*.

Este ejercicio hace que los participantes se formen opiniones acerca de los temas y reconozcan que un tema puede evaluarse de varias formas y que no pasa nada si uno cambia de opinión.



2. DEBATE (15 MINUTOS)

Una vez que la actividad haya concluido, los capacitadores pedirán a los participantes que se sienten en círculo o en medio círculo para que puedan dirigirse los unos a los otros. Las preguntas que presentamos a continuación pueden ser útiles para dar inicio al debate.

- ¿Qué clase de información suelen guardar los periodistas en la computadora?
- ¿Y en el teléfono inteligente?
- De esos equipos, ¿cuál es el más importante para el periodista? ¿Qué pasaría si alguien se lo robara?
- ¿Algún participante ha perdido información delicada alguna vez? ¿Cómo sucedió?
- ¿Alguien conoce casos relacionados con el tema?
- ¿Qué hacen actualmente los asistentes de la capacitación para proteger la información que guardan en su PC y en su celular?

NOTA: Se recomienda animar a cada quien a que comparta su “método”. Puede preguntarles por qué lo hacen así a fin de entender si están tomando estas medidas a conciencia.

- ¿Hacen los participantes copias de seguridad de su información?
- ¿Y usted, almacena información en Dropbox o en la Nube? ¿Cree que estos programas pueden presentar vulnerabilidades?

Los capacitadores tienen plena libertad para añadir elementos a la lista o improvisar según lo estimen oportuno.



3. INFORMACIÓN/EXPOSICIÓN (30 MINUTOS)

Esta sesión incluye un estudio de caso recomendado, ideas clave y algunos materiales para ayudar a transmitir la idea que se está abordando.

Estudio de caso

“El espía que surgió del código”

Presentación: Incluso los periodistas con amplia experiencia pueden perder el celular o la computadora por robo, catástrofe natural, o, como veremos, decomiso por parte de las autoridades. Cuando esto sucede, los periodistas no solo pierden información importante, sino que ponen en peligro a sus fuentes.

Historia: En el otoño de 2011, el periodista y cineasta inglés Sean McAllister se puso en contacto con Dīshad Othman, un joven activista kurdo de Siria y especialista en informática que vivía en Damasco. McAllister estaba rodando un documental para el Channel 4 en el Reino Unido acerca de los activistas clandestinos sirios y buscó a Othman para que le ayudara a hacer contactos.

McAllister, galardonado cineasta que había participado en rodajes en otras zonas de conflicto, incluidos Yemen e Iraq, había encontrado la manera de entrar al país clandestinamente, aunque el Gobierno sirio había dejado de otorgar visas a los periodistas internacionales.

Othman estaba ayudando a reporteros, activistas en derechos humanos y a la resistencia mediante herramientas de comunicación segura, y también estaba organizando servidores de red virtual privada (VPN) fuera del país. Él y otros activistas eran precavidos con su seguridad y tomaban medidas tales como cifrar sus comunicaciones, usar herramientas anonimizadoras, cifrar lo que almacenaban, etc.

Cuando el régimen del presidente Bashar al-Assad comenzó a tomar medidas drásticas en contra de los activistas políticos, Othman pensó que McAllister lograría contarle al mundo la historia de lo que estaba sucediendo y accedió a concederle a McAllister una entrevista acerca de su trabajo. En la entrevista ante las cámaras, el cineasta le aseguró a Othman que protegería su identidad y que, en la grabación final, su cara aparecería borrosa para evitar que fuera identificado. Othman también puso a McAllister en contacto con otros activistas.

Sin embargo, Othman recuerda comenzar a sentirse incómodo al observar algunas de las prácticas profesionales de McAllister. Se dio cuenta de que McAllister usaba su celular y SMS sin cifrado y que dejaba información no cifrada en su apartamento, incluidas filmaciones sin editar de entrevistas con activistas tras cuya pista se encontraba el Gobierno sirio. Asimismo, Othman sintió que McAllister no se daba cuenta de lo agresiva que era la vigilancia del régimen sirio, de los riesgos que corrían los activistas al acceder a hablar con él, y de las consecuencias que para los activistas acarrearía el ser señalados y expuestos.

Algunos días después de la entrevista que Othman le concedió a McAllister, Othman oyó que los agentes de seguridad sirios habían allanado el hotel de McAllister, lo habían arrestado y le habían confiscado la computadora portátil, el teléfono celular, la cámara, la filmación sin editar y lo que había investigado hasta ese momento, incluidos los nombres e información de contacto de sus fuentes.

Othman apagó su teléfono celular, sacó la tarjeta SIM del celular y abandonó el país poco después. También huyeron otros activistas a quienes McAllister había contactado. Muchos de los que no huyeron, o que no pudieron hacerlo, fueron arrestados, entre ellos el activista Omar al-Baroudi, quien había concedido una entrevista ante las cámaras y cuyo número telefónico estaba en el celular de McAllister. Baroudi desapareció al día siguiente y no se sabe nada de él desde entonces.

El régimen sirio también apoya la organización hacker proregimen Syrian Electronic Army (SEA). Los *hacktivistas* del SEA han atacado las plataformas digitales de los diarios *The Washington Post*, *The Telegraph*, *The Independent* y de Al Jazeera, y han inundado con propaganda a favor del régimen las cuentas de Twitter de la BBC Weather y la Associated Press. Este año, el SEA atacó el sitio web de *The New York Times*, debido a lo cual dicho sitio web permaneció caído durante más de 20 horas.

Los capacitadores tienen plena libertad para añadir más información o improvisar según lo estimen oportuno.

Referencias:

“The Spy Who Came in from the Code” [El espía que surgió del código] (Columbia Journalism Review).

Videos de apoyo:

- *Syrian Uprising: The Internet has been Central to the Revolution* [El alzamiento sirio: Internet ha sido crítica para la revolución] (*The Guardian*)
- *Interview: Dlshad Othman* [Entrevista con Dlshad Othman] (video del *Huffington Post*)
- *Sean McAllister: British Filmmaker Detained and Released from Syria* [Sean McAllister: cineasta inglés detenido y liberado en Siria] (CITIZENSYRIA, YouTube).

Grabaciones de audio de apoyo:

- *Reporters Unwittingly Exposing Sources* [Periodistas que exponen a sus fuentes sin saberlo] (<http://www.onthemedial.org/story/204629-reporters-unwittingly-exposing-sources>).

Interacción con los participantes

A partir del ejemplo de Othman, los capacitadores podrán ayudar a los participantes a reflexionar acerca de prácticas propias que podrían estar poniendo en peligro a sus fuentes. Suscite la participación activa de los asistentes mediante un debate sobre las siguientes preguntas:

- ¿Qué pudo haber hecho McAllister de otra forma?
- ¿Hizo Othman lo correcto al irse del país? ¿Se precipitó demasiado?
- En caso de que lo arrestaran a usted y le confiscaran sus herramientas, ¿peligrarían sus fuentes?

Ideas de conversación para el capacitador

Después de presentar el estudio de caso, el capacitador remitirá a los participantes a los [Apuntes de clase](#).

1. El cifrado convierte los archivos, que pasan de lucir como los vemos normalmente a obtener un formato protegido:

- Para desbloquear el archivo nuevamente, suele necesitarse una clave (o contraseña).
 - ✓ Si no conocemos la contraseña o la clave, no es posible convertir los archivos a un formato que reconozcamos.

Demostración de video: *What is a Caesar Cipher?* [¿Qué es un Ceasar Cipher?] (Khan Academy).

2. Ventajas:

- Ofrece protección: no hay acceso sin permiso (o clave);
- puede ser útil para celulares, computadoras PC y la Nube.

3. Sin embargo...

- Funciona únicamente para los archivos o dispositivos que el usuario quiera cifrar.
 - ✓ Si el usuario tiene una foto en el disco duro y una copia de esa misma foto en Facebook, cifrar la que está en el disco duro no incidirá en la que tiene en Facebook.
- No siempre oculta lo que está en un dispositivo.
 - ✓ Si el usuario abre un documento Word en su PC, lo edita, y después lo cierra y lo cifra, el archivo queda bloqueado, pero alguien que examine su PC podría ver rastros de que el documento se abrió recientemente. Esto podría verse en la lista de Documentos recientes de Word, por ejemplo, o el archivo podría aparecer si se hiciera una búsqueda.

NOTA PARA LOS CAPACITADORES

Los textos con un ✓ no figuran en los Apuntes de clase de las copias a repartir a los estudiantes.

4. Actualmente, la mayoría de los dispositivos vienen con herramientas de cifrado que permiten cifrar todo un disco (cifrado de disco completo) o “contenedores” o discos más pequeños, incluidas las memorias USB:

- Windows = BitLocker
- MacOS = FileVault
- Android y iPhone (integrado en la configuración)
 - ✓ Cabe destacar que es muy importante que, antes de aplicar el cifrado de disco completo, el usuario debe hacer copias de seguridad de sus datos (y de otros archivos fundamentales). El cifrado de disco completo puede tardar varias horas, y los apagones de luz mientras se está ejecutando el proceso podrían dañar la información del disco duro. Se recomienda que los alumnos interesados en hacer copias de seguridad de su información visiten el sitio web de [LevelUp](#).

5. Los riesgos del cifrado:

- El cifrado puede detectarse.
- En algunos países, el uso del cifrado está prohibido por la ley.
- No todo el cifrado supone una buena protección.
- El mero hecho de que un archivo esté cifrado no significa que deje de aparecer en la lista de Documentos recientes o en los resultados de una búsqueda.
 - ✓ **Por ejemplo:** la esteganografía –forma de ocultar información en un archivo (como guardar un mensaje dentro de lo que parece ser una fotografía común y corriente)– se presta al reconocimiento de patrones.
- Incluso un cifrado supuestamente bueno depende de lo buena que sea la contraseña utilizada para bloquearlo.
 - ✓ Las contraseñas “Password” y “passw0rd” siguen figurando entre las [contraseñas más utilizadas](#) del mundo, según la compañía de seguridad de software SplashData. Sin embargo, es importante recordar que utilizar una contraseña no es equivalente a emplear cifrado. Windows le permite al usuario proteger su cuenta de una PC con una contraseña, por ejemplo. Esta interesante función, que le permite al usuario personalizar su experiencia (mediante distintos wallpapers o aplicaciones) en una misma computadora, no cuenta con cifrado de información en la unidad de disco a no ser que el usuario haya activado BitLocker específicamente.

6. Cifrado + “3-2-1” = buenas copias de seguridad

La regla del “3-2-1” quiere decir que la mejor forma de hacer copias de seguridad de los datos es la siguiente:

- Tenga tres copias (el archivo original más otras dos copias).
- Manténgalas en dos ubicaciones distintas.
- Una de esas ubicaciones debe ser externa (lejos de la oficina).
 - ✓ Este sistema pretende garantizar que tenga un copia a mano, en caso de emergencia, pero que una segunda copia permanezca en otro lugar, en caso de decomiso o catástrofe natural en una de las ubicaciones.
 - ✓ Además, cifrar las copias de seguridad mantiene la información a salvo en la propia copia de seguridad.

7. TrueCrypt (en lo que nos centramos hoy):

- Es de código abierto.
- Se puede ejecutar en PC, Mac OS, Linux.
- Es portátil (funciona en memorias USB).
 - ✓ Los periodistas especializados en derechos humanos y los expertos en seguridad (como Bruce Schneier) se valen frecuentemente de TrueCrypt. Actualmente, se está llevando [a cabo un proyecto para confirmar que dicha aplicación no presenta vulnerabilidades ocultas](#), lo que la diferencia de las aplicaciones de código cerrado.



4. PROFUNDIZACIÓN (90 MINUTOS)

Este apartado se centra en el uso de TrueCrypt. También incluimos un ejercicio opcional referente a las contraseñas en caso de que sobre tiempo. Este puede ser un buen momento para que los capacitadores repartan los documentos impresos acerca de TrueCrypt.

Otros recursos que pueden ser útiles:

- Guía: [Cómo instalar y usar TrueCrypt](#) (Security in-a-box);
- Artículo: “[TrueCrypt FAQs](#)” [TrueCrypt, preguntas más frecuentes] y “[Help](#)” [Ayuda] (www.truecrypt.org);
- Video: [TrueCrypt Full Disk Encryption on Windows 7](#) [Cifrado de disco completo TrueCrypt en Windows 7] (CryptNode).

Ejercicio nro. 1: Cómo crear un volumen cifrado

El presente ejercicio es una demostración de la función más básica que ofrece TrueCrypt: hacer una carpeta cifrada en la que se puedan almacenar archivos de manera segura.

NOTA: El nombre que TrueCrypt da a las carpetas es *volúmenes*. Algunos capacitadores prefieren usar el término *dispositivo secreto*, de más fácil comprensión para los participantes. Al segundo ejercicio le sigue inmediatamente otro que tiene por objeto ayudar a los participantes a recordar dicho término.

- El capacitador creará un volumen con TrueCrypt, que estará instalado en el portátil que usará para la demostración. Las mejores instrucciones para este procedimiento se encuentran en el documento "[Instalar TrueCrypt y crear volúmenes comunes](#)," en el sitio web de Security in-a-box, aunque los videos que se enumeran a continuación también son útiles para repasar estos pasos:
 - [Using TrueCrypt to Create an Encrypted Volume](#) [Cómo crear un volumen cifrado con TrueCrypt];
 - [How to Encrypt a USB Drive Using TrueCrypt](#) [Cómo cifrar una memoria USB con TrueCrypt].
- Puesto que TrueCrypt puede llegar a ser complejo, recomendamos encarecidamente que los capacitadores repitan la demostración antes de pedirles a los participantes que creen su propio volumen común. Llegado el momento en que los participantes hagan el intento, nuestra recomendación es que:
 - El volumen sea de tamaño pequeño (1-2 MB);
 - Recuerden dónde crearon el volumen (para que puedan encontrarlo);
 - No olviden qué contraseña usaron en el paso de creación.

NOTA: El capacitador deberá dedicarle tiempo a cada participante para cerciorarse de que todos han creado un volumen.

Ejercicio nro. 2: Cómo abrir un volumen cifrado

El presente ejercicio tiene por objeto que los participantes aprendan a usar el volumen recién creado:

- Con TrueCrypt abierto, el capacitador deberá “montar” (es decir, abrir) su volumen cifrado.
- Algo clave en lo que debe insistirse es que el volumen tiene dos vías de acceso:
 - Al hacer clic en el nombre del volumen en la interfaz de TrueCrypt;
 - Mediante Mi equipo (para Windows) o Equipo (para MacOS), que “ven” el volumen como disco duro.
- El capacitador luego “desmontará” el volumen.
- Recomendamos que el capacitador repita la demostración al menos una vez antes de invitar a los participantes a que lo intenten por sí mismos.
- Llegados a este momento del ejercicio, el capacitador podría pasearse por el salón para ayudar a los participantes y comprobar que todos han podido abrir (es decir, montar) y cerrar (es decir, desmontar) sus volúmenes.

SOFTWARE E INSTALACIÓN

- [TrueCrypt](#). (El paquete de idiomas en Español se encuentra [aquí](#))
 - [Guía](#).

- Ideas principales que deben recalcar cuando los participantes estén llevando a cabo el ejercicio:
 - Cuando el volumen está montado (es decir, abierto), no está cifrado.
 - Cuando está desmontado (es decir, cerrado), está bloqueado/cifrado.
 - Es igual que cerrar una caja con llave: cuando uno la abre con la llave, permanece abierta hasta que uno la vuelve a cerrar.
- Una vez que todos los participantes hayan terminado el ejercicio, el capacitador podrá abrir un turno de preguntas. Suelen surgir, entre otras, las siguientes preguntas:
 - **¿Puedo hacer una copia de mi volumen?**
Sí. Es como un archivo en su computadora: se puede copiar y pegar y hacer copias perfectas. Esta es una de las formas posibles de usar TrueCrypt para hacer copias de seguridad, es decir, dejar un volumen en su PC de la oficina y otro en una unidad externa, por ejemplo.
 - **¿Existe un límite en cuanto al tamaño de un volumen?**
No que sepamos. Puede pesar cientos de gigabytes, o puede ser del tamaño de su PC. Lo remitimos a las instrucciones sobre el tema en los [Apuntes de clase](#).
 - **¿Qué es un volumen oculto?**
Se trata de una función avanzada. Quiere decir que usted puede bloquear su volumen con dos contraseñas en vez de una. Estas dos contraseñas juntas pueden abrir el 100 % del volumen. Por separado, sin embargo, solo pueden abrir una parte del volumen. De manera que, si alguien abre un volumen con la primera contraseña, solo podrá ver los archivos que corresponden a dicha contraseña. Encontrará más información al respecto en los documentos impresos que se entregarán a los participantes. Sin embargo, no recomendamos incluir esta función en el temario de la capacitación. Es fácil destruir información sin querer, lo que no debería ser necesario en ningún caso excepto en los más críticos.
 - **¿Qué es un archivo con llave o *archivo key (key file)*?**
Cuando crea un volumen, TrueCrypt le pregunta si desea asociarlo a un archivo con llave, además de asociarlo a su contraseña. Usar un archivo con llave o clave es parecido a la verificación en dos pasos de Gmail o Facebook (para más detalles, véase el módulo Protección de su correo electrónico). Quiere decir que para abrir su volumen tiene que proporcionar al mismo tiempo tanto una contraseña como un archivo (cualquier archivo, por ejemplo, un .txt o una foto). Si bien ofrece un nivel adicional de protección, también crea un riesgo adicional: si pierde su archivo con llave –al eliminarlo accidentalmente, por ejemplo–, ya no podrá abrir el volumen asociado a este.
 - **¿Qué es un *traveler disk* (a veces denominado en español *disco viajero*)?**
Es un término curioso que TrueCrypt utiliza para su versión portátil. TrueCrypt se puede instalar en una memoria USB, por ejemplo, y ejecutarse desde allí. Esta opción se encuentra en el menú de Herramientas, pero rogamos que esto se investigue después de la clase.

Ejercicio nro. 3: Lograr que los volúmenes sean de distintos tamaños

Antes de comenzar, los capacitadores deben repasar con los participantes las etiquetas poco comunes que TrueCrypt usa para referirse a conceptos o botones de navegación que se conocen por otros nombres:

- *Montar* significa “abrir”.
- *Desmontar* significa “cerrar”.
- Un *volumen* es una carpeta secreta o un disco secreto.

El presente ejercicio está pensado para ayudar a los participantes a sentirse más seguros cuando usen TrueCrypt. No solo les aportará más experiencia en cuanto al proceso de crear un volumen de TrueCrypt, sino que también les ayudará a familiarizarse con la elección del tamaño del volumen en función del tamaño del material que se esté almacenando:

- El capacitador les pedirá a los participantes que elijan en su PC una fotografía, canción o video divertidos que les gustaría compartir.

- Cuando los participantes estén listos, se les pedirá que elijan a un “compañero secreto”, alguien cerca a quien enviarán el archivo.
- Los compañeros secretos deben llegar a un acuerdo en cuanto a la contraseña que ambos usarán para este ejercicio.
- Una vez elegidas las contraseñas, los participantes podrán crear un volumen de un tamaño adecuado para el archivo que van a compartir.
NOTA: *Cada participante creará un volumen pequeño para intercambiar con su compañero. El capacitador tal vez quiera advertirles a los participantes que el tamaño de lo que compartan no puede superar el tamaño del volumen creado. De lo contrario, saldrá un mensaje de error.*
- Una vez que todos hayan creado un volumen, deberán montar (es decir, abrir) su volumen y colocar su archivo dentro.
- A continuación, deberán desmontar (o sea, cerrar) su volumen.
- Y ahora, es el momento de compartir: los compañeros secretos intercambiarán volúmenes.
NOTA: *El capacitador podrá asignar una serie de métodos. Por ejemplo, enviar volúmenes adjuntos por correo electrónico o intercambiar memorias USB.*
- Como paso final, los compañeros montarán (abrirán) los volúmenes que reciban usando las contraseñas acordadas al comienzo del ejercicio.
- Repitan estos pasos al menos tres veces o hasta que los participantes se sientan cómodos con el proceso de creación y la idea de definir el tamaño de un volumen.
- Ideas que se deben recalcar cuando los participantes estén llevando a cabo el ejercicio:
 - Estamos viendo un segundo uso de TrueCrypt: puede proteger archivos en la PC y ayudarnos a transferir archivos a otras personas.
 - Si usted comparte una contraseña para un archivo, ¿debe enviarla en un correo electrónico que tiene adjunto dicho archivo? (No). ¿Cómo puede compartir una contraseña de forma más segura? (No hay una única respuesta. Lo mejor es ponerse de acuerdo acerca de una contraseña en persona. De no ser posible, sin embargo, es fundamental que los periodistas usen cualquier otro medio distinto del que usan para compartir el volumen.)
 - Los volúmenes de TrueCrypt pueden subirse a Dropbox u otros servicios de uso compartido de archivos.

Ejercicio OPCIONAL

Si hay tiempo suficiente, los capacitadores podrán repasar junto con los participantes algunas de las recomendaciones para crear contraseñas seguras. ¿Por qué? Si una contraseña es débil (corta, fácil de adivinar), el cifrado no servirá de mucho. La importancia de que las contraseñas sean largas y seguras es suma.

Para el presente ejercicio, recomendamos que los capacitadores usen como material de referencia el capítulo de Security in-a-box titulado "[Cómo crear y mantener contraseñas seguras](#)", o este resumen de [SpeakSafe](#) (Capítulo 2: Proteger su información).

Para más ideas y actividades relacionadas, véase el sitio web de [LevelUp](#).



5. SÍNTESIS (15 MINUTOS)

Sugerimos que los capacitadores se valgan de esta sesión de recapitulación para hacer preguntas informales al grupo, estimular el debate y repasar el material visto en este módulo. Puesto que el presente módulo se centró en TrueCrypt, los capacitadores tal vez quieran mencionar lo siguiente antes de abrir la sesión:

- Si usted tiene un teléfono Android o iPhone, también puede activar la opción de cifrado de su celular. Para activar dicha opción en Android, vaya a Configuración→Seguridad→Cifrar teléfono.
- Los usuarios de iPhone encontrarán instrucciones y una lista de los dispositivos compatibles con cifrado en el sitio web de [Ayuda](#) de Apple.

Las siguientes preguntas podrían ayudar a los participantes a poner en práctica lo aprendido:

- ¿Cómo cree usted que podría usar el cifrado en la oficina?
- ¿Cree que el cifrado es parte de nuestro compromiso con la protección de nuestras fuentes? ¿Por qué?
- ¿El cifrado garantiza que nadie tenga acceso a sus archivos? ¿Qué podría pasar?
Podría adivinarse la contraseña. O usted podría verse obligado a entregar una contraseña.

Otras preguntas que podrían ayudar a los participantes a repasar lo visto en este módulo:

- Si su copia original de un archivo está segura y cifrada, pero su copia de seguridad no lo está, ¿se encuentra a salvo su información?
No.
- ¿Cree que el cifrado proporciona protección contra los virus?
No.
- Si la copia original que se encuentra en su PC está cifrada, pero la versión que tiene en Dropbox no lo está, ¿se encuentra a salvo su información?
No.
- Cuando almacenamos una fotografía en una PC en un volumen cifrado, ¿quedan cifradas automáticamente las copias de esa fotografía que ya están cargadas a la Web?
No.

