NDI
NATIONAL DEMOCRATIC INSTITUTE

Manual de Ciberseguridad

para

Organizaciones de la Sociedad Civil

Una guía para las organizaciones de la sociedad civil que deseen iniciar un plan de ciberseguridad



NDI
NATIONAL DEMOCRATIC INSTITUTE

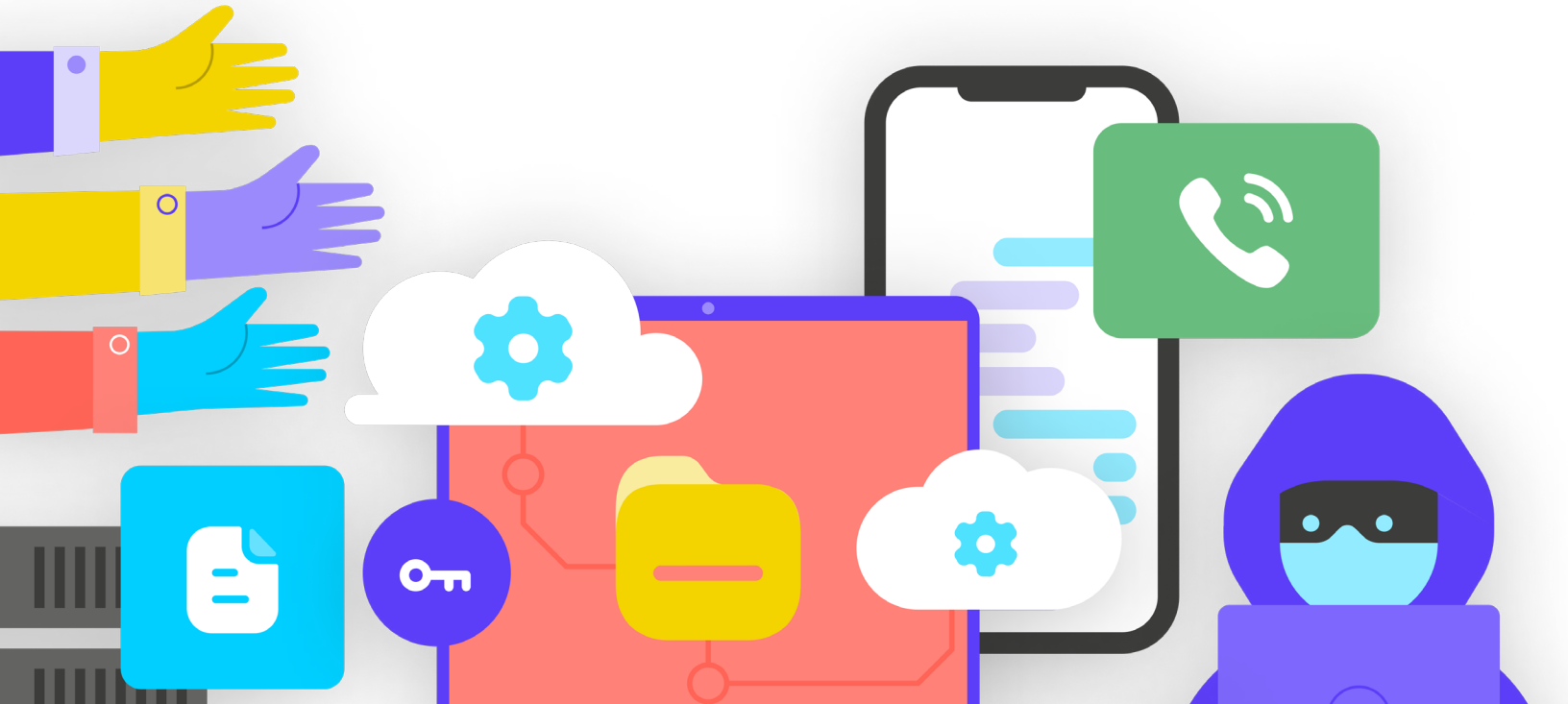
Manual de Ciberseguridad

para

Organizaciones de la Sociedad Civil

Una guía para las organizaciones de la sociedad civil
que deseen iniciar un plan de ciberseguridad

Este documento cuenta con la licencia de Creative Commons Attribution-ShareAlike 4.0 International.
Para ver una copia de esta licencia, visite http://creativecommons.org/licenses/by-sa/4.0/ o envíe
una carta a Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.