SaferJourno: recursos de seguridad digital para capacitadores de medios de comunicación es un proyecto de Internews que complementa el trabajo hecho en [SpeakSafe](#) y [LevelUp](#). Creado y compartido bajo [licencia Creative Commons Attribution-NonCommercial 3.0 Unported \(CC BY-NC 3.0\)](#).



MAC OS X: PROTECCIÓN DE DATOS

El material que se muestra a continuación incluye aplicaciones y ejercicios que podrían ser útiles para los participantes que tengan dispositivos Mac OS X e iOS. Los capacitadores que estén trabajando en parejas tal vez quieran repartirse las tareas durante los ejercicios de profundización. De esta manera un capacitador puede trabajar con los usuarios de Windows o Android y el otro, con los usuarios de OS X o iOS.

Información

Ideas de conversación para el capacitador

Es posible que, para el cifrado de disco completo, algunos periodistas quieran usar la herramienta de cifrado integrada para Mac OS X *FileVault 2*, y usar TrueCrypt para cifrar ciertos archivos o secciones del disco. Esta puede ser una táctica eficaz si lo que desea es ocultar archivos o documentos específicos en un entorno donde tal vez se vea obligado a compartir la información de inicio de sesión para su computadora con alguien en quien no confía.

Materiales útiles:

- Guía: [Acerca de FileVault 2](#) (Apple Support).



GLOSARIO

Las definiciones de términos que se muestran a continuación se proporcionan bajo [licencia Creative Commons Attribution-Share Alike 3.0 Unported](#) e incluyen entradas creadas por Tactical Technology Collective, Front Line Defenders e Internews.

El vocabulario relacionado con este módulo es el siguiente:

aplicación portátil. Programa que puede utilizarse en un dispositivo portátil, como una memoria USB o una tarjeta de memoria, y que no requiere que se instale en el sistema operativo de la PC.

BitLocker. Aplicación en las versiones Enterprise y Ultimate de Windows Vista, Windows 7 y Windows 8 que protege tanto unidades de disco duro como unidades externas.

cifrado. Forma de usar las matemáticas para *cifrar* información, o codificarla, de manera que solo pueda *descifrarla* y leerla quien tenga una pieza específica de información, como una contraseña, o una clave o llave de cifrado.

esteganografía. Método para ocultar información delicada a fin de que aparente ser otra cosa y no llame la atención.

inicialización o arranque (*booting*). Acto de inicializar una computadora.

Firefox. Navegador FOSS muy conocido que proporciona una alternativa al navegador Internet Explorer de Microsoft.

pirata informático (*hacker*). En este contexto, delincuente informático malintencionado que intenta acceder a información delicada o tomar control vía remota de la computadora del usuario.

software gratuito de código abierto (*free and open-source software*; FOSS, por sus siglas en inglés). Familia de software que se consigue sin costo alguno y que no tiene restricciones legales que impidan a los usuarios probar el software, compartirlo o modificarlo.

TrueCrypt. Herramienta FOSS para cifrado de archivos que permite almacenar información delicada de manera segura.

4. INVESTIGAR DE MANERA SEGURA



IMPORTANCIA DEL TEMA

Según informes recientes, no hay mucho que podamos hacer en Internet que sea totalmente seguro. A modo de ejemplo, podría ser que los periodistas que investigan en Internet para sus reportajes estén dejando registro de sus actividades en sus computadoras PC y en la Web, lo que podría potencialmente comprometer su seguridad y la de sus fuentes a la hora de investigar historias que otros estén queriendo ocultar. Asimismo, es posible que algunos periodistas se frustren al ver que algunas de las fuentes clave para su investigación no se encuentran donde ellos viven.

LO QUE APRENDERÁN LOS PARTICIPANTES

Ideas: conexiones a Internet seguras vs. conexiones que no lo son, huellas.

Competencias: usar una red virtual privada (VPN), usar Tor.

OBJETIVOS

Aprender cómo funciona Internet y a reducir la huella que allí dejamos

APLICACIONES PRÁCTICAS

Investigar temas delicados, evitar filtros de contenido, publicar de manera anónima

CONOCIMIENTOS PREVIOS EXIGIDOS

El presente módulo parte de la base de que los participantes saben hacer lo siguiente:

- Identificar sistemas operativos;
- Instalar aplicaciones;
- Guardar y ubicar archivos en sus computadoras.



NOTA PARA LOS CAPACITADORES: El presente módulo incluye la distribución y demostración de software cuyo uso tal vez no esté permitido por la ley en algunos países. Recomendamos que, antes de dictar este módulo, los capacitadores hagan una investigación básica acerca de la normativa local relativa al acceso a Internet de cada país donde se esté dictando esta capacitación. En algunos lugares, por ejemplo, la ley prohíbe el uso de redes virtuales privadas (que se abordan en el presente módulo).

ANTES DE COMENZAR

Los recursos que se enumeran a continuación podrían ayudar a los capacitadores a mejorar sus conocimientos acerca del tema del presente módulo antes de comenzar a dictarlo:

- "Navegar por internet de manera más segura" (Internews: Capítulo 4 de SpeakSafe);
- Guía: *Mantenerse en el anonimato y evadir la censura en Internet* (Security in-a-box);
- Video: *The Internet Explained* [Qué es Internet] (YouTube);
- Gráfico interactivo: *Tor and HTTPS* (EFF.ORG);
- Artículo: "How (and Why) to Surf the Web in Secret" [Cuándo y por qué navegar la Web en secreto] (PC World).

El presente módulo ayudará a los periodistas a instalar y usar software que puede aportarles mayor privacidad al investigar en Internet, así como darles acceso a recursos a los que no podrían acceder sin este tipo de ayuda.



MATERIALES

Además de los materiales de capacitación que recomendamos normalmente en la *Guía para capacitadores*, (véase el apartado "Consejos para la capacitación"), los capacitadores necesitarán lo siguiente para esta unidad didáctica:

Software e instalación

- CCleaner
 - Guía
- BleachBit
 - Guía
- Psiphon 3
 - Guía
- Tor Browser Bundle [Paquete de navegador de Tor]
- Navegador Web Firefox.

Documentos impresos a repartir

- Apuntes de clase
- Glosario
- "Mantenerse en el anonimato y evadir la censura en Internet" (Security in-a-box)
- "Tor - Anonimato y Camuflaje" (Security in-a-box).

NOTA: Los capacitadores que necesiten información acerca de los dispositivos Apple pueden consultar los *Apuntes de la capacitación de "Mac OS X"* que se encuentran justo después de la sesión de Síntesis de este módulo.



MÓDULOS RELACIONADOS

- Protección de su correo electrónico
- Seguridad para teléfonos celulares.

PLAN DE CLASE



1. ACTIVIDAD (20 MINUTOS)

Nosotros somos Internet

El objetivo de la presente actividad es ilustrar cómo funciona Internet y que los participantes vean todo lo que dejamos al descubierto o exponemos acerca de nosotros mismos cada vez que abrimos Internet.

Preparación

Antes de clase, el capacitador debe escribir las palabras que se enumeran a continuación en tarjetas y en letra grande:

- Wi-Fi;
- Proveedor de servicios de Internet (*Internet service provider*; ISP, por sus siglas en inglés);
- Enrutador;
- Proveedor de servicios de Internet (*Internet service provider*; ISP, por sus siglas en inglés);
- Puerta de entrada o de enlace;
- Proveedor de servicios de Internet (*Internet service provider*; ISP, por sus siglas en inglés);
- Enrutador;
- Proveedor de servicios de Internet (*Internet service provider*; ISP, por sus siglas en inglés);
- Sitio web.

Cómo empezar

- El capacitador les pedirá a tres voluntarios que se hagan pasar por periodistas, y les indicará que se pongan de pie juntos en un lado del salón. Los voluntarios podrán llevar plumas y libretas de apuntes para parecer periodistas.
- El capacitador les pedirá en ese momento a dos voluntarios que representen los sitios web más conocidos (p. ej., Google, Yahoo! o Wikipedia), así como que se pongan de pie juntos al otro lado del salón. Puesto que son famosos, podrán usar anteojos o gafas de sol para lucir con mucho estilo (esto queda a discreción del capacitador).
- A continuación, el capacitador anunciará: “Nuestros periodistas tienen que llevar a cabo una investigación. Los sitios web tienen la información que los periodistas necesitan. Hagamos que se conecten”.
- A los demás participantes se les pedirá que formen una fila entre los periodistas y los sitios web.
- El capacitador le pasará a la persona que esté más cerca de los periodistas una tarjeta con la palabra *Wi-fi* y anunciará que esa persona ahora representa el “punto de acceso”. (Está claro que el capacitador puede usar lo que quiera para identificar a esta persona, como por ejemplo pedirle a la persona que use una antena. Cuanto más entretenida sea la actividad, mejor.)
- Los demás participantes representarán otras partes de Internet, y cada persona llevará en la mano o puesta una tarjeta que la identifique:
 - ISP local;
 - ISP nacional;
 - enrutador;
 - puerta de entrada internacional;
 - enrutador;
 - ISP nacional;
 - ISP local;
 - ...y así sucesivamente. (El capacitador puede decidir cuántas tarjetas distribuir. El objetivo no es que los participantes se aprendan los términos, sino que entiendan que nadie se conecta directamente a un sitio web: la cadena tiene muchos eslabones).

Cómo organizar la actividad

El capacitador explicará que lo que acaban de hacer es crear Internet y se dispondrá a guiar a los participantes en el transcurso de los siguientes pasos:

- Les pedirá a todos los participantes que tomen unas cuantas tarjetas y escriban en cada una de ellas una pregunta que les gustaría hacer a los sitios web, quizás preguntas para un artículo que estén escribiendo. La pregunta debe comenzar con el encabezado “Querido (Google, Yahoo!, Wikipedia, etc.)”, de manera que todos sepan a quién va dirigida cada tarjeta.
- Les pedirá a los participantes que pasen sus tarjetas a la persona que representa el Wi-Fi, el primer eslabón de la cadena de Internet. Llegará un momento en el que la persona que representa el Wi-Fi tenga seis tarjetas en la mano.
- Le preguntará a la persona que representa el Wi-Fi lo siguiente: “Bien, Wi-Fi, ¿cómo saber a dónde enviar cada tarjeta?” (con suerte, el participante pueda ver el encabezado “Querido (nombre del sitio)” al comienzo de cada tarjeta).
- Cuando la persona que representa el Wi-Fi haya respondido la pregunta, el capacitador dirá: “¡Fantástico! ¿Cómo saber de dónde provino cada tarjeta?”. Aquí, el capacitador puede sugerir que Wi-Fi escriba la ubicación de cada persona que le entregó una tarjeta: *derecha, izquierda, centro*.
- El capacitador animará a Wi-Fi a entregar las tarjetas a quien represente un ISP, una por una, y a que diga: “Por favor, señor(a) ISP, entréguele esto a Google” (o Wikipedia, etc.), y así sucesivamente avanzando por la fila.
- En este momento, el capacitador detendrá el tráfico y le preguntará al ISP: “¡Fantástico! ¿Y usted, cómo sabrá de dónde provino cada tarjeta?” El capacitador puede sugerir que el ISP escriba la palabra *Wi-Fi* en cada tarjeta.

NOTA: Para ahorrar tiempo, no todos los participantes tienen que escribir de dónde provienen las tarjetas. El objetivo es ilustrar que una red no funciona a menos que los usuarios (y las máquinas) tengan direcciones.

- Después, se le pedirá al ISP que entregue todas las tarjetas, una por una, a la persona que le sigue, y que dicha persona diga en voz alta: “¡Me salió una tarjeta para (sitio web)!”, y que le entregue a su vez esa tarjeta a la persona que le sigue. (Normalmente, esta parte resulta cómica, pues varias personas exclaman en voz alta al mismo tiempo.)
- Cuando las personas que representan los distintos sitios web reciban sus tarjetas, dichas personas deben enviar una respuesta que ha de comenzar así: “Apreciada (persona a la derecha, izquierda, centro), esta es la respuesta a su pregunta...”, y devolver dichas tarjetas.
- Cuando Wi-Fi acabe de entregarle a cada participante cada tarjeta con su respuesta, deben darse todos un aplauso.

Con los participantes aún de pie, el capacitador puede preguntarles:

- ¿Qué sabían los sitios web acerca de las tarjetas que recibieron? ¿Qué información se expuso?
- ¿Qué sabía el Wi-Fi? ¿Qué sabían los ISP y los otros eslabones de la cadena?
- ¿Habrían podido los sitios web recibir las tarjetas dirigidas a ellos si dichas tarjetas no hubieran tenido el encabezado “Apreciado (sitio web)”?
- ¿Podrían los periodistas haber recibido una respuesta de los sitios web si los sitios web no hubieran sabido dónde estaban ubicados los periodistas?
- ¿Todos los de la cadena podían ver a dónde iban las tarjetas y de dónde provenían?

El capacitador pasará a explicar, antes de la sesión de debate, que este ejercicio es una versión muy simplificada de lo que sucede en Internet y de la clase de información que exponemos cada vez que hacemos clic en un vínculo. En lugar de tarjetas, enviamos “paquetes” que contienen muchos datos/código por medio de los que se nos puede identificar.

RECORDATORIO

Si el presente módulo es el primero de un taller más amplio, sugerimos que los capacitadores dediquen los primeros 10 minutos a trabajar con el grupo para definir los lineamientos de conducta y seguridad. Para más información, véase el apartado “Formalización de un contrato” de la *Guía para capacitadores*.

MATERIALES ADICIONALES:

- Marcadores;
- Plumas;
- Libretas de apuntes;
- Tarjetas;
- Sobres;
- Cinta adhesiva (de cualquier tipo);
- Anteojos o gafas de sol baratas (opcional).

Opciones

- No importa cuántas personas representen a los periodistas y a los sitios web. Sin embargo, debe haber dos o tres en cada grupo para ilustrar que es necesario que puedan ser identificadas.
- Para un grupo de clase grande, se puede poner a más personas a hacer de periodistas y puntos de acceso. Esto recalcará la idea de que los ISP también necesitan poder reconocer los puntos de acceso, de la misma manera que los puntos de acceso necesitan poder reconocer a los periodistas.



2. DEBATE (15 MINUTOS)

Una vez que la actividad haya concluido, los capacitadores pedirán a los participantes que se sienten en círculo o en medio círculo para que puedan dirigirse los unos a los otros. Las preguntas que presentamos a continuación pueden ser útiles para dar inicio al debate.

- ¿La actividad en la que acaba de participar le hizo ver algo que no sabía acerca de Internet?
- En su trabajo, ¿qué tipo de información debe mantenerse en privado cuando usa Internet para visitar sitios web?
- ¿Le importaría que alguien supiera qué términos usa en los motores de búsqueda, qué sitios web visita, o qué publica en un blog o red social?
- ¿Se le ocurren ejemplos aquí, en este país, que pusieran de manifiesto que no se estaba respetando la privacidad en Internet? (Los capacitadores deben incitar la participación activa de los asistentes en un debate acerca de la vigilancia.)
- ¿Ha oído hablar de vigilancia en otros países? ¿Ha estado pendiente de historias de esa índole? ¿Qué ha aprendido de ellas?
- ¿Alguna vez ha cambiado sus prácticas en Internet a raíz de lo que ha oído acerca del control y la vigilancia en la Web?
- ¿Se puede esperar que haya privacidad cuando navegamos en Internet, o deberíamos asumir que ya nada es privado? (Si los participantes creen que se trata más bien de una combinación de ambas cosas, animémoslos a participar en un debate acerca de lo que para ellos debería ser privado y lo que no importa que sea de conocimiento público.)

Los capacitadores tienen plena libertad para añadir elementos a la lista o improvisar según lo estimen oportuno.

Para más ideas y actividades relacionadas, véase el sitio web de [LevelUp](#).



3. INFORMACIÓN/EXPOSICIÓN (30 MINUTOS)

Este apartado incluye un estudio de caso recomendado, ideas clave y algunos materiales para ayudar a transmitir la idea que se está abordando. Los capacitadores tienen plena libertad para añadir más información o improvisar según lo estimen oportuno.

Estudio de caso

Ataques a una herramienta de privacidad

Presentación: La aplicación de software The Onion Router (Tor, por sus siglas en inglés) ha permitido que periodistas y activistas puedan navegar en la Web de forma relativamente anónima. No obstante, según documentos filtrados por el exconsultor de la Agencia Nacional de Seguridad de EE. UU. (National Security Agency; NSA, por sus siglas en inglés) Edward Snowden, dicho organismo y su contraparte en el Reino Unido, el Cuartel General de Comunicaciones del Reino Unido, más conocido como Government Communications Headquarters (GCHQ), han intentado esquivar la protección que ofrece la red Tor.

Historia: El diario *The Guardian* informó en octubre de 2013 que la NSA y el GCHQ habían estado colaborando para desarticular el conocido software de navegación anónima Tor.

Tor es una aplicación gratuita y una red que les permite a los usuarios proteger su identidad y actividad digital. Tor hace rebotar el tráfico de Internet entre una red de computadoras, normalmente ubicadas en varios países, lo que impide que quienes estén vigilando puedan ver los sitios que el usuario está visitando. Tampoco permite que los sitios web puedan ver quién los visita.

NOTA: El objetivo de esta unidad didáctica es que los participantes aprendan a usar Tor.

El diario *The Guardian* citó una presentación filtrada por el exconsultor de la NSA Edward Snowden, según la cual: “Jamás lograremos desanonimizar continuamente a todos los usuarios de Tor. Mediante el análisis manual, podemos desanonimizar una pequeñísima parte de los usuarios de esta red”. En su reportaje para *The Guardian*, se concluía que la NSA no había logrado “desanonimizar a un usuario” para atender una petición concreta. Otra presentación calificó a la red Tor de “soberano del anonimato digital seguro y de baja latencia”.

Pese a que la NSA y el GCHQ no han podido desarticular Tor exitosamente, los documentos citados en el reportaje de *The Guardian* muestran que estos organismos han tenido poco éxito cuando han logrado identificar a algunos usuarios y lanzar ataques por medio de software vulnerable instalado en las computadoras de esos usuarios. Uno de estos ataques se centraba en casos en los que el navegador Firefox se usaba junto con Tor Browser Bundle, puesto que ello significaba que la Agencia tenía el control absoluto de las computadoras de los usuarios, incluidos sus archivos, pulsaciones del teclado, historial de navegación y actividades en la Web.

Periodistas y activistas de todo el mundo (incluidos periodistas en Siria, Irán y China) se valen de Tor para garantizar la privacidad de sus comunicaciones. Los Gobiernos de China e Irán han intentado restringir el uso de Tor en sus respectivos países. El primero ha intentado bloquear su uso, mientras que el segundo ha intentado crear una “Internet nacional” para evitar que se eludan los controles estatales. Sin embargo, las autoridades de Occidente alegan que Tor lo usan quienes están involucrados en acciones terroristas, tráfico de pornografía infantil, tráfico de estupefacientes y trata de personas en línea, y que debe vigilarse su uso.

A pesar de que, según informan fuentes periodísticas, la NSA y el GCHQ aún no han penetrado en la red Tor en sí, lo que sí han hecho es probar modelos, como, por ejemplo, el modelo de vigilancia masiva de Tor. Para tal fin, han interceptado cables clave de Internet, lo que les ha permitido controlar una gran cantidad de nodos de salida de Tor y en cierto modo definir y preparar iniciativas futuras en materia de penetrabilidad de esta red. Asimismo, han interrumpido insistentemente el tráfico en la red Tor para obligar a los usuarios a salirse de dicha red.

La NSA infectó navegadores con código indeseable cuyo único fin era atacar a los usuarios de Tor. Para ello se valieron de un sitio web *trampa* (un *honeypot*) concebido específicamente para atacar a dichos usuarios. Según el reportaje de *The Guardian*, la versión número 17 de Firefox corrige la vulnerabilidad que la NSA estaba explotando.

“Lo bueno es que querían explotar una vulnerabilidad del navegador y no consiguieron mucho, lo que significa que no hay indicios de que puedan penetrar en el protocolo de Tor o analizar el tráfico de la red de Tor”, decía una cita del presidente de Tor, Roger Dingledine, que retomó el diario británico *The Guardian*. “La manera más fácil de obtener información acerca del individuo que está al otro lado de la pantalla sigue siendo infectar su computadora portátil, su celular o su computadora de escritorio”, puntualizó.

Fuentes:

- Artículo de *The Guardian*: “NSA and GCHQ Target Tor Network that Protects Anonymity of Web Users” [La NSA y el GCHQ tienen en la mira a la red de Tor que protege el anonimato de los usuarios de la Web].

Videos de apoyo:

- Entrevista: [Entrevista a Glenn Greenwald en BBC Newsnight](#);
- Explicación: [NSA Targeted Tor Users' Anonymity](#) [La NSA puso en la mira el anonimato de los usuarios de Tor] (Newsy Tech);
- Edward Snowden Interviews with Glenn Greenwald: [June 9, 2013, interview](#) and [July 9, 2013, interview](#) [Entrevistas de Edward Snowden con Glenn Greenwald: 9 de junio y 9 de julio de 2013] (*The Guardian*).

Interacción con los participantes

Para suscitar la participación activa de los asistentes, el capacitador podrá servirse de las siguientes preguntas relacionadas con el estudio de caso:

- ¿Está usted de acuerdo o no con la idea de que un Gobierno tenga derecho a llevar registro de lo que hacen sus ciudadanos en Internet? Explique por qué.
- ¿Deberían los Gobiernos vigilar a sus ciudadanos? ¿Existen circunstancias especiales que justifiquen que el Gobierno vigile a sus ciudadanos?

El capacitador tal vez quiera señalar que la vigilancia puede emplearse para fines nocivos, como vigilar a opositores políticos, activistas en derechos humanos y periodistas. Sin embargo, también puede servir para seguirles el rastro a quienes estén involucrados en trata de personas, pornografía infantil, así como comercialización de estupefacientes y armas.

- Independientemente de si cree que debería haber vigilancia o no, ¿cambiaría sus hábitos de navegación en la Web y utilizaría una herramienta como Tor, si hubiera algo así disponible?
- ¿Debería Snowden haber divulgado la información que divulgó? ¿Por qué? ¿Por qué no?

Ideas de conversación para el capacitador

Después de presentar el estudio de caso, el capacitador remitirá a los participantes a los [Apuntes de clase](#).

1. Puede identificarse lo siguiente:

- Direcciones IP;
- Direcciones MAC;
- Y más...
 - ✓ Al igual que los identificadores de llamadas de los celulares, los sitios web pueden ver quién está “llamando” cuando se establece una conexión. La dirección IP (en inglés, *internet protocol address*) es un ejemplo del tipo de información que pueden ver los sitios web. Esto fue justamente lo que mostramos en la sesión Actividad. Otro ejemplo del tipo de información visible es la dirección MAC, asociada al hardware de su PC. Este es un tema que no abordaremos en esta ocasión, al igual que otros aspectos que abordaremos asimismo más adelante.
 - ✓ **Demostración en vivo:** para ilustrar lo que es una dirección IP, el capacitador visitará los sitios [whatismyipaddress.com](#) o [whatismyip.com](#). Estos sitios web proporcionarán tanto la dirección IP como la ubicación geográfica de la PC del capacitador.
 - ✓ **Video de demostración:** [The Internet Explained](#) [Qué es Internet]. Para esta unidad didáctica, basta con mostrar algunos segundos de este video. Deténgase en 00:47.

2. Los sitios web también tienen identificadores.

- ✓ Cada sitio web tiene al menos una dirección IP para la computadora física en que se aloja. Algunos de los sitios web más conocidos se alojan en más de una computadora (o servidor), de manera que pueden tener varias direcciones IP asociadas a su nombre. De cualquier modo, esta es una manera de vigilar cuáles dispositivos están buscando contacto con cuáles sitios web. También les permite a las autoridades filtrar sitios web: sencillamente tienen que bloquear una dirección IP.

3. Los navegadores dejan “huellas”:

- Versión;
- Plug-ins (complementos);
- Historial;
- Y más...

NOTA PARA LOS CAPACITADORES

Los textos con un ✓ no figuran en los Apuntes de clase de las copias a repartir a los estudiantes.

- ✓ **Demostración en vivo:** [Panoptlick](#). Esta herramienta web de la Electronic Frontier Foundation (EFF.org) presenta información detallada acerca del navegador del usuario, información que los sitios web y las autoridades pueden usar para identificar una computadora o dispositivo móvil específicos.
- ✓ **Alternativa:** [JonDonym IP Check](#). En caso de no estar disponible Panoptlick, este sitio web podría reemplazarlo, ya que es parecido (aunque menos detallado) y realizado por los mismos desarrolladores de JonDo (una aplicación de anonimato).

4. Las aplicaciones y la configuración pueden ser útiles. Comience por el navegador web:

- No almacene contraseñas en el navegador.
- No guarde cookies de historial de navegación.
- Ejecute CCleaner o BleachBit cuando termine la sesión.
- Instale las extensiones [HTTPS Everywhere](#) y [NoScript](#) (Firefox).
 - ✓ [HTTPS Everywhere](#) crea un túnel seguro entre una PC y sitios web conocidos que son compatibles con las conexiones HTTPS. Los capacitadores pueden obtener más información acerca de [HTTPS Everywhere](#) en el sitio web EFF.org y leer acerca de lo que es [HTTPS en este artículo de Wikipedia](#).
 - ✓ [NoScript](#) evita que los sitios web maliciosos ejecuten aplicaciones en su PC sin su conocimiento. [NoScript](#) funciona en cierto modo como un firewall. Inicialmente, evita que se ejecuten en el navegador del usuario los *scripts* (forma abreviada de referirse al conocido lenguaje de código Javascript y cuya denominación en español es *archivos de órdenes*, *archivos de procesamiento por lotes* o *guiones*), y la página mostrará estos elementos bloqueados como si estuvieran dañados. El usuario puede entonces proceder a elegir qué elementos quiere permitir que se ejecuten.

5. VPN = red virtual privada (en inglés, *virtual private network*). Proporciona una conexión segura entre una PC o dispositivo móvil y un servidor (otra computadora) en Internet.

- ✓ Se diferencia levemente de Tor, red que acabamos de abordar. Una VPN exige que se instale un software en la PC o dispositivo móvil del usuario. Dicho software se conecta a otra computadora en Internet, computadora a la que se denomina *servidor de VPN*. Una vez establecida la conexión, lo que el usuario cargue a Internet o descargue se encuentra protegido entre su dispositivo y el servidor de VPN (aunque tal vez no lo esté entre el servidor de VPN y el sitio web que está visitando).
- ✓ **Video de demostración:** [Tutorial de VPN](#) (Google Privacy). Este video también explica la diferencia entre una conexión VPN y una conexión HTTPS (SSL) estándar.
- ✓ **Demostración en vivo:** el capacitador abrirá Psiphon 3 y visitará el sitio [whatismyipaddress.com](#) o [whatismyip.com](#) de nuevo, y mostrará que su dirección IP ha cambiado.

6. Existen los siguientes riesgos asociados a las VPN:

- No es privada a menos que visite un sitio web con HTTPS.
- No es anónima: el servicio de VPN está al tanto de lo que hace el usuario.
 - ✓ Si retomamos el video de privacidad de Google, vemos que una conexión VPN está protegida solamente entre una PC o un celular y un servidor de VPN. La conexión no está protegida entre el servidor de VPN y el sitio web que está visitando el usuario, a menos que dicho sitio web sea compatible con una conexión HTTPS.

7. Tor incorpora algunos pasos más para que la conexión sea más anónima:

- Red voluntaria y global;
- Conexión a través de tres voluntarios (o *proxies*).
 - ✓ La red Tor es más lenta que una VPN, aunque más segura, ya que usa tres proxies en lugar de uno. En cierto modo, es como conectarse a tres VPN una tras otra. El *enrutamiento de cebolla* que propone Tor se denomina así porque proporciona tres capas de cifrado que se pelan como las capas de una cebolla.
 - ✓ Cada VPN está conectada a la siguiente, en cadena, con una conexión protegida que solo comparten entre ellas. No comparten otro tipo información entre ellas, como por ejemplo dónde se origina la conexión o cuál es el sitio web que se está consultando (hasta el último paso de la cadena).
 - ✓ **Demostración en vivo:** el capacitador abrirá dos navegadores, el famoso Firefox y Tor Browser Bundle. El capacitador visitará el siguiente sitio web en los dos navegadores y hará una prueba: [JonDonym IP Check](#). El capacitador comparará después la diferencia entre la información que

los sitios web y las autoridades pueden recoger en cada uno de los dos casos mencionados (y se demostrará que la red Tor divulga muchísima menos información acerca del usuario).

- ✓ **Gráfico interactivo:** [este gráfico de EFF.org](#) ilustra qué información el usuario deja al descubierto cuando usa una conexión HTTPS en vez de usar una conexión Tor.

8. Tor conlleva riesgos:

- Como siempre, el malware puede sortear las precauciones que tomemos y dar a conocer nuestra ubicación.
 - ✓ El ejemplo visto en el estudio de caso muestra que ninguna tecnología de seguridad puede proporcionar una protección perfecta si otras partes de la PC no están seguras.
- Tor solo protege su actividad si usted visita un sitio a través de HTTPS.
 - ✓ Al igual que ocurre con una VPN, su conexión está cifrada únicamente mientras permanece en la propia red Tor. Una vez que su conexión abandona el último “nodo” y se dirige al sitio web, se puede ver el contenido de lo que usted publica o lee a menos que el sitio esté protegido con HTTPS.

9. Dado que las VPN y Tor camuflan la dirección IP del usuario y la del sitio web que visita, algunos periodistas han descubierto que se puede acceder a recursos que antes no estaban disponibles.

4. PROFUNDIZACIÓN (90 MINUTOS)

Este apartado presenta las siguientes aplicaciones:

- CCleaner y BleachBit
- Psiphon 3 y Tor Browser Bundle.

Si los participantes no han instalado el software previamente, el capacitador tal vez quiera tomar una pausa aquí para que quienes no hayan llegado al taller preparados se pongan al día.

PARTE I: Limpiar rastros y configurar el navegador

Ejercicio nro. 1: Cómo borrar su historial de navegación con BleachBit (10 minutos)

El presente ejercicio tiene como objetivo garantizar que los participantes sepan cómo borrar archivos temporales, incluido el historial de navegación. Antes de mostrarles los pasos que deben seguir, el capacitador debe asegurarse de que los participantes han instalado BleachBit o CCleaner en su PC.

- Los participantes abrirán Firefox (o su navegador por defecto) e irán al historial de navegación. En Firefox, vaya a Historial→Mostrar todo el historial.
- Tras confirmar que puede ver la información de navegación reciente, los participantes tendrán que cerrar el navegador y abrir BleachBit (o CCleaner).
- Para no perder información accidentalmente, los participantes tendrán que deseleccionar todo y luego seleccionar las siguientes casillas para Firefox: Historial de las direcciones URL, Caché, Restaurar sesión e Historial de descargas. Después, harán clic en Limpiar para comenzar a borrar la información relacionada con esos elementos.
- Llegados a este punto, los participantes tendrán que abrir Firefox e ir a su historial de navegación. Allí, deben poder constatar que se ha borrado el historial de navegación y el de descargas.

Ejercicio nro. 2 (opcional): Cómo borrar su historial de navegación con CCleaner (10 minutos)

Este ejercicio se parece al anterior. Sin embargo, acá el capacitador tendrá que dedicar más tiempo a señalar las otras funciones que tiene CCleaner, en especial la existencia de Drive Wiper (que se encuentra en la pestaña de Herramientas). Esta función le permite al usuario destruir la información de un disco duro para que nadie la pueda recuperar. ¿En qué se diferencia en este sentido de BleachBit?

¿Qué diferencias existen entre BleachBit y CCleaner? BleachBit es una aplicación de código abierto con la que los usuarios pueden experimentar. CCleaner no es libre. Por otra parte, CCleaner cuenta con más herramientas que pueden serles de gran utilidad a los participantes. En resumen, ambas aplicaciones merecen la pena.

Ejercicio nro. 3: Lograr que la configuración de su navegador proporcione más privacidad (10 minutos)

Con esta demostración, se pretende mostrar a los participantes dónde se encuentra la configuración de privacidad y seguridad en Firefox. Recomendamos hacer una demostración y no un ejercicio como tal, de manera que quede suficiente tiempo para los demás ejercicios, pues son de vital importancia. Los participantes podrán consultar su configuración de privacidad después de clase:

- En Firefox, ir a Herramientas→Opciones, y seleccionar la pestaña Ajustes de privacidad.
- En el menú desplegable de la sección de Historial seleccione Nunca recordar el historial, o, por el contrario, seleccione Usar una configuración personalizada para el historial y elija siempre la casilla Permanecer en modo de navegación privada.
- Los capacitadores también deben señalarles a los participantes la existencia de la casilla Limpiar el historial cuando Firefox se cierre.

SOFTWARE E INSTALACIÓN:

- CCleaner
 - Guía
- BleachBit
 - Guía
- Psiphon 3
 - Guía
- Tor Browser Bundle
- Navegador Firefox.

PARTE II: Cómo crear una conexión segura

Ejercicio nro. 1: Cómo confirmar que la conexión en una VPN es segura

En este ejercicio, los participantes usarán Psiphon 3 para crear una conexión segura:

- En el navegador, el capacitador visitará el sitio web whatismyipaddress.com y le mostrará a la clase la dirección IP que sale.
- Cerrará el navegador.
- Abrirá Psiphon 3 para cerciorarse de que la aplicación está configurada para conectarse por VPN y esperará a que se establezca la conexión y se abra una nueva ventana de navegación.
- Consultará whatismyipaddress.com nuevamente y le mostrará a la clase la nueva dirección IP.
- Los participantes deberían repetir el ejercicio hasta demostrar que entienden los pasos. Mientras los participantes están llevando a cabo el ejercicio, el capacitador podría aprovechar para recordarles lo siguiente:
 - El tráfico entre su PC y el servidor está cifrado. Atención: El tráfico entre el servidor y un sitio web no lo estará si el sitio web no es compatible con una conexión HTTPS.
 - Los sitios web que consulten se cargarán más lentamente cuando la conexión se establezca por VPN, lo cual es normal, ya que no están visitando el sitio web directamente.
 - Si alguno de los participantes no ha establecido una conexión VPN, no podrá usar la VPN.

Ejercicio nro. 2: Cómo cerciorarse con Tor de que la conexión es segura

En este ejercicio, los participantes usarán Tor no solo para crear una conexión segura, sino también para cambiar su nodo de salida.

- En el navegador, el capacitador visitará whatismyipaddress.com o whatismyip.com y le mostrará a la clase la dirección IP.
- Cerrará el navegador (y cualquier otra cosa que esté abierta).
- El capacitador abrirá la carpeta de Tor Browser Bundle y ejecutará Tor (“Iniciar Tor Browser.exe”).
- Aparecerá el panel de control (Vidalia) y mostrará cómo avanza el proceso de establecer la conexión. *Esto puede tardar algunos segundos.*
- La versión portátil de Firefox se abrirá cuando se ponga verde el indicador del estado del programa –un ícono en forma de cebolla–, y mostrará el mensaje que se incluye a continuación:
“Felicitaciones. Su navegador se ha configurado para usar TOR.”
Si la aplicación no logra establecer una conexión segura, aparecerá esta página de inicio con un mensaje de alerta.
- En la ventana del navegador Firefox que acaba de abrirse, el capacitador visitará whatismyipaddress.com o whatismyip.com nuevamente y verá que cambió la dirección IP. Es posible también que la ubicación geográfica aparezca completamente vacía.
- El capacitador explicará que siempre existe la posibilidad de que el nodo de salida –el servidor que el usuario usa para salir a la Internet pública– se encuentre ubicado en el mismo país donde está el usuario (!). De ser así, tal vez los usuarios quieran cambiar su nodo de salida al marcar el botón Usar identidad nueva en el Panel de control de Tor (véase la imagen a la derecha), y esperar unos segundos a que Tor establezca la conexión nuevamente.
- El capacitador cambiará su nodo de salida como se explica arriba y actualizará la página en el navegador (whatismyipaddress.com o whatismyip.com). La dirección IP habrá cambiado.
- Cerrará el navegador. En este momento, se cerrará tanto el navegador como, acto seguido, el panel de control.

Mientras los participantes están llevando a cabo el ejercicio por sí mismos, el capacitador podría aprovechar para recordarles que:

- Alguien que quiera usar Tor tiene que ejecutar Tor Browser Bundle y usar la versión especial de Firefox correspondiente. Si un usuario tiene más de un navegador (p. ej., Chrome o Internet Explorer), incluso si tiene la versión común y corriente de Firefox en su PC, debe tener en cuenta que estos navegadores no usarán la red de Tor automáticamente. Lo anterior se puede confirmar si la dirección IP de la PC se consulta simultáneamente con el navegador de Tor y con otro navegador que no sea Tor.
- Cabe reiterar que el usuario no estará usando la red de Tor a menos que Tor se esté ejecutando mientras este último navega, de manera que es importante prestar atención a qué navegador está usando el usuario.
- Puesto que las tácticas de vigilancia digital cambian continuamente, es muy importante que los participantes usen la versión más reciente de Tor Browser Bundle. Apenas se conecte, el navegador comprobará automáticamente si hay disponible una versión más reciente. La página de inicio señalará si la hay, pero no la descargará a menos que el usuario se lo indique. Es decir, que habrá que descargarla manualmente.
- Si los participantes quieren más información sobre cómo usar Tor o una VPN en un dispositivo Android, pueden consultar los [Apuntes de clase](#).

NOTA: Los capacitadores no deben olvidar mencionar durante los ejercicios con Tor que, puesto que las tácticas de vigilancia digital cambian continuamente, es muy importante que los participantes usen la versión más reciente de Tor Browser Bundle. Apenas se conecten, el navegador comprobará automáticamente si hay disponible una versión más reciente. La página de inicio señalará si la hay, pero no la descargará a menos que el usuario se lo indique. Es decir, habrá que descargarla manualmente.

Para más ideas y actividades relacionadas, véase el sitio web de [LevelUp](#).



5. SÍNTESIS (10 MINUTOS)

Sugerimos que los capacitadores se valgan de esta sesión de recapitulación para hacer preguntas informales al grupo y repasar el material visto en este módulo. Algunas ideas importantes de repaso:

■ **¿Qué protege exactamente una red virtual privada (VPN)?**

Una VPN protege la conexión entre PC y servidor, aunque no la conexión entre servidor y sitios web que visitamos.

■ **¿En qué se diferencian las VPN de Tor?**

- Una VPN no es anónima, pues el personal de la VPN puede ver nuestro tráfico de red. También puede verse lo que cargamos a la Web y lo que descargamos, a menos que también estemos conectados a un sitio web compatible con conexiones HTTPS. Tor es más anónimo, pero nuestro tráfico de red seguirá a la vista para el último proxy de la cadena, a menos que también estemos conectados a un sitio web compatible con conexiones HTTPS.
- Una VPN se canaliza o pasa por un proxy. Tor se canaliza por tres.
- Tor es más lento que una VPN porque consta de tres pasos más.

■ **¿Cuál de los dos, VPN o Tor, cree que utilizará en su trabajo?**

NOTA: Para cerciorarse de que los participantes lo están entendiendo, los capacitadores insistirán en que, puesto que las tácticas de vigilancia digital cambian continuamente, es muy importante que los participantes usen la versión más reciente de Tor Browser Bundle. Apenas se conecten, el navegador comprobará automáticamente si hay disponible una versión más reciente. La página de inicio señalará si la hay, pero no la descargará a menos que el usuario se lo indique. Es decir, habrá que descargarla manualmente.

SaferJourno: recursos de seguridad digital para capacitadores de medios de comunicación es un proyecto de Internews que complementa el trabajo hecho en [SpeakSafe](#) y [LevelUp](#). Creado y compartido bajo [licencia Creative Commons Attribution-NonCommercial 3.0 Unported \(CC BY-NC 3.0\)](#).



MAC OS X: INVESTIGAR DE MANERA SEGURA

El material que mostramos a continuación incluye aplicaciones y ejercicios que podrían serles útiles a los participantes que tengan dispositivos Mac OS X e iOS. Los capacitadores que estén trabajando en parejas podrán repartirse las tareas durante los ejercicios de profundización. De esta manera, un capacitador puede trabajar con los usuarios de Windows o Android y el otro, con los usuarios de OS X o iOS.

Software e instalación

- CCleaner
- Tor Browser Bundle [Paquete de navegador de Tor]
 - [Guía](#)
 - [Video paso a paso](#)
- Navegador web Firefox
 - [Guía](#).

NOTA: Ni BleachBit ni Psiphon 3 están disponibles actualmente para Mac OS X. Los usuarios de Mac OS X que tengan un servicio de VPN tal vez quieran probar [Tunnelblick](#), una aplicación que permite a los usuarios agregar y controlar conexiones OpenVPN.

GLOSARIO

Las definiciones de términos que se muestran a continuación se proporcionan bajo [licencia Creative Commons Attribution-Share Alike 3.0 Unported](#) e incluyen entradas creadas por Tactical Technology Collective, Front Line Defenders e Internews.

El vocabulario relacionado con este módulo es el siguiente:

aplicación portátil. Programa que puede utilizarse en un dispositivo portátil, como una memoria USB o una tarjeta de memoria, y que no requiere que se instale en el sistema operativo de la PC.

CCleaner. Herramienta freeware (es decir, software gratuito) que elimina del disco duro archivos temporales y rastros de información potencialmente delicada que han dejado tanto programas que el usuario acaba de utilizar como el propio sistema operativo de Windows.

certificado de seguridad. Método de cifrado del que se valen los sitios web seguros y otros servicios de Internet para demostrar que son quienes dicen ser. Sin embargo, para que su navegador reconozca un certificado de seguridad, el servicio debe pagar por tener una firma digital de una organización validada. Puesto que esto representa un costo monetario, que algunos proveedores del servicio no quieren o no pueden asumir, de vez en cuando le aparecerá un error de certificado de seguridad aun cuando esté visitando un servicio validado.

cifrado. Forma de usar las matemáticas para *cifrar* la información, o codificarla, de manera que solo pueda *descifrarla* o leerla quien tenga una pieza específica de información, como una contraseña, o una clave o llave de cifrado.

cookie. Archivo pequeño que el navegador guarda en la computadora y del que se vale un sitio web para guardar información sobre un usuario dado o para identificarlo en dicho sitio web.

dirección de protocolo de Internet (dirección IP). Identificador único asignado a una computadora cuando está conectada a Internet.

elusión. Acto de sortear filtros de Internet para acceder a sitios web y otros servicios de Internet que estén bloqueados.

Firefox. Navegador FOSS muy conocido que proporciona una alternativa al navegador Internet Explorer de Microsoft.

HTTPS. En inglés, *hypertext transfer protocol secure* (o HTTP seguro). Protocolo de cifrado de uso generalizado en Internet que protege las conexiones entre los sitios web y los usuarios. También se le denomina *capa de protección segura* (*secure pocket layer*; SSL, por sus siglas en inglés).

nombre de dominio. Dirección, en palabras, de un sitio web o servicio de Internet, por ejemplo, *speaksafe.internews.org*.

pirata informático (hacker). En este contexto, delincuente informático malintencionado que intenta acceder a información delicada o tomar control vía remota de la computadora del usuario.

proveedor de servicios. Compañía privada o pública que presta a sus clientes servicios de telefonía móvil o servicios de Internet.

proveedor de servicios de Internet (internet service provider; ISP, por sus siglas en inglés). Compañía u organización que provee la conexión inicial a Internet. Los Gobiernos de muchos países ejercen control de Internet con métodos tales como el filtrado y la vigilancia a través de los ISP que operan en esos países.

proxy. Servicio intermediario mediante el cual el usuario puede canalizar toda o una parte de su comunicación en Internet. Los proxies pueden utilizarse para eludir la censura en la Web. Un proxy puede ser público o puede que el usuario tenga que iniciar sesión con su nombre de usuario y contraseña para entrar. Únicamente algunos proxies son seguros, lo que significa que usan cifrado para proteger la privacidad de la información que pasa entre la computadora del usuario y los servicios de Internet a los que dicho usuario se conecta por medio del proxy.

punto de acceso. Punto en el que un dispositivo se conecta a Internet, normalmente un punto de acceso inalámbrico (Wi-Fi).

SSL (secure sockets layer; en español, capa de conexión segura). Protocolo de cifrado que proporciona una conexión segura entre la computadora del usuario y algunos de los sitios web y servicios de Internet que el usuario visita. Cuando un usuario se conecta a un sitio web por SSL, la dirección del sitio web comienza por *HTTPS* y no por *HTTP*.

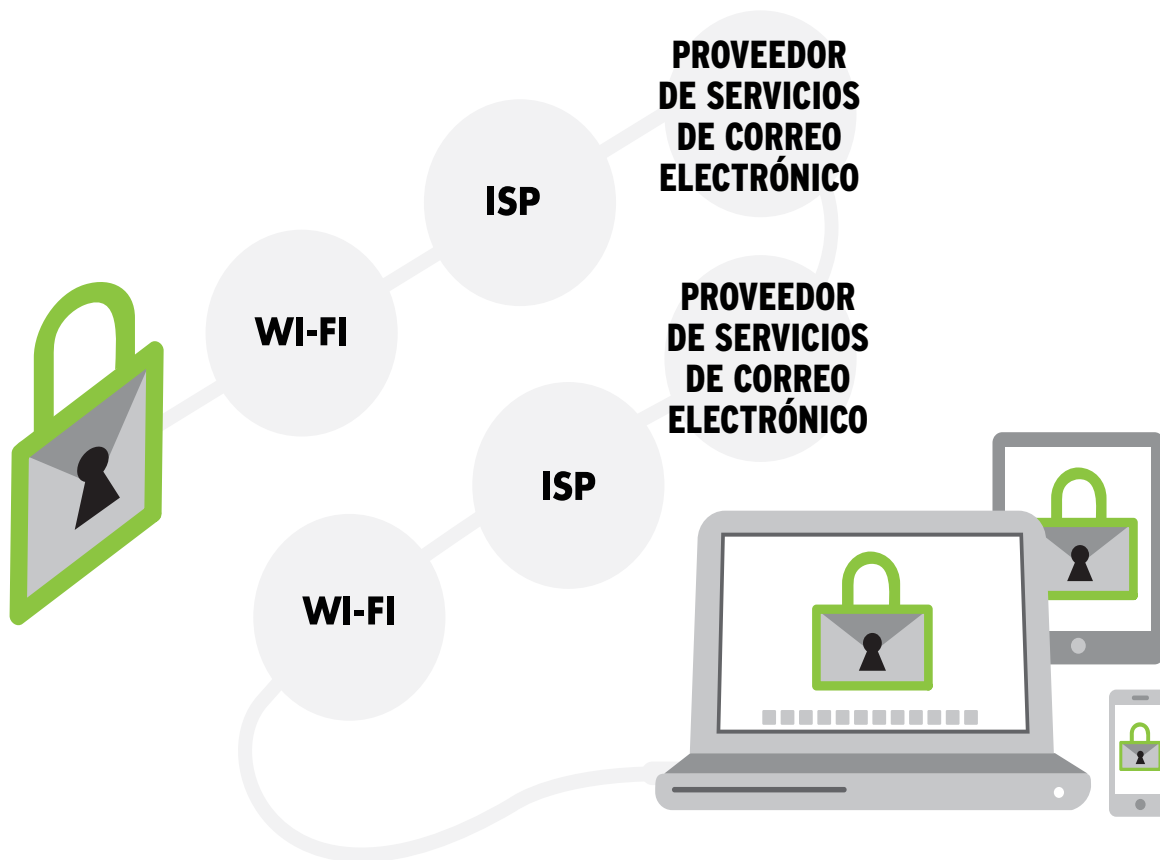
servidor. Computadora que permanece encendida y conectada a Internet para proporcionar algún servicio a otra computadora, como por ejemplo alojar un sitio web o enviar y recibir correos electrónicos.

software gratuito de código abierto (*free and open-source software*; FOSS, por sus siglas en inglés). Familia de software que se consigue sin costo alguno y que no tiene restricciones legales que impidan a los usuarios probar el software, compartirlo o modificarlo.

Tor (The Onion Router; Tor, por sus siglas en inglés). Herramienta anonimizadora que permite sortear la censura en Internet y ocultar los sitios y servicios web que visita el usuario a fin de que quien esté vigilando al usuario no pueda seguir sus movimientos en línea. También camufla la ubicación del usuario.

VPN (virtual private network; en español, red virtual privada). Las VPN utilizan programas de software en una PC o en un dispositivo móvil para establecer una conexión cifrada a un servidor de Internet. Las VPN no garantizan el anonimato del usuario, es decir, la actividad en línea del usuario es visible al proveedor de servicios de la VPN.

5. PROTECCIÓN DE SU CORREO ELECTRÓNICO



IMPORTANCIA DEL TEMA

Los periodistas dependen del correo electrónico para toda una serie de tareas delicadas, aunque tal vez no se den cuenta de que enviar un correo electrónico es como enviar una postal a la antigua: en su trayectoria por el sistema postal, cualquier persona por cuyas manos pase la postal puede leerla.

Las historias de los documentos que filtró Edward Snowden son prueba de la poca privacidad con la que cuentan la mayor parte de los correos electrónicos y otras comunicaciones digitales.

LO QUE APRENDERÁN LOS PARTICIPANTES

Ideas: falta de privacidad con la que cuentan las comunicaciones digitales, verificación en dos pasos, cifrado de extremo a extremo.

Competencias: cómo usar Thunderbird y otras extensiones de seguridad y cómo habilitar la verificación en dos pasos para cuentas de Internet compatibles con dicha función.

OBJETIVOS

Aprender a mejorar la privacidad del correo electrónico

APLICACIONES PRÁCTICAS

Comunicarse de forma segura con fuentes y colegas

CONOCIMIENTOS PREVIOS EXIGIDOS

El presente módulo parte de la base de que los participantes pueden instalar aplicaciones, añadir la contraseña de su cuenta de correo electrónico a aplicaciones, así como ubicar y guardar archivos en la computadora.



NOTA PARA LOS CAPACITADORES: El presente módulo incluye la distribución y demostración de software cuyo uso tal vez no esté permitido por la ley en algunos países. Es recomendable que, antes de dictar este módulo, los capacitadores hagan una investigación básica acerca de la normativa local relativa al acceso a Internet de cada país donde se esté dictando esta capacitación. En algunos países, por ejemplo, la ley prohíbe el uso de programas de cifrado (incluidas las redes virtuales privadas).

ANTES DE COMENZAR

Los recursos que se enumeran a continuación podrían ayudar a los capacitadores a mejorar sus conocimientos acerca del tema del presente módulo antes de comenzar a dictarlo:

- "Mantener privada tu comunicación en Internet" (Security in-a-box);
- "Correo electrónico más seguro" (Capítulo 3 de Speaksafe);
- Video: *Gmail Security Tips* [Consejos en materia de seguridad en Google] (Ayuda de Google);
- "Verifique su configuración de Gmail" (Google support).

ATENCIÓN: Resulta de suma importancia que los capacitadores que hagan los ejercicios de nivel avanzado en la sesión de *Profundización* se cercioren visualmente de que los participantes están usando adecuadamente el software recomendado. Es normal que los participantes asuman que sus correos electrónicos quedan cifrados automáticamente una vez instaladas las aplicaciones. Sin embargo, no siempre es así: ninguno de los correos del usuario queda cifrado automáticamente si el usuario no cambia sus preferencias de seguridad. Lo cierto es que los usuarios deben seleccionar la opción de cifrar sus correos individuales para que, efectivamente, queden cifrados.



MATERIALES

Además de los materiales de capacitación que recomendamos normalmente en la *Guía para capacitadores* (véase el apartado "Consejos para la capacitación"), los capacitadores necesitarán lo siguiente para esta unidad didáctica:

Documentos impresos a repartir

- Apuntes de clase
- Glosario
- Apuntes para usuarios de Mac
- "Mantener privada tu comunicación en Internet" (Security in-a-box).

(Nivel avanzado únicamente)

- Guía: *Thunderbird con Enigmail y GPG* (Security in-a-box).

NOTA: Los capacitadores que necesiten información acerca de los dispositivos Apple, pueden consultar los *Apuntes de la capacitación de "Mac OS X"* que se encuentran justo después de la sesión de Síntesis de este módulo.



MÓDULOS RELACIONADOS

- Seguridad para teléfonos celulares
- Malware y protección básica
- Investigar de manera segura.

PLAN DE CLASE



1. ACTIVIDAD (20 MINUTOS)

(El presente ejercicio se extrajo del proyecto [LevelUp](#), concebido por el [Tactical Technology Collective](#).)

Preparación

Se necesitan algunos materiales para la presente actividad:

- Marcadores;
- Postales en blanco;
- Dos copias de un criptograma pequeño (véase la siguiente imagen).

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	Y
6	Z	.	,	!	?

Puede utilizar esta tabla (arriba) para convertir palabras en números. Cada letra y signo de puntuación corresponde a dos dígitos (uno por fila y otro por columna). Según este sistema, la letra *A* corresponde al número 11, y la letra *B*, al 12. HOLA! sería 23 35 32 11 64.

CARACTERÍSTICAS DEL MÓDULO

El presente módulo está dividido en actividades básicas, actividades avanzadas, apuntes de la exposición y ejercicios. Bajo ningún concepto aconsejamos a los capacitadores que presenten material avanzado (es decir, material clasificado como de “nivel avanzado”) sin antes haber hecho un repaso de las herramientas más básicas de correo web (webmail), las cuales forman parte del “nivel básico”

RECORDATORIO

Si el presente módulo es el primero de un taller más amplio, sugerimos que los capacitadores dediquen los primeros 10 minutos a trabajar con el grupo para definir los lineamientos de conducta y seguridad. Para más información, véase el apartado “Formalización de un contrato” de la *Guía para capacitadores*.

Cómo organizar la actividad

Parte 1: Conexiones desprotegidas

El capacitador dividirá a los participantes en tres grupos y los separará físicamente. Un grupo debe quedar ubicado entre los otros dos.

1. Después, el capacitador explicará lo siguiente: Hemos retrocedido 25 años en el tiempo y el correo electrónico no existe: dependemos únicamente del correo postal. Los participantes tienen que enviar uno o varios mensajes urgentes con estas postales a otro equipo y tienen que lograr que el correo postal (el grupo del medio) se acerque a recoger las postales y las entregue.
2. El capacitador les pedirá a los participantes que pongan direcciones en las postales, y que incluyan el nombre del remitente y un mensaje breve. Después de todo, es lo que habría que hacer en la vida real.
3. El capacitador le explicará al otro grupo (al del medio) que son la Oficina de Correos y que su tarea es transmitir mensajes entre los dos grupos que están recibiendo y enviando mensajes. Les dirá que, sin embargo, no son cualquier correo postal, pues están recogiendo toda la información enviada y deben presentar un informe al grupo después de la actividad.
4. El capacitador dejará que ambos lados hagan una “ronda de intercambios de comunicación”, y después les agradecerá su participación en el ejercicio.
5. El capacitador les preguntará a los participantes si se puede confiar en el correo postal.
6. A continuación, el capacitador invitará a un representante del correo postal a que informe acerca de los mensajes que la Oficina de Correos recibió. Suelen presentarse situaciones cómicas. El capacitador también podrá proponer las siguientes preguntas: ¿Vio quién le envió un mensaje a tal y tal persona? ¿Vio el mensaje? ¿Alguno de los mensajes le pareció cómico?

Debate

Llegado este momento, el capacitador podrá moderar un debate acerca de lo que acaban de ver y aprender. Algunas preguntas que podrían serles útiles son las siguientes:

1. ¿El correo postal de su país funcionó así alguna vez?
2. ¿Confiaría en dicho servicio si funcionara así?
3. Si usted supiera que el sistema funciona así, pero esa fuera la única forma de comunicarse, ¿qué querría cambiar?
4. ¿Cree que Internet funciona así?
5. Si es así, ¿qué podríamos cambiar para que fuera más segura?

Antes del siguiente paso, el capacitador debería aclarar que, aunque sea muy simple, este ejercicio muestra cómo funciona el tráfico web (también llamado *tráfico HTTP*). Cuando emitimos información, como por ejemplo una publicación en un blog, esa información pasa por muchas manos y muchas personas pueden ver lo que estamos haciendo.

Parte 2: Conexiones desprotegidas

1. El capacitador les pedirá a los participantes que regresen a los puestos que les han sido asignados para esta actividad y que repitan el ejercicio. Esta vez, sin embargo, el capacitador le entregará a cada uno de los dos grupos, al de remitentes y al de destinatarios, una copia del cifrado (véase arriba).
2. El capacitador les pedirá a uno o dos participantes de cada grupo que se escriban mensajes entre sí, pero que usen el cifrado para el texto del mensaje. Sin embargo, no podrán usar el cifrado para escribir la dirección, pues la Oficina de Correos no sabría cómo descifrarla.
3. El capacitador les pedirá a los grupos de remitentes y destinatarios que envíen sus mensajes.

Debate

El capacitador les agradecerá a los participantes haberle ayudado a ilustrar otro tipo de tráfico web, el tráfico cifrado, y estimulará el siguiente debate:

1. A quienes estaban enviando los mensajes, ¿se les hizo difícil entender el cifrado?
2. ¿Las personas del medio tenían idea alguna de lo que decía el código? ¿Intentaron descifrarlo?
3. Si vemos el cifrado, ¿parece ser un cifrado complejo?
4. Quienes estaban enviando los mensajes, ¿se divertieron con el ejercicio?
5. ¿Les gustaría hacer lo mismo con sus comunicaciones digitales?



1. ACTIVIDAD (30 MINUTOS). NIVEL AVANZADO

El presente módulo propone otras actividades y vínculos a más información acerca del uso del cifrado de clave pública en el correo electrónico. Se recomienda a los capacitadores no presentar este material a los participantes hasta que no se haya repasado el material que conforma el nivel básico.

Postales y ladrones de dulces

La presente actividad pretende ilustrar la trayectoria que sigue casi todo correo electrónico, así como presentar un método para proteger el contenido del mismo. (Está basada en la actividad “The Postcard Game” [El juego de las postales] que aparece en [LevelUp](#).)

Preparación

El capacitador preparará una tarjeta para sí mismo, pero no se lo dirá a la clase. La tarjeta debe contener una ilustración que muestre que el capacitador es un villano, como, por ejemplo, una carita con mirada malvada o cuernos puntudos.

Antes de dar inicio a la sesión, el capacitador preparará dos sobres con la siguiente información en ambos, como si fueran cartas:

De: mi-usuario@yahoo.com

A: ti-usuario@yahoo.com

Asunto: Urgente e importante

Dirección: Correo electrónico 101 Snowdonia

Cómo empezar

El capacitador guiará a los participantes en los siguientes pasos:

- Les pedirá que se organicen en forma de *U* (lo ideal es un máximo de 10 participantes, o grupos más pequeños de un máximo de 10 personas).
- Pedirá que dos voluntarios, uno en cada extremo de la *U*, se hagan pasar por dos amigos que se escriben por correo electrónico.
- Los demás participantes representarán otros elementos relacionados con Internet, y cada persona llevará pegada o en la mano una tarjeta que la identifique como:
 - Remitente;
 - Punto de acceso Wi-Fi;
 - ISP local;
 - ISP nacional;
 - Proveedor de servicios de correo electrónico: Yahoo!;
 - Proveedor de servicios de correo electrónico: Gmail;
 - ISP nacional;
 - ISP local;
 - Punto de acceso Wi-Fi;
 - Destinatario.
- El capacitador repartirá las tarjetas de tal manera que los proveedores de servicios de correo electrónico (Yahoo! y Gmail) se queden en el “fondo” de la *U*, y uno junto al otro.
- Luego le pedirá a un participante que finja vivir en un país donde Internet está restringida y posiblemente vigilada.

MATERIALES ADICIONALES:

- Marcadores;
- Postales en blanco;
- Sobres (de dos tamaños);
- Tarjetas en blanco o fichas preparadas con los elementos de la Web (véase la lista de la siguiente página: remitente, punto de acceso, etc.)

Cómo organizar la actividad

El capacitador felicitará a los participantes por su acertada representación de Internet y les pedirá que se preparen para lo más difícil: representar la trayectoria típica de un correo electrónico. El capacitador guiará a los participantes en los siguientes pasos:

- Le pedirá al remitente que escriba un mensaje en una tarjeta. Después guardará la tarjeta en uno de los sobres previamente preparados (véase “Preparación” más arriba).
- El remitente le pasará el sobre a quien represente el punto de acceso Wi-Fi, quien lo guardará mientras el capacitador explica lo siguiente:
 - Cuando un remitente está enviando un correo electrónico, el punto de acceso Wi-Fi es el primer lugar a donde llegan los bits del correo.
 - Este punto de acceso es como el enrutador de una oficina. Si hay un administrador de la red de la oficina, esa persona puede ver el tráfico que pasa por la red y muy probablemente vea la información en la parte exterior del sobre (*de, a, dirección*, etc.).
 - Algunas veces oímos hablar de *conexiones seguras* y de algo así como *HTTPS*. Si asumimos que en este caso se trata de ello y que el administrador de la red no puede leer el contenido del correo, ¿entonces qué es lo que ve?
- La persona que representa el punto de acceso Wi-Fi le pasará la tarjeta a la persona que representa al ISP local. Después, el capacitador explicará lo siguiente:
 - Esta es la compañía a la que su organización le paga para tener acceso a Internet. Todo lo que usted haga en Internet se canaliza a través de los servidores de esa compañía.
 - La compañía puede grabar sus actividades y, al igual que su administrador de red, puede ver todo lo que está en la parte exterior del sobre.
 - Si además es su proveedor de servicios de correo electrónico, también puede ver el contenido del mensaje (lo que está dentro del sobre). ■ La persona que representa al ISP local le pasará la tarjeta a la persona que representa al ISP nacional. Después, el capacitador explicará lo siguiente:
 - A menudo, los ISP locales son compañías pequeñas que alquilan equipos y ancho de banda a los ISP nacionales. Estos proveedores nacionales pueden ser compañías privadas, pero también pueden ser públicas.
 - Tal y como sucede con el ISP local, todo lo que usted haga en Internet va a manos del ISP nacional. La compañía puede grabar sus actividades y, al igual que su administrador de red, puede ver todo lo que está en la parte exterior del sobre.
- La persona que representa al ISP nacional le pasará la tarjeta a la persona que representa a Yahoo! Después, el capacitador explicará lo siguiente:
 - Este correo electrónico le llegó a Yahoo! porque el remitente es un cliente de Yahoo! y su correo electrónico es de Yahoo!
 - El personal de Yahoo! puede leer todo lo que contenga la postal, incluido el mensaje.
 - El capacitador le pedirá a la persona que representa a Yahoo! que abra el sobre y saque la carta de dentro.
- La persona de Yahoo! le pasará la carta a la persona de Gmail, sin el sobre. Después, el capacitador explicará lo siguiente:
 - Puesto que nuestro destinatario tiene cuenta de Gmail, Yahoo! tiene que pasarle el mensaje a Google. Las conexiones entre grandes proveedores de servicios de correo electrónico a veces no están protegidas.
- En este momento, el capacitador dará a conocer su propia tarjeta, que muestra el dibujo de una cara amenazante, y se ubicará en medio de las personas que representan a Yahoo! y a Gmail. Después, el capacitador explicará lo siguiente:
 - Esto es lo que a algunos les preocupa que pueda estar pasando en uno de los programas de vigilancia de la NSA.
- La persona que representa a Gmail se quedará con la tarjeta. Después, el capacitador explicará lo siguiente:
 - Tal y como sucede con Yahoo!, el personal de Gmail puede leer todo lo que contenga la postal, incluido el mensaje, y además la postal se quedará allí hasta que alguien la reclame, lo cual podría ser mucho tiempo.
 - El capacitador formulará la siguiente pregunta: ¿Durante cuánto tiempo creen que Yahoo! y Google se quedarán con la postal, incluso después de entregada a su destinatario? Respuesta: Para siempre. Estas compañías guardan copias en varios servidores para que usted no pierda su correo electrónico. Además, la normativa local en algunos países exige que se conserven esas copias durante seis meses o más.

- El capacitador anunciará que el destinatario ha iniciado sesión y pedirá que se le haga llegar la postal pasando por las personas de la cadena que faltan:
 - La persona que representa a Gmail meterá la carta en el segundo sobre.
 - El capacitador felicitará al grupo por haber hecho un buen trabajo.

El capacitador les pedirá a los participantes que permanezcan donde están y explicará que se disponen a examinar un método para proteger los correos electrónicos, incluido su contenido. A continuación, el capacitador procederá como se describe a continuación:

- Con una bolsa de dulces en la mano, anunciará que el remitente quiere enviársela al destinatario, pero que (y esto lo dice con una sonrisa) no confía en que los otros participantes la entreguen.
- Sacará una pequeña caja metálica que puede cerrarse con candado, guardará allí la bolsa de dulces, cerrará la tapa y la cerrará con llave.
- Explicará que no tiene la llave del candado para abrir la caja.
- Enviará la caja por la fila de los representantes de Internet y explicará que este procedimiento es igual al de enviar un correo electrónico sellado con pgp (privacidad bastante buena, del inglés *pretty good privacy*).
- Cuando la caja llegue al final, la última persona sacará una llave y abrirá la caja. Y bueno, ¡ojalá esa persona comparta los dulces con los demás participantes!

NOTA: Para el ejercicio, los capacitadores deben avisar a los participantes que hay pasos adicionales, o nodos, que se han obviado, incluidas las puertas de entrada internacional, para que el ejercicio no resultara demasiado largo.

Véase una demostración
parcial del ejercicio en
YouTube.



2. DEBATE (15 MINUTOS)

Una vez que la actividad haya concluido, los capacitadores pedirán a los participantes que se sienten en círculo o en medio círculo para que puedan dirigirse los unos a los otros. Las preguntas que presentamos a continuación pueden ser útiles para dar inicio al debate. Los capacitadores tienen plena libertad para añadir elementos a la lista o improvisar según lo estimen oportuno.

- ¿Se percataron los miembros del grupo por cuántas etapas tiene que pasar un correo electrónico antes de llegar a su destino?
- ¿Les quedó claro a los participantes que enviar un correo a una persona en realidad implica enviárselo a un servicio de correo electrónico que lo guarda hasta que el destinatario inicie sesión y solicite recibir sus mensajes?
- ¿Quién de la cadena de Internet tenía acceso al nombre y asunto del correo electrónico? ¿Quién podía leer el correo en sí?
- ¿Quién tenía una copia del correo?
- ¿Les quedó claro a los participantes que, aunque tengan una conexión protegida a la que no pueden acceder estos servicios, el contenido en sí del correo no está protegido de los mismos?
- Según los participantes, ¿quién, en este país, podría estar interesado en los correos electrónicos de los periodistas?
- ¿Qué servicio de correo electrónico utilizan? ¿Por qué?
- ¿Hay alguien que en este momento esté tomando medidas para proteger su correo electrónico? ¿Cómo exactamente?

Materiales para suscitar el debate:

Video: *Story of Send* [La historia de *Enviar*] (Google). Este video animado con fines de mercadeo recalca los conceptos presentados en la sesión Actividad y muestra cómo transcurre la trayectoria de un correo electrónico desde una PC a los servidores de Google. Sin embargo, los capacitadores deberían tener en cuenta que se trata de un video de mercadeo, y que, como tal, Google estará promocionando sus servicios.



3. INFORMACIÓN/EXPOSICIÓN (30 MINUTOS)

A continuación, presentamos un estudio de caso recomendado, ideas clave y algunos materiales para ayudar a transmitir la idea que se está abordando.

Estudio de caso

Edward Snowden

Presentación: Resulta poco probable que Glenn Greenwald, periodista del diario *The Guardian*, hubiera podido reunirse con Edward Snowden sin antes aprender a usar software que protegiera algunas de sus conversaciones.

Historia: Cuando el ahora residente en Rusia Edward Snowden —exconsultor de la Agencia Nacional de Seguridad de EE. UU. y responsable de destapar las prácticas de espionaje de dicho organismo— divulgó que la Agencia estaba interceptando llamadas telefónicas privadas y vigilando las conversaciones de mandatarios extranjeros, se cuidó mucho de proteger sus comunicaciones con los periodistas que más adelante escribieron acerca de él y los documentos que había filtrado.

Los artículos publicados en el sitio web Salon cuentan que Snowden se puso en contacto con el reportero de *The Guardian* Glenn Greenwald a comienzos de 2013 por primera vez y que le escribió diciéndole que tenía información que “le interesaría mucho”. Sin embargo, Snowden solo quería comunicarse por medio de comunicaciones que estuvieran cifradas. Recordemos que el cifrado es una forma de camuflar un mensaje para que solo puedan leerlo quienes tengan una contraseña o clave especial. Cuando Greenwald respondió diciendo que no tenía software de cifrado, Snowden le envió un video que explicaba paso a paso las instrucciones para instalar una pgp.

El correo electrónico cifrado es muy eficaz cuando se usa la criptografía de clave pública, puesto que los usuarios finales a quienes está destinado el correo son las únicas personas que deberían poder descifrar esas comunicaciones protegidas. Pero también puede ser un proceso largo y complejo. Por lo que se dice, Greenwald vio el video pero nunca llegó a instalar el programa de cifrado.

Después, Snowden se puso en contacto con Laura Poitras, productora de documentales, y le pidió su clave pública de cifrado. A diferencia de Greenwald, Poitras había escrito acerca de los problemas de vigilancia y había trabajado con fuentes delicadas para la filmación de WikiLeaks, de manera que estaba más familiarizada con esta tecnología y se sentía más cómoda cifrando sus comunicaciones. Envío su clave pública de cifrado, lo que le permitiría a Snowden enviar un correo que solo ella podría abrir con su clave privada.

“Yo ya tenía claves de cifrado”, le dijo al medio digital Salon. “Pero lo que me estaba pidiendo Snowden superaba lo que yo estaba usando en términos de seguridad y anonimato”.

Snowden después le envió a Laura Poitras instrucciones para crear un sistema aún más seguro para proteger sus intercambios y le mandó un mensaje cifrado que señalaba la existencia de una serie de programas secretos de vigilancia que el Gobierno estaba ejecutando y de cuya existencia él podía aportar pruebas. Cuando Snowden sugirió que Poitras y Greenwald colaboraran, ella ayudó a Greenwald a instalar el software de cifrado. De esta manera, Greenwald y Snowden comenzaron a comunicarse a través de un programa cifrado de chat.

Estudio de caso a partir de:

- [“How Laura Poitras Helped Snowden Spill His Secrets”](#) [Cómo le ayudó Laura Poitras a Snowden a revelar sus secretos] (The New York Times);
- [“Cryptic Overtures and a Clandestine Meeting Gave Birth to a Blockbuster Story”](#) [Entre oberturas cifradas y una reunión clandestina nació un taquillazo] (The New York Times);
- [“How Glenn Greenwald Began Communicating With NSA Whistleblower Edward Snowden”](#) [De cómo empezó a comunicarse Glenn Greenwald con el responsable de destapar las prácticas de espionaje de la NSA, Edward Snowden] (HuffingtonPost.com);
- [“How We Broke the NSA Story”](#) [De cómo divulgamos la historia de la NSA, en primicia] (Salon.com).

Videos relacionados:

- [Glenn Greenwald Full Interview on Snowden, NSA, GCH](#) [Entrevista completa a Glenn Greenwald sobre Snowden, NSA, GCH] (BBC Newsnight);
- [PRISM Whistleblower – Edward Snowden in his own words](#) [El denunciante del proyecto PRISM, Edward Snowden, nos cuenta de viva voz] (Freedom of the Press Foundation).

Los capacitadores tienen plena libertad para actualizar, añadir elementos a la lista o improvisar según lo estimen oportuno.

Interacción con los participantes:

El caso ilustra la importancia de proteger el correo electrónico. Preguntas que deben tenerse en cuenta:

- Ahora que sabemos hasta dónde puede llegar la vigilancia de algunos organismos de inteligencia, ¿cómo de probable habría sido que Greenwald y Snowden se hubieran reunido en Hong Kong si no hubieran cifrado sus correos electrónicos?
- ¿Alguna vez le ha preocupado que sus correos electrónicos y sus conversaciones por chat sean objeto de interceptación?
- ¿Qué medidas ha tomado (videos *paso a paso*, guías en Internet)?
- Aunque Glenn Greenwald escribía acerca de temas muy delicados, admitió que el cifrado le parecía muy complicado (incluso hizo caso omiso del video y guía *paso a paso* que le había enviado Snowden). ¿De estar en su lugar, qué habría hecho usted?

Ideas de conversación para el capacitador (NIVEL BÁSICO)

Una vez concluido el estudio de caso, el capacitador remitirá a los participantes a los [Apuntes de clase](#).

1. **En Internet, las comunicaciones personales siempre pasan por un tercero a quien no conocemos.**
 - ✓ Algunos individuos tienen acceso a dichas comunicaciones debido a cómo está diseñado el sistema, como los proveedores de servicios de Internet (o ISP); otros, debido a cuestiones legales, como la NSA u otros organismos de inteligencia; y, otros muchos, debido a fallas en los sistemas empleados, como los piratas informáticos.
2. **Una conexión segura a un servicio de correo electrónico no protege el contenido de los mensajes de la persona o compañía que preste dicho servicio.**
 - ✓ El dueño de Lavabit, el servicio de correo electrónico del que Edward Snowden se valió para comunicarse con Glenn Greenwald, cerró sus puertas cuando la NSA le exigió las claves para acceder a las conexiones seguras establecidas con sus servidores. Si la NSA hubiera podido obtener el certificado, ahora podría estar observando los correos electrónicos del servicio de Lavabit, como si la conexión no fuera segura.
3. **Una forma más segura de proteger sus comunicaciones es a través de una conexión HTTPS (protocolo seguro de transferencia de hipertexto), conocida en ocasiones como SSL (protocolo seguro de encriptación).**
4. **En webmail, el HTTPS puede proteger su conexión cuando usted inicia sesión, y también puede proteger los mensajes que intercambie con su proveedor de servicios de correo electrónico.**
 - ✓ El proveedor de servicio Google es un buen ejemplo. Cuando uno usa Gmail, ve que las letras HTTPS aparecen al comienzo de la dirección (<https://mail.google.com>), ubicada en la parte superior del navegador. Esto significa que la conexión entre su PC y Google está protegida.
5. **No todos los servicios de webmail son compatibles con HTTPS. Lo puede comprobar si, en la dirección, escribe una S al final de las letras H T T P.**
6. **La extensión HTTPS Everywhere también puede redirigirlo automáticamente a la versión HTTPS de algunos de los sitios web más conocidos.**
7. **Deben tenerse en cuenta lo siguientes aspectos:**
 - El HTTPS protege su conexión, no el contenido del correo electrónico.
 - ✓ Esto significa que su proveedor de servicios de correo electrónico podría ver el contenido de sus mensajes.
 - La persona que recibe su correo electrónico también debe estar utilizando HTTPS para que la conexión de esa persona esté protegida.
 - ✓ Esto significa que no solamente su proveedor de servicios de correo electrónico, sino también el proveedor de su destinatario podrían ver el contenido de sus mensajes.

NOTA PARA LOS CAPACITADORES

Los textos con un ✓ no figuran en los Apuntes de clase de las copias a repartir a los estudiantes.

- Si ve un mensaje de alerta de seguridad cuando consulte un sitio HTTPS diciéndole que no reconoce el certificado, no prosiga.
 - ✓ Investigue. Este tipo de advertencia puede significar que alguien ha creado un sitio web que se está haciendo pasar por el que usted estaba buscando.

8. Un método más avanzado para proteger el contenido de sus correos electrónicos es usar una clave pública de cifrado.

- ✓ La privacidad bastante buena es un buen ejemplo, pero no la abordaremos en este módulo de nivel básico.

9. Otras medidas que podemos tomar para proteger nuestras cuentas y que nadie pueda acceder a ellas son las siguientes:

- Asigne contraseñas seguras (véanse los consejos de Security in-a-box).
- Active la verificación en dos pasos (en este video se muestra cómo hacerlo).
 - ✓ La verificación en dos pasos se suele describir como se explica a continuación: Al iniciar sesión, se le pide que proporcione un dato que usted conoce (como una clave, por ejemplo) y algo suyo (como una huella digital). En el siguiente ejercicio, veremos cómo utilizar en nuestro celular no solo una contraseña, sino también un código para aumentar la seguridad de nuestra cuenta de correo electrónico.

10. Varios servicios son compatibles en mayor o menor medida con alguna versión de verificación en dos pasos:

- [Dropbox](#)
- [Facebook](#)
- [Google](#) (todos los servicios)
- [Microsoft](#)
- [Twitter](#)
- [Yahoo!](#)

Ideas de conversación para el capacitador (NIVEL AVANZADO)

Una vez concluido el estudio de caso, el capacitador remitirá a los participantes a los [Apuntes de clase](#).

1. En Internet, las comunicaciones personales siempre pasan por un tercero a quien no conocemos.

- ✓ Algunos individuos tienen acceso a dichas comunicaciones debido a cómo está diseñado el sistema, como los proveedores de servicios de Internet (o ISP); otros, debido a cuestiones legales, como la NSA u otros organismos de inteligencia; y, otros muchos, debido a fallas en los sistemas empleados, como los piratas informáticos.

2. Una conexión segura a un servicio de correo electrónico no protege el contenido de los mensajes de la persona o compañía que preste dicho servicio.

- ✓ El dueño de Lavabit, el servicio de correo electrónico del que Edward Snowden se valió para comunicarse con Glenn Greenwald, cerró sus puertas cuando la NSA le exigió las claves para acceder a las conexiones seguras establecidas con sus servidores. Si la NSA hubiera podido obtener el certificado, ahora podría estar observando los correos electrónicos del servicio de Lavabit, como si la conexión no fuera segura.

3. Una forma más segura de proteger comunicaciones es con cifrado de clave pública.

- ✓ Fue precisamente lo que mostramos en la actividad de las postales y los ladrones de dulces.

4. La privacidad bastante buena es un método que brinda:

- Confidencialidad
 - ✓ Cifrando el contenido de su mensaje para que incluso su proveedor de servicios o cualquiera que logre interceptarlo no pueda leer el contenido, lo que también se conoce como *cifrado de extremo a extremo*.
- Autenticación
 - ✓ Permitiendo que el mensaje solo lo pueda leer quien tenga la clave correspondiente. Sin embargo, no cifra los metadatos del correo electrónico (es decir, la información que contienen los campos *de*, *a*, *asunto*, así como la hora en que el mensaje fue enviado y recibido). Los

NOTA PARA LOS CAPACITADORES

Los textos con un ✓ no figuran en los Apuntes de clase de las copias a repartir a los estudiantes.



metadatos se pueden ver, tal y como se vería lo que está escrito en el sobre de una carta común y corriente.

5. La privacidad bastante buena protege únicamente el contenido de su correo electrónico, pero no cifra ningún otro dato.
6. Se pueden tomar medidas para proteger una cuenta y evitar que terceros puedan acceder a ella:
 - Asigne [contraseñas seguras](#) (véanse los consejos de [Security in-a-box](#)).
 - Active la [verificación en dos pasos](#) (en [este video se muestra cómo hacerlo](#)).
 - ✓ La verificación en dos pasos se suele describir como se explica a continuación: Al iniciar sesión, se le pide que proporcione un dato que usted conoce (como una clave, por ejemplo) y algo suyo (como una huella digital). En el siguiente ejercicio, veremos cómo utilizar en nuestro celular no solo una contraseña, sino también un código para aumentar la seguridad de nuestra cuenta de correo electrónico.
7. Varios servicios son compatibles en mayor o menor medida con alguna versión de verificación en dos pasos:
 - [Dropbox](#)
 - [Facebook](#)
 - [Google](#) (todos los servicios)
 - [Microsoft](#)
 - [Twitter](#)
 - [Yahoo!](#)

4. PROFUNDIZACIÓN (90 MINUTOS)

Este apartado se centra en aplicaciones Windows y contiene ejercicios de nivel básico y de nivel avanzado. Para capacitadores y participantes que necesiten las mismas aplicaciones para Mac OS, consúltese el documento [Apuntes para usuarios de Mac](#).

NIVEL BÁSICO

PARTE I: Verificación en dos pasos (20 minutos)

El capacitador les mostrará a los participantes, en su propio teléfono inteligente, el proceso de configuración de la verificación en dos pasos (cómo habilitar la función en línea y cómo activar la aplicación Google Authenticator). Una vez terminada la demostración, el capacitador puede pedirles a los participantes que habiliten la misma función en sus propios teléfonos. Sin embargo, para ahorrar tiempo, recomendamos que el capacitador asigne esta actividad como tarea. Véanse las instrucciones completas en la [página de Ayuda de Google](#).

Cuestiones que deben tenerse en cuenta sobre la verificación en dos pasos:

- Los usuarios pueden elegir entre dos opciones: recibir los códigos de verificación a través de la aplicación Google Authenticator o por mensaje de texto.
- Los usuarios deberían imprimir los códigos de seguridad de sus cuentas cuando el sistema se lo proponga durante el proceso de configuración. Estos códigos de seguridad brindan acceso de emergencia a una cuenta en caso de pérdida, robo o decomiso del celular. Se recomienda que se guarden los códigos en un lugar seguro.
- Los usuarios pueden crear un código de excepción especial para una aplicación de correo electrónico (como Thunderbird o Outlook), sin el cual dicha aplicación no podría servirse de la verificación en dos pasos.

Materiales útiles:

- Video: [2 Step Verification](#) [Verificación en dos pasos] (Ayuda de Google).

PARTE II: HTTPS Everywhere

En este ejercicio, el capacitador les pedirá a los participantes que instalen el add-on o extensión HTTPS Everywhere en su navegador y les mostrará lo que hace a la hora de visitar una página que tenga una versión HTTP y otra HTTPS.

1. El capacitador empezará abriendo los navegadores Firefox o Chrome.
2. Sirviéndose del proyector, demostrará cómo llegar a la página de descarga de HTTPS Everywhere.
3. El capacitador les pedirá a los participantes que esperen un momento mientras instala HTTPS Everywhere y, si es necesario, reiniciará el navegador.
4. El capacitador abrirá otro navegador (Internet Explorer o Safari, por ejemplo) que no tenga HTTPS Everywhere instalado.
5. A modo de demostración, el capacitador abrirá la página microsoft.com con el segundo navegador y recalcará que la dirección del sitio web empieza por *HTTP* (sin *S*).
6. El capacitador explicará y demostrará que se puede añadir una *S* después de *HTTP* y volver a cargar la página. La página debería estar ahora protegida con HTTPS, y en la barra de direcciones debería aparecer un pequeño icono con un candado.
7. El capacitador volverá al primer navegador y escribirá la misma dirección: microsoft.com. La página que debería aparecer es <https://www.microsoft.com> (con *S*).
8. Acto seguido, el capacitador les pedirá a los participantes que reproduzcan la demostración que acaba de hacer. Los participantes deberán comprobar en pantalla que la operación se ha concluido con éxito.

SOFTWARE E INSTALACIÓN

- Firefox o Chrome
- extensión HTTPS Everywhere (EFF.org)
- Google Authenticator (para Android o iPhone)

NIVEL AVANZADO:

- Thunderbird
- Enigmail (extensión de Thunderbird)
- GnuPG

Cuestiones que se deben tener en cuenta sobre HTTPS Everywhere:

- Contiene una lista (no exhaustiva) de los sitios web más visitados compatibles con conexiones HTTPS.

PARTE III: Otras herramientas de Gmail

En este ejercicio, el capacitador les mostrará a los participantes el vínculo Información detallada de Gmail, que ofrece la posibilidad de consultar dónde y cuándo se ha accedido a una cuenta.

1. El capacitador explicará que, a pesar de que Gmail no es el único servidor de correo electrónico público existente, fue el primero en ofrecer funciones de seguridad que se han adoptado ampliamente, como las conexiones HTTPS y la verificación en dos pasos.
2. El capacitador añadirá que otra función útil de Gmail es la pestaña de Información detallada a la que se accede desde la bandeja de entrada.
3. El capacitador, tras iniciar sesión en la cuenta que utilice para la demostración, irá a la bandeja de entrada y se desplazará hasta la parte inferior de la página. Se detendrá en la parte inferior derecha y mencionará lo siguiente:
 - Hay un mensaje que informa al usuario sobre cuándo fue la última vez que se accedió a la bandeja de entrada.
 - Hay un vínculo llamado *Información detallada*. Al hacer clic en este vínculo, se abrirá otra ventana con la información siguiente:
 - a. Tipo de acceso: ¿se accedió a la cuenta a través de un navegador, mediante una aplicación especial como Outlook, Mail o Thunderbird, o a través de un dispositivo móvil?
 - b. Ubicación (dirección IP): ¿desde dónde se accedió a la cuenta?, ¿con qué dirección digital se accedió a la cuenta? (IP es una sigla en inglés que significa “protocolo de Internet”. Se asigna un protocolo a cada dispositivo que se conecta a Internet durante cada conexión);
 - c. Fecha y hora: ¿cuándo se llevó a cabo la actividad?
4. Después de examinar la ventana de Información detallada, el capacitador les pedirá a los participantes que experimenten con esta herramienta.

Cuestiones que deben tenerse en cuenta sobre el vínculo Información detallada:

- Si el usuario detecta algo fuera de lo normal con el vínculo de Información detallada, como el acceso periódico a su cuenta desde otra ciudad o país, esto puede indicar que alguien se ha apropiado de su contraseña de correo electrónico.
- En ese caso, es importante que el usuario haga clic en Cerrar todas las demás sesiones (al principio de la página de Información detallada) y, acto seguido, cambie la contraseña.
- Si se continúa detectando el mismo problema, cabe comprobar si el usuario ha dado permiso de acceso a su cuenta de correo electrónico a otros servicios. Algunas personas que viajan mucho permiten el acceso a su cuenta a aplicaciones de viajes para recibir alertas.

NIVEL AVANZADO

PARTE I: Verificación en dos pasos (20 minutos)

El capacitador debería hacer referencia al ejercicio equivalente a este del apartado de “Nivel básico” (más arriba). Es recomendable que el capacitador no les pida a los participantes que habiliten esta función en clase. Si la verificación en dos pasos está activada durante este ejercicio, el capacitador deberá enseñarles a los participantes a crear un código de excepción llamado *contraseña de aplicación*.

PARTE II: Thunderbird y GnuPG (60 minutos)

Los participantes tienen que haber descargado e instalado el software recomendado para este módulo antes de la clase o durante un descanso. Si antes de la capacitación no se envió a los participantes la guía práctica *Thunderbird con Enigmail y GPG, cliente de correo seguro*, ahora es el momento de repartirla.

El capacitador les recordará a los participantes que están a punto de aprender el método que Snowden y Greenwald utilizaron para comunicarse, es decir, el mismo tipo de protección que se ilustró con la actividad “Postales y ladrones de dulces” al inicio de este módulo.

Antes de empezar, puede ser una buena idea mostrar el siguiente video como ejemplo:

- Video: *Gambling with Secrets: 8/8 (RSA Encryption)* [Jugando con secretos: 8/8 (Cifrado RSA)]. Solo es necesario mostrarlo hasta el minuto 01:57.

Ejercicio nro. 1: Crear un par de claves o llaves (key pair)

El capacitador demostrará cómo crear un *par de claves o llaves*, es decir, el equivalente de una llave y la caja correspondiente. Los participantes deberán esperar a que el capacitador complete el proceso antes de intentar repetirlo.

1. Abra Thunderbird (GnuPG y Enigmail deben estar instalados en la misma PC).
2. Abra la ventana Gestión de claves (en el menú, seleccione OpenPGP→Gestión de claves).
3. Desde el menú, vaya a Generar y seleccione Nuevo par de claves en la lista desplegable.
4. Seleccione una cuenta de correo electrónico para la cual quiera crear un par de claves.
5. El sistema le pedirá que cree una *frase clave* (una contraseña), que es otra forma más de proteger el uso de una llave y un candado nuevos. El capacitador tiene la posibilidad de activar la opción Sin frase clave. Ahora bien, si la activa, deberá anunciarlo durante la demostración.
6. Haga clic en Generar clave. Este proceso puede tardar varios minutos. Durante la espera, y antes de que los participantes repitan el ejercicio, el capacitador puede mencionar lo siguiente:
 - a. Aunque el par de claves se creara para una cuenta de correo electrónico determinada, se pueden utilizar las mismas claves para más de una cuenta.
 - b. Dado que no se puede abrir una cuenta pgp sin una clave personal, es importante proteger dicha clave con una contraseña de seguridad (idealmente, cifrada). Para más información sobre cifrado, véase el módulo Protección de datos.
7. Haga clic en Generar certificado y guárdelo en el escritorio. Explique que el certificado de revocación es una herramienta de emergencia que permite invalidar la clave pública en caso de pérdida o robo de la clave privada. Igual que la clave privada, la clave de revocación también tiene que estar protegida.

Una vez que el capacitador haya terminado, los participantes deberán repetir estos pasos por su cuenta. Para repasar los pasos de crear un par de claves y mandárselas a alguien, el capacitador puede pedirle a un voluntario que pruebe a repetir dichos pasos delante de la clase y con la ayuda de los demás compañeros.

Finalmente, el capacitador felicitará a los participantes por haber completado con éxito la parte más difícil del ejercicio.

Ejercicio nro. 2: Compartir la clave pública

A continuación, cada participante puede enviar su clave pública (y no la privada) a los demás participantes. La clave privada nunca deberá compartirse ni enviarse por correo electrónico. (Alternativa: si el capacitador ha creado una lista de distribución de correo para la capacitación, los participantes podrán enviar las claves públicas a esa dirección para compartirlas con todo el mundo a la vez.)

Método 1: manualmente

Instrucciones:

1. Abra Thunderbird (GnuPG y Enigmail deben estar instalados en la misma PC).
2. Abra la ventana Gestión de claves (en el menú, seleccione OpenPGP→Gestión de claves).
3. Seleccione la cuenta de correo para la cual creó un nuevo par de claves en el ejercicio anterior.
4. Haga clic con el botón derecho en la cuenta de correo y seleccione Exportar claves a un fichero.
5. Seleccione Exportar solo claves públicas. (Es importante exportar únicamente la clave pública.)
6. Exporte la clave a una memoria USB u otro tipo de unidad externa.

Ideas clave que hay que transmitir

El capacitador puede destacar que el método más seguro para intercambiar claves es en persona, puesto que ambas partes tienen control sobre sus claves y pueden ver con quién las intercambian. Sin embargo, no siempre puede optarse por este método.

Método 2: por correo electrónico

Instrucciones:

1. Abra Thunderbird (GnuPG y Enigmail deben estar instalados en la misma PC).
2. Abra la ventana Gestión de claves (en el menú, seleccione OpenPGP→Gestión de claves).
3. Seleccione la cuenta de correo para la cual creó un nuevo par de claves en el ejercicio anterior.
4. Haga clic con el botón derecho en la cuenta de correo y seleccione Enviar claves públicas por correo.
5. Introduzca una dirección destinataria y haga clic en Enviar (a efectos de este ejercicio, el capacitador puede enviárselo a sí mismo o a la lista de distribución de correo, si hubiera creado una previamente).

Una vez que el capacitador haya terminado, los participantes deberán repetir estos pasos por su cuenta. Mientras los participantes llevan a cabo el ejercicio, el capacitador puede explicar que este es tan solo uno de los métodos posibles para compartir una clave pública. Las claves públicas también pueden guardarse y compartirse sirviéndose de un dispositivo externo. Asimismo, también pueden copiarse y pegarse en el cuerpo de un correo electrónico. Para quienes estén interesados en obtener más información sobre el uso del método pgp en el correo electrónico, véase el documento "[Thunderbird con Enigmail y GPG, cliente de correo seguro](#)".

Ejercicio nro. 3: Importar una clave pública

Este último ejercicio consiste en que los participantes añadan las claves públicas de sus compañeros a la biblioteca de claves. Es recomendable que el capacitador demuestre el primer paso y advierta a los participantes que no compartan las claves privadas por error.

Método 1: manualmente

Instrucciones:

1. Abra Thunderbird (GnuPG y Enigmail deben estar instalados en la misma PC).
2. Reciba la clave pública de un participante en una memoria USB.
3. Abra la ventana Gestión de claves (en el menú, seleccione OpenPGP→Gestión de claves).
4. Vaya a Archivo y seleccione Importar claves desde un fichero.
5. Una ventana emergente le pedirá que seleccione las claves públicas que desee importar.

Método 2: por correo electrónico

Instrucciones:

1. Abra Thunderbird (GnuPG y Enigmail deben estar instalados en la misma PC).
2. Abra el correo que un participante le haya enviado con su clave pública. Guarde la clave en un lugar de fácil ubicación, como el escritorio.
3. Abra la ventana Gestión de claves (en el menú, seleccione OpenPGP→Gestión de claves).
4. Vaya a Archivo y seleccione Importar claves desde un fichero.
5. Una ventana emergente le pedirá que seleccione la(s) clave(s) pública(s) que se ha(n) descargado.

A continuación, los participantes deberán repetir los pasos de intercambiar e importar hasta que hayan recibido las claves públicas de todos sus compañeros.

Ejercicio nro. 4: Validar y firmar

Este ejercicio pone de manifiesto la importancia de confirmar la autenticidad de las claves públicas.

Recomendamos que los capacitadores consulten el [apartado 4.4](#) de la guía [Cómo utilizar Enigmail con GnuPG en Thunderbird](#) y sigan los pasos descritos a modo de demostración. Después los participantes pueden reproducir los mismos pasos.

Ejercicio nro. 5: ¡Manos a la obra!

Si los ejercicios anteriores se han completado satisfactoriamente y el capacitador ha confirmado que todo el mundo ha seguido todos los pasos, los participantes pueden mandar mensajes de prueba al capacitador o a algún compañero de clase.

Como siempre, primero el capacitador demostrará los pasos:

1. Crear un mensaje;
2. Seleccionar un destinatario cuya clave ya se haya importado;
3. Activar el botón OpenPGP del mensaje;
4. Seleccionar Firmar mensaje;
5. Seleccionar Cifrar mensaje;
6. Enviar el mensaje.

Al cabo de cinco minutos, el capacitador puede preguntarles a los participantes si han logrado repetir estos pasos. Es probable que algunos participantes hayan enviado o recibido mensajes sin cifrar.

En ese caso, el capacitador debería repasar las siguientes ideas clave. Si hay tiempo, el capacitador puede demostrar los pasos de establecer una regla para un destinatario determinado.

Ideas clave que hay que transmitir:

- Estas aplicaciones (Thunderbird, Enigmail y GnuPG) no cifran mensajes por defecto: es necesario activar la función de cifrado manualmente.
- Para que todos los correos que se envíen desde una cuenta se cifren automáticamente, vaya a Configuración de la cuenta en Thunderbird, seleccione Seguridad OpenPGP, y active la casilla Cifrar mensajes por defecto. Aun así, los mensajes que se envíen a destinatarios de quienes no se tenga la clave pública no se cifrarán. En esos casos, Enigmail le pedirá al usuario que introduzca la clave.
- También se pueden cifrar por defecto todos los mensajes que se envíen a un destinatario mediante la definición de una regla para un destinatario determinado. Para empezar, abra un correo de una persona para la cual desee definir una regla, haga clic con el botón derecho en la dirección del remitente y seleccione Crear regla OpenPGP a partir de la dirección...

NOTA: Remitimos a los capacitadores a que consulten la siguiente [guía paso a paso preparada por los desarrolladores de Enigmail](#).

CONSIDERACIONES (REPETICIÓN):

Es fundamental que los capacitadores que se encarguen de este módulo se cercioren visualmente de que los participantes estén usando adecuadamente el software recomendado. A menudo, los participantes asumen que sus correos se cifrarán automáticamente una vez que han instalado las aplicaciones. Sin embargo, dichas aplicaciones no funcionan así. Por defecto, ninguno de los correos del usuario se cifra automáticamente, a no ser que el usuario cambie las preferencias de seguridad. Por lo tanto, los usuarios deberán seleccionar manualmente la opción de cifrado en cada correo.

SaferJourno: recursos de seguridad digital para capacitadores de medios de comunicación es un proyecto de Internews que complementa el trabajo hecho en [SpeakSafe](#) y [LevelUp](#). Creado y compartido bajo [licencia Creative Commons Attribution-NonCommercial 3.0 Unported \(CC BY-NC 3.0\)](#).



5. SÍNTESIS (10 MINUTOS)

Sugerimos que los capacitadores se sirvan de esta sesión de recapitulación para hacer preguntas informales al grupo y repasar el material visto en este módulo. Las siguientes preguntas podrían ayudar a los participantes a poner en práctica lo aprendido:

- ¿Para qué sirve la verificación en dos pasos?
- Otros servicios de Internet muy conocidos, incluidos Facebook, Twitter, Microsoft (SkyDrive, por ejemplo) y Dropbox, también ofrecen la función de verificación en dos pasos.
- Gmail tiene otras funciones de seguridad que pueden consultarse en la página de Ayuda de Google (los vínculos incluidos en el apartado “Antes de comenzar” del presente módulo pueden ser útiles).
- También hemos hablado sobre cómo proteger el contenido de los correos electrónicos que se envían con la función pgp.
- Pgp no cifra el asunto del mensaje ni tampoco oculta quién envió y recibió el correo.
- Se puede añadir una protección similar a las conversaciones de chat. Los participantes pueden leer el capítulo “Pidgin + OTR” del sitio web Security in-a-box.
- ¿Existen otras formas de proteger cuentas y correos electrónicos que no hayamos tenido en cuenta?
- Conclusión final: existen distintos niveles de protección para correos electrónicos y otras formas de comunicación. Esta sesión ha abordado uno de los métodos más seguros porque protege el contenido del mensaje. Si quieren aprender otras formas de proteger comunicaciones por correo electrónico, consulten los recursos complementarios que encontrarán más adelante.



MAC OS X: PROTECCIÓN DE SU CORREO ELECTRÓNICO (NIVEL AVANZADO)

Este apartado incluye aplicaciones y ejercicios útiles para aquellos participantes que utilicen Mac OS X y dispositivos iOS. Los capacitadores que trabajen en parejas pueden repartirse tareas durante la sesión de Profundización: uno puede trabajar con los usuarios de Windows y Android, y el otro con los de OS X e iOS.

Software e instalación

(Sesiones de nivel avanzado)

- Thunderbird
- Enigmail (complemento de Thunderbird)
- GPG Suite (GPGTools)
 - Guía: [First Steps](#) [Primeros pasos].

Profundización

Ejercicios nro. 1 y 2: Para acceder a las instrucciones, consúltese la guía oficial del programa [First Steps](#)

Ideas clave que hay que transmitir

- Al subir una clave pública para que otros puedan acceder a ella, GPGTools subirá automáticamente la nueva clave al servidor de claves y la definirá como clave predeterminada en el panel de Preferencias de GPG Keychain. Es probable que esta clave no coincida con la clave predeterminada del servidor de Enigmail. Por consiguiente, algunos usuarios podrían tener dificultades a la hora de ubicar y descargar claves públicas de otros usuarios si han utilizado Enigmail o GPGTools para crear y subir su primera clave pública. Recomendamos que el usuario acceda manualmente al panel de Preferencias de GPG Keychain Access, explore cada uno de los servidores de claves de la lista, haga clic con el botón derecho (CTRL + clic) en su clave y seleccione la opción Enviar a un servidor de claves. De este modo, podrá accederse a la clave pública del mismo usuario desde más de un servidor de claves.
- También recomendamos que se añadan los servidores de claves disponibles en Enigmail que no estén definidos como servidores de claves predeterminados en el panel de Preferencias de GPG Keychain, en la pestaña Servidor de claves. Escriba el nombre del servidor de claves en el campo de texto y presione la tecla Enter. A continuación, defina el objeto deseado como servidor de claves y haga clic en Enviar a un servidor de claves.

Ejercicio nro. 3: Importar una clave pública

Instrucciones sobre GPG Keychain Access de GPGTools:

1. Si quiere buscar la clave asociada a una dirección de correo conocida, vaya a Clave→Buscar clave→y escriba la dirección.
 - a. Seleccione la clave deseada y haga clic en Obtener clave.
 - b. Igual que cuando descarga claves públicas, es probable que tenga que buscar en varios servidores de claves, ya que GPGTools no hace búsquedas automáticamente en todos los servidores. Vaya al panel de Preferencias→Servidor de claves y repita el mismo paso con distintos servidores. Si sabe o cree que una clave determinada está almacenada en un servidor de claves concreto, añada dicho servidor a la lista de Preferencias. Dos de los servidores más utilizados entre los usuarios de GPG son pgp.mit.edu y <http://pool.sks-keyservers.net>.

Ejercicio nro. 4: Validar y firmar

- **Validación:** En la medida de lo posible, siempre se debería verificar que una clave (recuerde que también se denomina *llave*) pertenece a la persona que uno cree comprobando la huella digital de dicha clave (fingerprint). (El usuario tendría que hacer lo mismo con su propia clave.) En Keychain, se puede localizar la huella digital asociada a una clave haciendo doble clic en la clave y seleccionando Clave.
- **Firma:** Para enviar a otro usuario mensajes cifrados o firmados, es necesario *firmar* la clave de dicho usuario. Le recomendamos que firme las claves en un dispositivo electrónico que le pertenezca. Haga clic con el botón derecho (CTRL + clic) en una entrada y seleccione Firmar... La clave con la que firmará será la suya (por defecto). A continuación, podrá especificar el nivel de confianza de la clave, que dependerá de cómo haya verificado que la clave pertenece al usuario que cree. Finalmente, puede definir la fecha de vencimiento de la firma y seleccionar Firma local.

Ideas clave que hay que transmitir

- Las firmas públicas permiten a terceras partes determinar quién se relaciona con quién teniendo en cuenta qué claves ha firmado ese usuario. Le recomendamos que seleccione la Firma local para firmar claves siempre que el propietario de la clave no le indique lo contrario.
- Si quiere buscar la clave de un contacto con el identificador de clave, que está formado por los ocho últimos dígitos de la huella digital de la clave precedidos de 0x (ej.: 0xAC5409EC), vaya a Clave→Obtener clave desde el servidor e introduzca el identificador. Seleccione la clave deseada y haga clic en Obtener clave.

GLOSARIO

Las definiciones de términos que se muestran a continuación se proporcionan bajo [licencia Creative Commons Attribution-Share Alike 3.0 Unported](#) e incluyen entradas creadas por Tactical Technology Collective, Front Line Defenders e Internews.

El vocabulario relacionado con este módulo es el siguiente:

aplicación portátil. Programa que puede utilizarse en un dispositivo portátil, como una memoria USB o una tarjeta de memoria, y que no requiere que se instale en el sistema operativo de la PC.

cifrado. Forma de usar las matemáticas para *cifrar* la información, o codificarla, de manera que solo pueda *descifrarla* y leerla quien tenga una pieza específica de información, como una contraseña o una clave de cifrado.

cliente de correo electrónico. Aplicación instalada en una PC o dispositivo móvil que organiza el correo y permite a los usuarios leer y escribir mensajes sin conexión a Internet. Algunos ejemplos de aplicaciones conocidas son Outlook de Microsoft y Thunderbird de Mozilla.

dirección de protocolo de Internet (dirección IP). Identificador único asignado a una computadora cuando está conectada a Internet.

Enigmail. Complemento o extensión de la aplicación de correo electrónico Thunderbird que permite mandar y recibir mensajes cifrados y con firma digital.

Firefox. Navegador web FOSS muy conocido que proporciona una alternativa a Microsoft Internet Explorer.

fuera de registro (*Off the Record*; OTR, por sus siglas en inglés). Complemento de cifrado del programa de mensajería instantánea Pidgin.

HTTPS. En inglés, *hypertext transfer protocol secure* (o HTTP seguro). Protocolo de cifrado de uso generalizado en Internet que protege la conexión entre un sitio web y el usuario. También se denomina *capa de conexión segura* (*secure sockets layer*; SSL, por sus siglas en inglés).

multi-factor authentication. Método de protección de una cuenta web que requiere que el usuario introduzca un mínimo de dos categorías de información al iniciar sesión, en vez de simplemente una contraseña. Los sistemas de verificación en dos pasos que emplean Google, Facebook, Twitter y Dropbox son ejemplos de lo que suele entenderse por *multi-factor authentication*.

nombre de dominio. Dirección, en palabras, de un sitio web o servicio de Internet (por ejemplo, [speaksafe.internews.org](#)).

pgp (*pretty good privacy*; pgg, por sus siglas en inglés). Privacidad bastante buena. Método de uso muy extendido para cifrar el contenido de correos electrónicos y ficheros adjuntos. Requiere que emisor y destinatario compartan sus claves públicas, que se utilizarán para cifrar los correos. Solo pueden descifrarse correos con la clave privada del destinatario (que nunca debe compartirse).

Pidgin. Herramienta de mensajería instantánea FOSS compatible con el complemento de cifrado *fuera de registro* (u *off the record*).

pirata informático (*hacker*). En este contexto, delincuente informático malintencionado que intenta acceder a información delicada o tomar control vía remota de la computadora del usuario.

proveedor de servicios. Compañía privada o pública que presta a sus clientes servicios de telefonía móvil o servicios de Internet.

proveedor de servicios de Internet (*Internet service provider*; ISP, por sus siglas en inglés). Compañía u organización que provee la conexión inicial a Internet. Los Gobiernos de muchos países ejercen control de Internet con métodos tales como el filtrado y la vigilancia a través de los ISP que operan en esos países.

punto de acceso. Punto en el que un dispositivo se conecta a Internet, normalmente un punto de acceso inalámbrico (Wi-Fi).

servidor. Computadora que permanece encendida y conectada a Internet para proporcionar algún servicio a otra computadora, como, por ejemplo, alojar un sitio web o enviar y recibir correos electrónicos.

software gratuito de código abierto (*free and open-source software*; **FOSS, por sus siglas en inglés**). Familia de software que se consigue sin costo alguno y que no tiene restricciones legales que impidan a los usuarios probar el software, compartirlo o modificarlo.

SSL (*secure sockets layer*; **en español, capa de conexión segura**). Protocolo de cifrado de uso generalizado en Internet que protege las conexiones entre los sitios web y los usuarios. También se denomina *protocolo seguro de transferencia de hipertexto* (*hypertext transfer protocol secure*; HTTPS, por sus siglas en inglés).

Thunderbird. Programa FOSS de gestión de correo electrónico con varias funciones de seguridad integradas y compatible con el complemento de cifrado Enigmail.

verificación en dos pasos. Método de protección de una cuenta web o de un archivo que requiere que el usuario introduzca un mínimo de dos categorías de información al iniciar sesión en vez de simplemente una contraseña.

6. SEGURIDAD PARA TELÉFONOS CELULARES



IMPORTANCIA DEL TEMA

En muchas ocasiones, el celular o el teléfono inteligente es la herramienta de trabajo más valiosa del periodista. Contiene listas de contactos, fotografías, correos electrónicos, mensajes de chat, etc. Pero los celulares también son una excelente herramienta para controlar y seguirle la pista a alguien. Si bien es poco realista pensar que algún día prescindiremos de ellos, como periodistas tenemos que saber cómo funcionan y poder tomar decisiones informadas a la hora de utilizarlos.

LO QUE APRENDERÁN LOS PARTICIPANTES

Ideas: inseguridad de las redes de telefonía móvil. Adoptar ciertos hábitos puede mitigar riesgos.

Competencias: instalación de los programas Orbot, Orweb y ChatSecure, que permiten definir contraseñas sólidas y habilitar funciones de cifrado en celulares Android.



NOTA PARA LOS CAPACITADORES: El presente módulo incluye la distribución y demostración de software cuyo uso tal vez no esté permitido por la ley en algunos países. Es recomendable que, antes de dictar este módulo, los capacitadores hagan una investigación básica acerca de la normativa local relativa al acceso a Internet de cada país donde se esté dictando esta capacitación. En algunos lugares, por ejemplo, la ley prohíbe el uso de redes virtuales privadas (VPN, por sus siglas en inglés).

OBJETIVOS

Aprender sobre los riesgos y las precauciones en materia de seguridad con respecto al uso del celular

APLICACIONES PRÁCTICAS

Evitar ser vigilado, proteger datos guardados en el celular y evitar exponer la información de llamadas y mensajes de texto

CONOCIMIENTOS PREVIOS EXIGIDOS

El presente módulo parte de la base de que los participantes saben instalar aplicaciones en el celular.

ANTES DE COMENZAR

Los recursos que se enumeran a continuación podrían ayudar a los capacitadores a mejorar sus conocimientos acerca del tema del presente módulo antes de comenzar a dictarlo:

- *Surveillance Self-Defense: Mobile Devices* [Vigilancia y autodefensa: dispositivos móviles] (eff.org);
- *Utilizar los teléfonos móviles de la manera más segura posible* (Security in-a-box).



MATERIALES

Además de los materiales de capacitación que recomendamos normalmente en la *Guía para capacitadores* (véase el apartado “[Consejos para la capacitación](#)”), los capacitadores necesitarán lo siguiente:

Documentos impresos a repartir

- Apuntes de clase
- Glosario
- Guía: *Utilizar los teléfonos móviles de la manera más segura posible* (Security in-a-box)
- Guía: *Utilizar los teléfonos inteligentes de la manera más segura posible* (Security in-a-box).

NOTA: Los capacitadores que necesiten información acerca de los dispositivos Apple pueden consultar los [Apuntes de la capacitación de “Mac OS X”](#), que se encuentran justo después de la sesión de Síntesis de este módulo.



MÓDULOS RELACIONADOS

- Evaluación de riesgos
- Protección de su correo electrónico
- Protección de datos.

MÁS INFORMACIÓN

Requisitos adicionales

A la fecha de redactar esta guía, el sistema operativo Android (para celulares y tabletas) es compatible con la mayoría de las aplicaciones de código abierto relacionadas con la privacidad que se abordan en este módulo. Si bien existen varias herramientas de privacidad compatibles con el sistema operativo iOS (para iPhone e iPad), en el momento de redactar esta guía, la única aplicación de código abierto que recomendamos es ChatSecure para iOS. Cada vez surgen más aplicaciones prometedoras compatibles con iOS que merece la pena explorar (como [Wickr](#) y [Lookout](#)), pero no son de código abierto. Dado que se han detectado múltiples vulnerabilidades en las aplicaciones para iOS de código cerrado ([Snapchat](#) es el ejemplo más sonado a la fecha de redacción de esta guía), desaconsejamos su empleo. Para más información sobre software de código abierto, véase la [Guía para capacitadores](#).

PLAN DE CLASE



1. ACTIVIDAD (30 MINUTOS)

VIDEO (10 minutos)

Aconsejamos a los capacitadores que empiecen este módulo mostrando el siguiente video de una charla reciente de TED Talk:

- **Video:** TED Talks: Malte Spitz. *Your Phone Company is Watching* [Su compañía de telefonía lo está observando] (10 minutos);
- **Video alternativo:** [versión resumida de la charla de Malte Spitz](#) (8,5 minutos).

NOTA: En cualquier video de YouTube, los capacitadores pueden habilitar la función de subtítulos si el sonido no es óptimo.

Sobre el video

TED es una asociación dedicada a la tecnología, el entretenimiento y el diseño que organiza charlas bianuales sobre tendencias científicas y tecnológicas.

El político alemán del partido de Los Verdes, **Malte Spitz**, cuenta lo que aprendió sobre privacidad móvil (o más bien sobre la falta de privacidad) al denunciar a la compañía de telefonía Deutsche Telecom (DT) cuando quiso tener acceso a todos los datos que la compañía había almacenado a partir de su celular. Cuando Spitz recibió los datos (en un formato sin procesar), colaboró con periodistas de *Zeit Online* para crear **un mapa interactivo que demuestra claramente que la compañía había seguido todos los pasos de Spitz**, minuto a minuto. (La visualización del mapa requiere conexión a Internet.)

Las líneas grises situadas justo debajo del mapa corresponden a los días; el cuadradito rojo que aparece encima del día seleccionado indica la hora y puede desplazarse hacia arriba y hacia abajo.

¿Qué se almacena en su celular? (20 minutos)

Al ver el video, los participantes se habrán dado cuenta de la información tan detallada a la que los proveedores de servicios móviles tienen acceso (y que almacenan) sobre sus clientes. Ahora es importante que los participantes también puedan reflexionar sobre lo que se almacena en sus celulares. Esta actividad puede llevarse a cabo con la ayuda de un único voluntario o con la participación de todo el grupo.

Cómo organizar la actividad

Ejercicio con un único participante

El capacitador seleccionará a un voluntario de la clase y, antes de empezar el ejercicio, le explicará que le va a pedir que comparta información sobre los datos que guarda en el celular. A continuación, el capacitador seguirá los siguientes pasos:

- Le pedirá al participante que escriba todos los datos que guarda en el celular en el rotafolio. Lista de algunos ejemplos:
 - Contactos;
 - Fotografías;
 - Mensajes de texto;
 - Notas;
 - Correos electrónicos;
 - Contraseñas guardadas (de cuentas de redes sociales como Twitter y Facebook).

RECORDATORIO

Si el presente módulo es el primero de un taller más amplio, sugerimos que los capacitadores dediquen los primeros 10 minutos a trabajar con el grupo para definir los lineamientos de conducta y seguridad. Para más información, véase el apartado "Formalización de un contrato" de la Guía para capacitadores.

- Le pedirá al voluntario que valore cómo de delicado es cada dato en una escala del 1 al 5 (donde 1 equivale a información no delicada y 5, a información que podría utilizarse en contra de uno mismo o de algún contacto). (El capacitador puede pedirle al voluntario que dé distintas puntuaciones en función de la naturaleza de cada *adversario*: ¿Qué pasaría si la policía tuviera acceso a su celular? ¿O alguien de la competencia? ¿O alguien con quien tiene relaciones personales?)

Ejercicio con todo el grupo

El capacitador también puede optar por una versión de grupo de este mismo ejercicio, en la que participará toda la clase. Para ello, el capacitador hará lo siguiente:

- Explicará al grupo que van a crear un mapa con la información de sus celulares y les pedirá a los participantes que piensen en las categorías de información que tienen guardadas en el celular. Lista de algunos ejemplos:
 - Información telefónica (por ejemplo, registro de llamadas, mensajes de texto y contactos);
 - Aplicaciones de correo electrónico;
 - Aplicaciones de redes sociales;
 - Aplicaciones de video, audio y fotografías;
 - Aplicaciones de navegadores (Google, Firefox, Safari).
- Escribirá las categorías en la parte superior del rotafolio o pegará notas autoadhesivas en la pared.
- Dividirá la superficie (la hoja del rotafolio o la pared) en dos secciones: pública y privada. La sección pública representará información que a uno no le importa compartir públicamente, mientras que la privada contendrá información que uno solo está dispuesto a compartir con un número reducido de personas o consigo mismo.
- Repartirá notas autoadhesivas a los participantes y les pedirá que escriban qué tipo de información de cada categoría guardan en el celular. Les pedirá que clasifiquen la información en función de si es pública o privada, y pegará las notas autoadhesivas en el rotafolio o la pared.
- Después de crear el mapa, les pedirá a los participantes que reflexionen sobre el tipo de información que guardan en el celular.
- Ante el mapa, el capacitador les pedirá a los participantes que piensen también en la información que ni siquiera han tenido en cuenta, pero que el celular genera automáticamente: datos sobre la ubicación, registros de llamadas, estadísticas de uso del celular, etc. El capacitador puede añadir los elementos que falten al mapa, tal vez en otro color para distinguirlos.

Ejercicio extraído de “What Is on Your Phone?” [¿Qué tiene en el celular?] (disponible en el sitio web de [LevelUp](#)).



2. DEBATE (15 MINUTOS)

Después de completar las dos partes de la sesión Actividad, los capacitadores pueden pedirles a los participantes que se sienten en círculo o semicírculo para que puedan dirigirse los unos a los otros. Las preguntas que presentamos a continuación pueden ser útiles para dar inicio al debate.

- ¿Les sorprendió el video de TED Talk? ¿Aprendieron algo nuevo?
- Spitz cuenta que DT, su compañía de telefonía, almacena todos los datos durante un mínimo de dos años. ¿Saben cuál es la política de almacenamiento de datos de su proveedor de servicios? ¿Podrían averiguarlo?
- ¿Les sorprendió darse cuenta de todo lo que uno guarda en el celular?
- Últimamente han surgido muchas noticias relacionadas con los documentos de la Agencia Nacional de Seguridad de los Estados Unidos (National Security Agency; NSA, por sus siglas en inglés) filtrados por Edward Snowden. ¿Creen que la NSA es el único organismo que lleva a cabo programas de vigilancia? ¿O tal vez todos los servicios de inteligencia lo hagan? ¿O tan solo algunos?
- ¿Han cambiado su forma de utilizar el celular desde que salieron a la luz los documentos de Edward Snowden? ¿Han hecho algún cambio en la configuración del celular?
- ¿Cómo protegen su celular ahora (y los datos que contiene)?
- ¿Tienen alguna pregunta sobre celulares y privacidad que querrían abordar en esta clase?

Los capacitadores tienen plena libertad para añadir elementos a la lista o improvisar según lo estimen oportuno.



3. INFORMACIÓN/EXPOSICIÓN (30 MINUTOS)

El presente apartado incluye un estudio de caso recomendado, ideas clave y algunos materiales para ayudar a transmitir las ideas que se están abordando.

Estudio de casos

Escuchas telefónicas en las noticias

Presentación: Mucha gente se ha alarmado cuando se ha sabido que los servicios de inteligencia controlan la información que contienen los celulares, pero lo que realmente ha enturbiado el asunto han sido las prácticas de algunas organizaciones de noticias.

Historia: En septiembre de 2010, Sean Hoare, exreportero de entretenimiento de *News of the World*, comunicó a *The New York Times Magazine* que lo habían “animado insistentemente” para que espíara las cuentas de buzón de voz de famosos a quienes daba cobertura periodística.

El caso, que se convirtió en un sonado escándalo en el que estuvieron presentes famosos, agentes de policía y dinero, y que terminó con el cierre de un periódico, se destapó cuando Hoare contó a la revista *The New York Times* que un redactor jefe podía acceder a información sobre el movimiento y la ubicación de una persona a partir de su número de teléfono y que a los reporteros del tabloide se les pedía constantemente que llevaran a cabo este tipo de prácticas.

Otra noticia sobre el mismo caso, publicada por el periódico británico *The Guardian*, citó las siguientes palabras de Hoare: “Cada 15 o 30 minutos venía alguien de redacción y decía: ‘Muy bien, aquí están’”.

Cinco años antes, el tabloide había sido acusado de escuchar mensajes de voz de distintos personajes famosos, entre los cuales se encontraban los miembros de la familia real británica. La pista que destapó el escándalo fue que los mensajes de voz que los destinatarios todavía no habían escuchado aparecían en sus buzones como escuchados y guardados. Gracias a este método, información a la cual tan solo unos pocos tenían acceso aparecía publicada en el tabloide.

La Policía Metropolitana del Reino Unido (la famosa *Scotland Yard*) se vio envuelta en el asunto y denunció a Clive Goodman, periodista encargado de dar cobertura a la familia real, y a Glenn Mulcaire, un investigador privado contratado por el periódico.

Aunque al registrar el domicilio del investigador privado la policía encontró documentos que contenían miles de números de celulares, códigos PIN y una grabación de Mulcaire en la que este explicaba a un periodista los pasos a seguir para piratear el buzón de voz de una figura del mundo del fútbol, la policía se centró en el caso de la monarquía, que culminó con el encarcelamiento de Mulcaire y Goodman.

Aun así, la policía británica no logró tirar de las pistas que indicaban que los episodios de espionaje no únicamente afectaban a la familia real, sino también a otros ciudadanos. Hubo protestas públicas contra el periódico y su propietario, Rupert Murdoch, cuando en julio de 2011 se supo que el tabloide también había interceptado los celulares de una niña asesinada, de familiares de soldados británicos fallecidos y de víctimas del atentado de Londres del 7 de julio.

Al parecer, la policía y los organismos públicos encargados de velar por el cumplimiento de la ley también se sirven de este método de seguimiento: piden periódicamente a las compañías de telefonía móvil que les proporcionen información a tiempo real sobre el paradero de sospechosos y desaparecidos. La policía también puede solicitar un volcado o transferencia de datos, lo que le permite hacerse con un registro histórico completo de la ubicación del celular de una persona. Hay dos formas mediante las cuales se pueden obtener datos sobre la ubicación de una persona a partir del celular:

- Cuando el usuario utiliza el celular para hacer una llamada o mandar un mensaje de texto;
- Cuando el usuario no está utilizando el celular, se puede localizar el dispositivo enviándole señales y triangulando los resultados de las torres de señales de celulares. La precisión con la que se ubicará el dispositivo dependerá de la proximidad de las torres y puede variar entre los cien metros y los dos kilómetros.

Los capacitadores tienen plena libertad para añadir elementos a la lista o improvisar según lo estimen oportuno.

Fuentes

- “Tabloid Hack Attack on Royals, and Beyond” [Espionaje del tabloide a la realeza y más allá] (The New York Times Magazine);
- “News of the World Phone-hacking Whistleblower Found Dead” [Hallan muerto al responsable de destapar las prácticas de espionaje de News of the World] (The Guardian).

Video de apoyo sobre el estudio de caso: *Sean Hoare – NoW Whistle-Blower Found Dead – Speaking About Hacking in March 2011* [Hallan muerto al responsable de destapar las prácticas de espionaje de NoW. Sean Hoare habla sobre el pirateo de celulares, marzo de 2011] (NOTWPhoneHacking).

Interacción con los participantes

Este estudio de caso pone de manifiesto que los celulares no son por naturaleza seguros. Recomendamos que los capacitadores den pie a un debate entre los participantes a partir del estudio de caso. Algunas preguntas que podrían ser de ayuda son las siguientes:

- ¿Aprueban la práctica periodística de espiar conversaciones privadas de ciudadanos?
- ¿Difiere esta práctica de la vigilancia de celulares que llevan a cabo los organismos públicos encargados de velar por el cumplimiento de la ley? ¿En qué sentido?
- ¿Se les ocurre algún caso hipotético en el que un periodista podría justificar estas prácticas de espionaje? ¿Y los servicios de inteligencia? ¿Y una compañía de telefonía?
- ¿Cómo utilizan el celular? ¿Creen que alguien podría tener algún interés en escuchar sus conversaciones telefónicas? ¿Cabe la posibilidad de que alguien haya escuchado sus conversaciones telefónicas?

Ideas de conversación para el capacitador

Una vez haya concluido el estudio de caso, el capacitador remite a los participantes a los [Apuntes de clase](#).

1. Es muy fácil robar o confiscar un celular.

- ✓ Artículo: “[Mobile Phone Crime Soars](#)” [Se disparan los delitos relacionados con teléfonos celulares] (The Daily Mail).

2. Los celulares son como radios.

- ✓ Esto significa que envían información sobre su ubicación geográfica a las torres de telefonía y, por lo tanto, permiten identificar y localizar la ubicación de sus propietarios. A principios de 2014, las autoridades ucranianas se sirvieron de esta particularidad para mandar mensajes de alerta a los manifestantes de un mitin político que tomó un cariz violento.
- ✓ Artículo: “[Ukraine’s Opposition Says Government Stirs Violence](#)” [La oposición ucraniana afirma que el Gobierno incita la violencia] (The New York Times).
- ✓ Esto también significa que el aire que respiramos está colmado de miles de llamadas telefónicas y que aquellos equipados con dispositivos especiales podrían escucharlas.
- ✓ Artículo: “[Smart Trash Can Knows How Fast You Walk and Which Smartphone You Use](#)” [Basurero inteligente sabe a qué velocidad caminamos y qué teléfono inteligente llevamos] (TheVerge.com).

3. Cada vez hay más personas interesadas en vigilarnos.

- ✓ Los programas de software de vigilancia ya están al alcance del público general:
 - ✓ **Video:** [Phone Tracker](#) [Seguidor de celulares] (YouTube). En este video de phone-track.net se afirma que este sitio web ofrece un servicio de búsquedas que permite vincular números de teléfono con datos sobre ubicaciones geográficas. No aconsejamos el uso de este servicio. Con este video solo queremos destacar que la industria de servicios y software que permiten seguirle la pista a alguien está creciendo a pasos agigantados.
 - ✓ **Sitio web:** “[Ultimate Cell Phone Monitoring Software](#)” [El software definitivo para vigilar celulares] (Mobistealth.com).

NOTA PARA LOS CAPACITADORES

Los textos con un ✓ no figuran en los Apuntes de clase de las copias a repartir a los estudiantes.

4. Los proveedores de servicios de telefonía móvil pueden almacenar los siguientes metadatos del usuario:

- Ubicación;
- Llamadas (duración y a qué número);
- Mensajes de texto;
- Acceso a servicios web.
 - ✓ Artículo: “[Spy Scandal Grows: Telekom Accused of Tracking Journalists’ Mobile Phone Signals](#)” [El escándalo de espionaje sigue: Telekom acusada de dar seguimiento a las señales de los celulares de periodistas] (Spiegel Online);
 - ✓ Artículo: “[Chinese Sell Iran £100m Surveillance System Capable of Spying on Dissidents’ Phone Calls and Internet](#)” [China vende a Irán un sistema de vigilancia para espiar llamadas y la actividad en línea de disidentes por 100 millones de libras] (The Daily Mail);
 - ✓ Artículo: “[EU Company Admits Blame for Sale of Phone-snooping Gadgets to Iran](#)” [Compañía europea admite haber vendido tecnología de vigilancia a Irán] (EUobserver).

5. Los dispositivos tienen un identificador único llamado IMEI (del inglés, international mobile equipment identity).

- ✓ Este código nunca cambia, ni siquiera si el usuario cambia la tarjeta SIM (la parte del celular donde se guarda el número de teléfono).

6. Existen distintas formas de garantizar la seguridad física:

- Preste atención a su entorno.
 - ✓ ¿Tiene a alguien cerca?
- No deje el celular a la vista.
 - ✓ No lo deje encima de la mesa de un restaurante. Esta práctica incita el robo.
- Decida qué necesita guardar en el celular.
 - ✓ En caso de robo o decomiso, cuanta menos información guarde, mejor. Es aconsejable que los participantes adquieran el hábito de revisar el contenido de su celular al menos una vez a la semana.

7. Existen distintas formas de garantizar la seguridad digital:

- Asigne contraseñas difíciles de adivinar.
 - ✓ Muchas personas utilizan códigos PIN (normalmente un número de cuatro dígitos que el usuario debe introducir para hacer una llamada). Sin embargo, Android, iPhone y Blackberry funcionan con contraseñas más difíciles de adivinar y, por lo tanto, son dispositivos más seguros. Este tipo de contraseñas puede habilitarse en la configuración del celular.
- Habilite la función de cifrado.
 - ✓ Los números PIN y las contraseñas no permiten que otra persona pueda hacer llamadas desde su celular, pero seguramente no protegen los datos guardados, especialmente si utiliza una tarjeta SD o cualquier otra tarjeta de memoria de este tipo.

8. Evite lo siguiente:

- Descargar aplicaciones, wallpapers o ringtones innecesarios.
 - ✓ Estos elementos pueden ser divertidos, pero también contienen virus.
- Descargar aplicaciones que solicitan acceso a información que no necesitan.
 - ✓ Por ejemplo, una aplicación despertador que solicita acceso al registro de llamadas.
- Tener las redes de Wi-Fi y Bluetooth activadas cuando no se están utilizando.
 - ✓ No solo gastan batería, sino que hacen que el celular sea vulnerable a posibles ataques.

4. PROFUNDIZACIÓN (80 MINUTOS)

Esta sesión dotará a los participantes de conocimientos básicos sobre la configuración del celular y varias aplicaciones móviles. El material que presentamos a continuación es para Android. Los capacitadores que deseen obtener información aplicable a dispositivos iOS (iPhone o iPad) pueden consultar el documento sobre dispositivos iOS.

Dado que esta sesión aborda muchas aplicaciones, es probable que los capacitadores no tengan tiempo de terminarla en 90 minutos. Por lo tanto, recomendamos que se dé prioridad a las aplicaciones de comunicación TextSecure y ChatSecure.

NOTA: Para estos ejercicios, antes de empezar la clase, los participantes deberían haber abierto una cuenta en cualquiera de las siguientes aplicaciones: Facebook chat, Gchat (Google), VKontakte, Yandex, Hyves, Odnoklassniki, StudiVZ, LiveJournal, Jabber o *Bonjour (ZeroConf)*, de Apple.

PARTE I: Configuración del sistema

La primera parte de la sesión de profundización es bastante corta. El capacitador les mostrará a los participantes los pasos que tiene que seguir para activar el mecanismo de bloqueo y la función de cifrado en el celular y, si procede, en una tarjeta SD adicional.

Información preliminar: El capacitador puede leer este breve artículo de ghacks.net antes de dictar la clase para familiarizarse con las distintas funciones: “[Encrypt All Data on Your Android Phone](#)” [Cifrado de todos los datos en Android].

NOTA: Recomendamos al capacitador que haga una demostración de cada ejercicio dos veces antes de pedirles a los participantes que lo reproduzcan ellos. También recomendamos que el capacitador se asegure de que todos los participantes han completado una tarea antes de pasar a la siguiente.

Ejercicio nro. 1: Pantalla de bloqueo y contraseñas largas en Android

1. Vaya a Ajustes→Seguridad→Pantalla de bloqueo.
2. Seleccione Contraseña.
3. Asigne una contraseña.

Materiales útiles:

- **Guía:** [Crear y mantener contraseñas seguras](#) (Security in-a-box);
- **Video:** [Enabling or Changing Screenlock](#) [Activar o cambiar la pantalla de bloqueo].
Nota: Aunque este video hace referencia al Samsung 4G, los pasos descritos también son aplicables a dispositivos Android. Sin embargo, es probable que haya diferencias mínimas en otros dispositivos.

Ejercicio nro. 2: Activar la función de cifrado en el celular

1. Vaya a Ajustes→Seguridad→Cifrado.
2. Seleccione Cifrar dispositivo.



ATENCIÓN: El procedimiento de habilitar la función de cifrado puede ser largo y, en algunos casos, se requiere que el dispositivo esté enchufado a la corriente para llevar a cabo dicho paso.

Por lo tanto, aconsejamos que simplemente se enseñe a los participantes cómo habilitar la función, en vez de tratar de completar este paso. Si la capacitación es de varios días, el capacitador puede asignar el ejercicio de cifrado como tarea. Asimismo, es importante que los participantes entiendan que, aunque los dispositivos Android están diseñados para hacer copias de seguridad de casi todos los datos del usuario, si se sincronizan con una cuenta de Google, no todos los datos guardados en el dispositivo (especialmente fotografías, borradores de correos electrónicos y datos de otras aplicaciones) disponen de copias de seguridad. **Es aconsejable que, antes de activar la función de cifrado en el dispositivo, los usuarios hagan copias de seguridad de todo aquello que consideren de valor y que no quede automáticamente guardado en la cuenta de Google.** Para la mayoría de los usuarios se tratará únicamente de fotografías, aunque puede que algunos deseen guardar otros datos.

SOFTWARE E INSTALACIÓN*

- TextSecure
 - Guía
- ChatSecure
 - Guía**
- Orbot
 - Guía
- Orweb
 - Guía.

* Los participantes pueden descargar todo esto en Google Play y guardarlo directamente en el celular. Los capacitadores pueden recomendar a los participantes que preinstalen estas aplicaciones antes de la clase para aprovechar más el tiempo.

** ChatSecure es el nombre nuevo de Gibberbot. Esta guía de Security in-a-box todavía hace referencia al antiguo nombre de la aplicación. Sin embargo, los principios que describe son también válidos para ChatSecure.

Ejercicio nro. 3: Cifrar una tarjeta SD

1. Vaya a Ajustes→Seguridad→Cifrar tarjeta SD.
2. Seleccione Habilitar.

NOTA: Las mismas consideraciones del ejercicio nro. 2 (arriba indicadas) son válidas para el presente ejercicio.

Materiales útiles:

- **Video:** [How to Encrypt Files on your SD Card using your Android Phone](#) [Cómo cifrar archivos en la tarjeta SD de un celular Android] (YouTube: Howik.com).

PARTE II: Aplicaciones

Información general: Las siguientes aplicaciones están diseñadas para garantizar la seguridad del usuario a la hora de enviar mensajes de texto y chatear (con una sola persona) y mejorar la confidencialidad del usuario a la hora de utilizar un navegador web.

A. TextSecure

TextSecure es una aplicación de código abierto y gratuita que cifra el contenido de mensajes de texto intercambiados entre dos celulares que tienen dicha aplicación instalada. También almacena los mensajes en una base de datos protegida con una contraseña.

Ejercicio nro. 1: Instalación y demostración de TextSecure

- Guía paso a paso: [TextSecure para dispositivos Android](#) (Security in-a-box).

Establecimiento de comunicaciones seguras y prueba

- Este ejercicio sigue los pasos descritos en una [guía paso a paso de Security in-a-box](#). Los participantes tendrán que verificar la identidad del dispositivo de su pareja de trabajo antes de enviarse entre sí mensajes de prueba.
- El capacitador deberá pedirles a los participantes que trabajen en parejas.
- Según las instrucciones de la guía de Security in-a-box, los participantes deben agregar el número de teléfono de su pareja de trabajo a su lista de contactos e iniciar sesión segura.
- Una vez que hayan intercambiado claves, los participantes podrán probar el sistema enviándose mensajes de texto. Este [apartado de la guía paso a paso](#) de Security in-a-box también puede ser útil. Es importante que los participantes comprueben que les ha aparecido **el ícono del candado** junto al botón de Enviar. En caso contrario, el mensaje de texto no estará protegido.
- Los participantes pueden cerrar la sesión segura.

Ideas clave que hay que transmitir

Mientras los participantes llevan a cabo el ejercicio, el capacitador debería recalcar lo siguiente:

- Si el ícono del candado no aparece junto al botón de Enviar, el mensaje de texto no estará protegido.
- TextSecure cifra el contenido de los mensajes de texto, pero no cifra ninguna otra información relacionada con los mensajes, como el remitente y el destinatario, o el día y hora de envío.
- TextSecure tiene la función de cifrar únicamente mensajes de texto. Es decir, no protege ningún otro tipo de comunicaciones que el usuario lleve a cabo desde el celular.

B. ChatSecure

Hasta hace muy poco ChatSecure se llamaba Gibberbot, y algunos materiales que citamos todavía lo llaman así. ChatSecure es una aplicación de chat que permite verificar la identidad de la persona con quien se chatea y cifrar los mensajes intercambiados entre dos celulares. Es compatible con aplicaciones muy conocidas como GTalk o Facebook Chat. Cuando el chat está cifrado significa que la compañía de telefonía móvil no lo puede leer.

Ejercicio nro. 2: Instalación y demostración de ChatSecure

- Guía paso a paso: [How to Chat Securely](#) [Cómo chatear de forma segura] (The Guardian Project).
NOTA: A fecha de hoy (octubre de 2013), este vínculo describe los pasos a seguir para Gibberbot, el predecesor de ChatSecure. Las instrucciones descritas son también válidas para ChatSecure. Sin embargo, es probable que al principio las capturas de pantalla que contiene el vínculo confundan un poco a algunos participantes. Es aconsejable informar a los participantes que algunas capturas de pantalla ya no están vigentes.

Intercambio de claves de verificación

- Antes de empezar el ejercicio, los participantes deberían crear una cuenta de chat en la aplicación ChatSecure.
- Los participantes trabajarán en parejas.
- Siguiendo las instrucciones de The Guardian Project, los participantes deberían intercambiar 1) el nombre de usuario y 2) la información de verificación necesaria para iniciar una sesión de chat segura.
NOTA: La guía paso a paso de The Guardian Project recomienda que se intercambie esta información a través de un canal en línea validado. Dado que los participantes se encontrarán en el mismo salón de clase, el capacitador puede mencionar que el método más seguro de compartir información es siempre en persona. Sin embargo, otros canales (que no sean la aplicación ChatSecure) servirán de alternativa cuando no sea posible quedar en persona.
- Los participantes deberían empezar la sesión de chat con su pareja de trabajo utilizando el modo inseguro (que es el predeterminado). Es importante que se fijen en el ícono que aparece en la parte superior de la pantalla, que indica que la sesión de chat no es segura.
- A continuación, los participantes deberían intentar activar el modo seguro. La aplicación les pedirá que verifiquen la identidad de su interlocutor. Para hacerlo, deben ir siguiendo los pasos que aparezcan en la pantalla.
- Una vez que se haya establecido una sesión de chat segura, los participantes pueden cambiar de pareja y repetir el mismo procedimiento. Objetivo: recopilar la información de verificación de todos los participantes para poder establecer comunicaciones seguras por chat.

Ideas clave que hay que transmitir

Mientras los participantes llevan a cabo los ejercicios de verificar la identidad de los demás e iniciar sesiones de chat, el capacitador les puede recordar lo siguiente:

- ChatSecure tiene la función de proteger sesiones de chat entre dos personas que utilicen la aplicación ChatSecure. No protege ningún otro tipo de información ni ninguna otra aplicación del celular. Por ejemplo, no protege los mensajes de texto, completamente visibles a los proveedores de servicios móviles.
- ChatSecure también funciona en una red anonimadora Tor. En el siguiente ejercicio se aprenderá a utilizar Orbot, una aplicación que permite conectarse a este tipo de redes. Los capacitadores que no estén familiarizados con las redes Tor pueden consultar [este sitio web de su creador](#).

C. Orbot

Orbot es la versión de Tor (del inglés *The Onion Router*) para Android y permite al usuario conectarse a la red anonimizadora Tor. Al utilizar esta red, el usuario no se conecta directamente a un sitio web, sino que se conecta de forma segura a tres computadoras “dispuestas” en cadena. Cada una de estas computadoras solo conoce la identidad de la computadora que le “precede” y de la que le “sigue”. Las conexiones entre las tres computadoras de esta red están cifradas y, por lo tanto, la red Tor ofrece al usuario un alto nivel de anonimato.

1. Los sitios web que uno visita a través de Tor no pueden conocer la ubicación real del usuario, puesto que solo ven la ubicación de la última computadora de la red a la que accedió el usuario.
2. Las computadoras de la red Tor no saben qué sitios web visita un usuario en concreto, sino que simplemente detectan que alguien está visitando un sitio web determinado.

Ejercicio nro. 3: Instalación y demostración de Orbot y Orweb

Esta guía describe paso a paso cómo instalar e iniciar la aplicación Orbot (que permite conectarse al anonimizador Tor) y el navegador Orweb (que utiliza la red Tor).

Guía paso a paso: [Using Orbot & Orweb to browse freely](#) [Navegar libremente con Orbot y Orweb] (The Guardian Project).

NOTA: Algunas de las diapositivas de esta guía contienen animaciones programadas. Es por eso por lo que, en algunas páginas, el botón para pasar a la siguiente diapositiva no aparece hasta al cabo de unos segundos.

Comprobación de que se está utilizando una conexión segura

En este ejercicio los participantes tendrán que comprobar que la conexión de datos de su celular se ejecuta a través de Orbot (la red Tor).

- Abra la aplicación Orbot y espere hasta que se detecte una conexión.
- Abra el navegador Orweb y espere hasta que le aparezca un mensaje de la red Tor que confirme (o desmienta) que la conexión se ha establecido.
- Abra el navegador Orweb y vaya a la siguiente dirección URL: whatismyipaddress.com.
- Los participantes deberían anotar la dirección que les aparece en la pantalla.
- Los participantes deben repetir estos mismos pasos, pero utilizando su navegador favorito, en vez de Orweb.
- Los participantes deberían anotar la dirección IP que les aparezca en el sitio web whatismyipaddress.com. Dado que no estarán utilizando la red Tor, les tendría que aparecer la dirección de su ubicación real.
- Los participantes pueden repetir los mismos pasos hasta que los hayan asimilado. Es aconsejable que pongan los íconos de acceso a estas aplicaciones en algún lugar al que puedan acceder de forma segura.

Ideas clave que hay que transmitir

Mientras los participantes comprueban que están utilizando una red segura, el capacitador les puede recordar lo siguiente:

- Orbot (y la red Tor) protegen únicamente la navegación web: no protegen automáticamente ninguna otra acción que realice el usuario.

Para más ideas y actividades relacionadas, véase el sitio web de [LevelUp](#).



5. SÍNTESIS (15 MINUTOS)

En otros módulos, se ha recomendado que se dedique esta sesión a repasar el material abordado y recapitular. En este caso, sin embargo, proponemos que se lleve a cabo un ejercicio de cinco minutos que también tiene la función de revisar lo aprendido.

Plan de seguridad personal

El capacitador les pedirá a los participantes que se pongan en parejas. Cada pareja dispondrá de cinco minutos para escribir, a grandes rasgos, lo que incluirían en un plan de seguridad personal. Las siguientes pautas ayudarán a los participantes a elaborar su plan:

- Llamadas telefónicas. (¿Qué harían respecto a las llamadas telefónicas? Posible respuesta: “Si alguien de la oficina se pone en contacto conmigo para hablar de algo delicado y estoy en un tren lleno de gente, pospondré la llamada hasta que llegue a mi destino y pueda mantener una conversación en privado”.);
- Mensajes de texto;
- Aplicaciones:
 - Aplicaciones que deben eliminarse (por ejemplo: “Eliminaré la aplicación Map my location”);
 - Aplicaciones que se deben utilizar con prudencia;
 - Aplicaciones que se deben utilizar activamente.

Al cabo de cinco minutos, el capacitador les pedirá a los participantes que vuelvan a formar un círculo (como en la sesión Debate) e instará a cada pareja a compartir sus conclusiones.

SaferJourno: recursos de seguridad digital para capacitadores de medios de comunicación es un proyecto de Internews que complementa el trabajo hecho en [SpeakSafe](#) y [LevelUp](#). Creado y compartido bajo [licencia Creative Commons Attribution-NonCommercial 3.0 Unported \(CC BY-NC 3.0\)](#).



MAC OS X: SEGURIDAD PARA LOS TELÉFONOS CELULARES

Este apartado incluye aplicaciones y ejercicios útiles para aquellos participantes que utilicen Mac OS X y dispositivos iOS. Los capacitadores que trabajen en parejas pueden repartirse tareas durante la sesión de Profundización: uno puede trabajar con los usuarios de Windows y Android y el otro, con los de OS X e iOS.

Software e instalación

- TextSecure (en proceso de desarrollo)
 - Solicite que le envíen una notificación cuando la versión estable esté disponible.
- ChatSecure
 - [Página de ayuda.](#)

NOTA: Si desea mostrar cómo utilizar la versión de ChatSecure para iOS, le recomendamos que usted o un cocapacitador se la instale y se familiarice con ella antes del taller. Una vez instalada, ChatSecure para iOS funciona igual que la versión para Android.

Profundización

PARTE I: Configuración del sistema. Dispositivos iOS (iPhone o iPad)

La primera parte de la sesión de profundización será bastante corta, especialmente teniendo en cuenta que la función de cifrado ya está habilitada de forma predeterminada en los dispositivos iOS 4 y versiones posteriores. Sin embargo, esta función presenta algunas limitaciones.

Ejercicios nros. 1 y 2: Pantalla de bloqueo y contraseñas largas en iOS

- Por defecto, la contraseña de los dispositivos iOS es de cuatro dígitos (y se denomina *código simple*). Cuatro dígitos es mejor que nada, pero es muy aconsejable establecer una contraseña alfanumérica más larga.

Para asignar un *código simple* de cuatro dígitos:

- Vaya a Ajustes→General→Código.
- Siga las instrucciones para crear el código de cuatro dígitos.

Asignar una contraseña alfanumérica (**recomendado**)

- En la misma pantalla, desactive la opción Código simple y siga las instrucciones para crear una contraseña alfanumérica más larga. ¡Cuanto más larga y compleja, mejor! Siempre que pueda recordarla... En el apartado "[Elementos de una contraseña sólida](#)" de Security in-a-box encontrará consejos útiles.

Después de asignar la contraseña, vaya a Solicitar y seleccione De inmediato. De este modo, en cuanto deje de utilizar el celular, el bloqueo automático se activará instantáneamente.

Ideas clave que hay que transmitir

- Apple ofrece una función de cifrado (denominada *protección de datos*) en dispositivos con iOS 4 y versiones posteriores, y en iPhone 3GS y versiones posteriores. Sin embargo, los usuarios necesitan tener una contraseña para poder activar la función integrada de cifrado.
- A diferencia de la función de cifrado integrada de Android, que protege todos los datos, la función de Apple no ofrece un cifrado completo de datos, es decir, no todo lo que contenga el dispositivo va a estar cifrado aunque la protección de datos esté activada. Esto se debe a que las aplicaciones no desarrolladas por Apple tienen que ser activadas por sus desarrolladores para ser compatibles con el sistema de cifrado de Apple. De manera que si los usuarios tienen contraseña y habilitan la protección de datos, las aplicaciones de Apple y sus correspondientes datos estarán cifrados; sin embargo, no hay garantía alguna de que las aplicaciones de otras compañías y sus correspondientes datos estén cifrados también. De hecho, es casi imposible saber si las aplicaciones de otras compañías están diseñadas para adoptar la función de cifrado integrada de iOS o no, especialmente si, como sucede a menudo, no son de código abierto. Es importante que el capacitador haga esta precisión, por si acaso los participantes utilizan a diario una

aplicación de otra compañía para gestionar o guardar información confidencial en sus dispositivos.

Ejercicio solo para Mac: Habilitar la función Borrar datos

- iOS también ofrece la función de borrar todos los datos de un dispositivo después de diez intentos fallidos de introducción de la contraseña. Aconsejamos que los usuarios habiliten esta función. Aunque no podrá contrarrestar ataques sofisticados por parte de adversarios con recursos que dispongan de un acceso ininterrumpido durante un tiempo ilimitado a un dispositivo, sí podrá evitar la mayoría de los intentos de ataque y de acceder a un dispositivo en un breve periodo de tiempo (por ejemplo, cuando un usuario deja el celular desatendido durante unos minutos y alguien intenta tener acceso a sus datos).

Pasos para activar esta función

- Vaya a Ajustes→Seguridad→Cifrado
- Active Borrar datos

Materiales útiles:

- Guía: [Elementos de una contraseña sólida](#) (Security in-a-box).

GLOSARIO

Las definiciones de términos que se muestran a continuación se proporcionan bajo [licencia Creative Commons Attribution-Share Alike 3.0 Unported](#) e incluyen entradas creadas por Tactical Technology Collective, Front Line Defenders e Internews.

El vocabulario relacionado con este módulo es el siguiente:

Avast! Antivirus gratuito.

Bluetooth. Estándar físico de las comunicaciones inalámbricas para el intercambio de datos a través de distancias cortas desde dispositivos móviles y fijos. Bluetooth usa transmisiones de radio de onda corta.

cifrado. Forma de usar las matemáticas para *cifrar* información, o codificarla, de manera que solo pueda *descifrarla* y leerla quien tenga una pieza específica de información, como una contraseña o una clave de cifrado.

cliente de correo electrónico. Aplicación instalada en una PC o dispositivo móvil que organiza el correo y permite a los usuarios leer y escribir mensajes sin conexión a Internet. Algunos ejemplos de aplicaciones conocidas son Outlook de Microsoft y Thunderbird de Mozilla.

elusión. Acto de sortear filtros de Internet para acceder a sitios y otros servicios de Internet que estén bloqueados.

firewall. Herramienta que protege la computadora de conexiones no seguras a redes locales e Internet.

IMEI (*international mobile equipment identity*; **en español, identidad internacional de dispositivo móvil**). Identificador único de un dispositivo móvil determinado e independiente del número de teléfono del cliente, que se almacena en la tarjeta SIM. A veces, los proveedores de servicios utilizan el código IMEI para bloquear dispositivos que se han declarado como robados.

malware. Término general para referirse a todo software malicioso, incluidos los virus, el spyware, los caballos de Troya y a otras amenazas de este tipo.

metadatos. Información relacionada con los medios y las comunicaciones digitales que aunque no sea obvio a ojos del usuario puede contener información que lo identifica. Por ejemplo, una llamada telefónica puede contener la fecha y la hora en que se efectuó y una fotografía puede ir vinculada a información sobre la ubicación desde donde se tomó o el modelo de la cámara con que se tomó. Un documento podría incluir el nombre de la PC que lo creó.

pirata informático (*hacker*). En este contexto, delincuente informático malintencionado que intenta acceder a información delicada o tomar control vía remota de la computadora del usuario.

proveedor de servicios. Compañía privada o pública que presta a sus clientes servicios de telefonía móvil o servicios de Internet.

proxy. Servicio intermediario mediante el cual el usuario puede canalizar toda o una parte de su comunicación en Internet. Los proxies pueden utilizarse para eludir la censura en la Web. Un proxy puede ser público o puede que el usuario tenga que iniciar sesión con su nombre de usuario y contraseña para entrar. Únicamente algunos proxies son seguros, lo que significa que usan cifrado para proteger la privacidad de la información que pasa entre la computadora del usuario y los servicios de Internet a los que dicho usuario se conecta por medio del proxy.

software gratuito de código abierto (*free and open-source software*; **FOSS, por sus siglas en inglés**). Familia de software que se consigue sin costo alguno y que no tiene restricciones legales que impidan a los usuarios probar el software, compartirlo o modificarlo.

tarjeta SIM. Tarjeta extraíble y de dimensiones reducidas que se inserta en un celular y a través de la cual una compañía de telefonía provee el servicio a un celular determinado. Las tarjetas SIM también guardan números de teléfono y mensajes de texto.

Tor (*The Onion Router*; **Tor, por sus siglas en inglés**). Herramienta anonimizadora que permite sortear la censura en Internet y ocultar los sitios y servicios web que visita el usuario a fin de que quien esté vigilando al usuario no pueda seguir sus movimientos en línea. También camufla la ubicación del usuario.

verificación en dos pasos. Método de protección de una cuenta web o de un archivo que requiere que el usuario introduzca un mínimo de dos categorías de información al iniciar sesión en vez de simplemente una contraseña.

VPN (*virtual private network*; **en español, red virtual privada**). Las VPN utilizan programas de software en una PC o en un dispositivo móvil para establecer una conexión cifrada a un servidor de Internet. Las VPN no garantizan el anonimato del usuario, es decir, la actividad en línea del usuario es visible al proveedor de servicios de la VPN.

GUÍA DE INICIO RÁPIDO:

CONSEJOS PARA GARANTIZAR LA SEGURIDAD DE TELÉFONOS INTELIGENTES

Los teléfonos inteligentes son un imán de ladrones. Contienen registros de llamadas, listas de contactos, fotografías e información delicada, por lo que es muy importante no perderlos nunca de vista. A continuación presentamos algunas recomendaciones básicas para que el usuario pueda empezar a velar por la seguridad de su celular o teléfono inteligente:

- **Bloquéelo con una contraseña difícil de adivinar.** Bloquee siempre su celular con un código PIN o, aún mejor, con una contraseña alfanumérica. Tanto en Android como en iOS se pueden habilitar bloqueos de pantalla y contraseñas desde los ajustes de seguridad. Los usuarios de iOS también pueden definir que el celular borre todos los datos automáticamente después de un número determinado de intentos fallidos de introducir la contraseña.

Para recomendaciones sobre cómo asignar una contraseña difícil de adivinar, véase "Elementos de una contraseña sólida" (Security-in-a-box).

- **Borre la información delicada:** la pérdida, robo o decomiso de celulares es muy habitual. Por este motivo, no es aconsejable guardar datos delicados en el celular:
 - Haga inventario de la información guardada en su dispositivo. ¿Qué necesita realmente?
 - Si necesita guardar información delicada en el celular, considere la opción de transferirla de la memoria del dispositivo a una tarjeta SIM o a una tarjeta SD externa, que son más fáciles de extraer o destruir.
 - Visite el sitio web del fabricante del celular y lea las instrucciones sobre cómo borrar de forma segura los datos del celular antes de venderlo.

Para más información, véase [Utilizar los teléfonos móviles de la manera más segura posible](#) (Security in-a-box).

- **Cifre todo lo que guarde.** Los teléfonos inteligentes de hoy en día pueden proteger archivos y otro tipo de información guardada en el dispositivo gracias a la función de cifrado, una forma de codificar datos en virtud de la cual se requiere una contraseña para acceder a la información. Explore los ajustes de seguridad de su dispositivo para habilitar esta función y recuerde que nunca está de más hacer copias de seguridad de los datos del celular antes de empezar a cifrar la información. De este modo evitará pérdidas de información involuntarias.
- **Utilice programas de software que protegen la privacidad del usuario.** Los usuarios de Android pueden descargarse aplicaciones de código abierto y gratuitas que protegen la privacidad del usuario en sesiones de chat y en las búsquedas en línea. Para más información sobre estas aplicaciones, consúltense las siguientes páginas [en inglés] de Security in-a-box:
 - [TextSecure](#): protege la privacidad de los mensajes de texto;
 - [ChatSecure](#): protege la privacidad de los mensajes de chat;
 - [Orbot](#): red anonimizadora;
 - [Orweb](#): navegador anonimizador.

Para más información:

- [Utilizar los teléfonos móviles de la manera más segura posible](#) (Security in-a-box);
- [Utilizar teléfonos inteligentes de la manera más segura posible](#) (Security in-a-box).

NOTA: El objeto de esta guía es complementar, y no sustituir, una capacitación presencial o un recurso exhaustivo en línea, ya que tanto dichos recursos como las capacitaciones brindan información mucho más detallada.

GUÍA DE INICIO RÁPIDO:

CONSEJOS PARA GARANTIZAR LA SEGURIDAD DE COMPUTADORAS Y CUENTAS EN LÍNEA

Mantener una PC limpia y protegida es fundamental para garantizar la privacidad digital. Si una PC está infectada con un virus o no saca el máximo partido de algunas funciones básicas de seguridad, es probable que cualquier medida que el usuario tome para proteger datos sea en vano.

A continuación, presentamos algunas recomendaciones básicas para que el usuario pueda empezar a velar por la seguridad de su PC y sus cuentas en línea:

- **Instálese una aplicación antivirus.** Una aplicación antivirus ofrece protección contra malware (software malicioso) que puede dañar su PC o brindarle a alguien acceso remoto a sus archivos. Si ya dispone de una aplicación antivirus, compruebe que es legítima. Una opción de antivirus gratuito que da resultados comparables a los antivirus de pago es Avast!

Para más recomendaciones, véase "[Proteger tu computadora de software malicioso y piratas informáticos](#)" (Security in-a-box).

- **Actualice todas las aplicaciones.** Es necesario actualizar las aplicaciones de antivirus constantemente para que estén al día de nuevos virus y otras vulnerabilidades de seguridad. La mayoría de las aplicaciones de antivirus se actualizan automáticamente, pero algunas requieren actualizaciones manuales. Dedique cinco minutos a descubrir los métodos de actualización de su antivirus y a comprobar que el programa está al día. Asimismo, acostúmbrese a actualizar todas las aplicaciones que tenga. Secunia PSI es una herramienta gratuita que puede ayudarle a realizar estas tareas.

Para más información, véase "[Mantener su software actualizado](#)" (Security in-a-box).

- **Habilite las actualizaciones automáticas.** Para Windows, vaya a Panel de control y escriba "Windows Update". Seleccione Activar o desactivar la actualización automática. Compruebe que el sistema está configurado para recibir actualizaciones automáticas. Para Mac OS X, vaya a Preferencias del sistema de App Store (menú Apple→Preferencias del sistema→App Store) y compruebe que la casilla de Instalar archivos de datos del sistema y actualizaciones de seguridad está activada.
- **Compruebe que el firewall está activado.** Tanto las computadoras Windows como las Apple tienen firewalls integrados, es decir, un sistema que ordena a la computadora que bloquee las conexiones a Internet que el usuario no haya autorizado. Para comprobar que el firewall está activado en Windows, vaya al Panel de control y escriba "Firewall de Windows". A continuación, haga clic en el vínculo y verá si la función está activada o no. Para Mac OS X, haga clic en el ícono de menú de Apple y vaya al panel de preferencias de Seguridad. Allí podrá ver si la opción de firewall está activada o no.
- **Asigne contraseñas difíciles de adivinar.** Las contraseñas cortas o fáciles de adivinar (como "c0ntraseña") no garantizan la protección de la PC ni de las cuentas en línea. Siga las siguientes pautas para mejorar la eficacia de su contraseña:
 - Cree una contraseña larga (si solo va a aplicar un consejo de esta lista, que sea este).
 - No incluya información personal en la contraseña.
 - No utilice la misma contraseña para más de una cuenta.

Para más consejos relacionados con la contraseña, véase "[Crear y mantener contraseñas seguras](#)" (Security in-a-box).

- **Cifre toda la información.** Los programas de cifrado le permitirán bloquear los archivos de la PC con una contraseña para que nadie pueda leerlos. Si todavía no ha adoptado el hábito de cifrar archivos, esta aplicación gratuita será de su interés: [TrueCrypt](#). (El paquete de idiomas en Español se encuentra [aquí](#))

Para más información, véase [Proteger los archivos sensibles en tu computadora](#) (Security in-a-box).

NOTA: El objeto de esta guía es complementar, y no sustituir, una capacitación presencial o un recurso exhaustivo en línea, ya que tanto dichos recursos como las capacitaciones brindan información mucho más detallada.

- **Proteja las cuentas con el método de verificación en dos pasos.** La verificación en dos pasos, junto con el uso de una contraseña difícil de adivinar, puede complicarle mucho las cosas a quien desee acceder a sus cuentas en línea. Si decide habilitar esta función para alguna de sus cuentas, además de la contraseña tendrá que introducir un segundo dato, como un código que recibirá en el celular. Estos son algunos de los sitios web más utilizados que integran esta función:
 - [Dropbox](#)
 - [Facebook](#)
 - [Google](#)
 - [Microsoft](#)
 - [Twitter](#)
 - [Yahoo!](#)

- **Piense antes de actuar.**
 - Descargue programas de software **directamente del sitio oficial del desarrollador de la aplicación** o de una página que analice malware, como FileHippo o Softpedia.
 - **No haga clic en los vínculos incluidos en correos electrónicos.** Si quiere visitar una dirección que alguien le ha enviado, copie y pegue el vínculo en el navegador o escríbala en la barra de direcciones.
 - **No abra los archivos adjuntos** si no conoce el remitente del correo electrónico. Recuerde que siempre tiene la opción de escanear un archivo adjunto con el antivirus antes de abrirlo. También puede abrir el archivo en Google Drive.
 - **No se instale software pirata.** Puede que sea barato, pero suele venir acompañado de sorpresas, como virus informáticos.

Sobre Internews

Internews es una organización internacional sin fines de lucro que presta apoyo a medios de comunicación locales de todo el mundo para brindar a la población las noticias y la información que necesitan, la capacidad de conectarse y los medios para hacerse escuchar.

Internews dota a las comunidades de recursos para que puedan transmitir noticias e información locales con integridad e independencia. Con pericia y alcance globales, Internews capacita a profesionales de medios de comunicación y reporteros ciudadanos, idea innovadoras soluciones ante los nuevos retos en materia de comunicación, contribuye a aumentar la cobertura mediática de problemáticas cruciales y apoya la adopción de políticas que garantizan el acceso libre a la información.

Los programas de Internews crean plataformas de diálogo que permiten llevar a cabo debates informados. Estos, a su vez, fomentan el progreso social y económico.

El firme compromiso de Internews con la investigación y la evaluación continua permite idear programas eficaces y sostenibles incluso en los contextos más difíciles.

Fundada en 1982, Internews es una organización designada 501(c)(3), con sede en California. Internews ha trabajado en más de 75 países y actualmente tiene oficinas en África, Asia, Europa, Oriente Medio, América Latina y América del Norte.

OFICINA DE INTERNEWS EN WASHINGTON, D. C.
1640 Rhode Island Ave. NW Suite 700
Washington, D. C. 20036 (Estados Unidos)
+ 1 202 833 5740

SEDE ADMINISTRATIVA DE INTERNEWS
PO Box 4448
Arcata, CA 95518 Estados Unidos
+ 1 707 826 2030

www.internews.org
E-mail: info@internews.org
Twitter: [@internews](https://twitter.com/internews)
facebook.com/internews