Índice

Leyenda Visual 4
Los 10 Principales 6
Autores y Agradecimientos 7
¿Quiénes somos? 7
¿A quién va dirigido este Manual? 8
¿Qué es un plan de seguridad y por qué debe tenerlo mi organización? 8
¿Qué activos tiene su organización y qué quiere proteger? 9
¿Quiénes son sus adversarios y cuáles son sus habilidades y motivaciones? 9
¿A qué amenazas se enfrenta su organización? ¿Qué tan probables y de alto impacto son? 10
Creación del Plan de Ciberseguridad de su Organización 11
Formar una cultura de seguridad 12
Integre la Seguridad en su Estructura Operativa Habitual 13
Consiga el Apoyo de la Organización 14
Establezca un Plan de Capacitación 14
Cimientos Sólidos: Protección de Cuentas y Dispositivos 16
Cuentas Seguras: Contraseñas y Autenticación de Dos Factores 18
Dispositivos Seguros 26
Suplantación de Identidad: Una Amenaza Común para los Dispositivos y las Cuentas 32
Comunicar y almacenar los datos de manera segura 37
Comunicaciones e Intercambio de Datos 38
Almacenamiento Seguro de Datos 50
Mantenerse Seguro en Internet 53
Navegar de Manera Segura 54
Seguridad en las Redes Sociales 64
Mantenga sus Sitios Web en Línea 66
Proteja su Red Wifi 67
Proteger la seguridad física 68
Protección de los Activos Físicos 70
Qué Hacer Cuando las Cosas Van Mal 74
Apéndice A: Recursos Recomendados 78
Apéndice B: Kit de Inicio del Plan de Seguridad 79

Leyenda Visual

A lo largo del Manual, encontrará varios elementos recurrentes y destacados, además del texto principal. He aquí una breve "leyenda" para ayudarle a comprender los elementos fundamentales:



Estudio de Caso

Indica estudios de caso que ponen de relieve el impacto real de un determinado tema en las organizaciones de la sociedad civil a nivel mundial o en un país específico.



Consejos Adicionales

Destaca algunos consejos e información adicionales a los que debe prestar atención mientras lee el Manual.



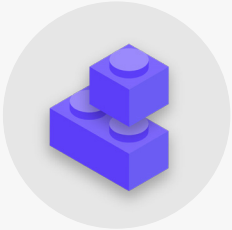
Mundo Real

Expone ejemplos comunes de herramientas de tácticas de ciberseguridad utilizadas en el "mundo real", tanto para bien como para mal.



Avanzado

Indica un tema avanzado: información que es importante que su organización tenga en cuenta, pero que puede ser un poco más técnica o complicada.



Elementos Esenciales del Plan de Seguridad

Indica los "Bloques Esenciales del Plan de Seguridad", que son los elementos clave de cada sección del Manual.

1



Crear una cultura de seguridad

2



Cimientos Sólidos: Protección de Cuentas y Dispositivos

3



Comunicar y almacenar los datos de manera segura

4



Mantenerse seguro en internet

5



Proteger la seguridad física

6



Qué hacer cuando las cosas van mal

Los 10 Principales

Estos diez elementos son fundamentales para el plan de seguridad de su organización. Si busca un punto de partida, mire primero aquí.

1. **Realice una capacitación periódica en materia de seguridad dentro de su organización.**
2. **Esté alerta ante el *phishing* y cuente con un sistema de reportes.**
3. **Utilice el cifrado para todas las comunicaciones, de extremo a extremo, cuando sea posible.**
4. **Exija contraseñas seguras e implemente un administrador de contraseñas en toda su organización.**
5. **Exija la autenticación de dos factores siempre que sea posible.**
6. **Asegúrese de que todos los dispositivos y el software del personal estén actualizados.**
7. **Utilice el almacenamiento seguro en la nube.**
8. **Utilice HTTPS y, en su caso, una VPN, para acceder a internet.**
9. **Proteja los activos físicos de su organización.**
10. **Desarrolle un plan de respuesta a incidentes de la organización.**

Autores y Agradecimientos

Autor principal: **Evan Summers (NDI)**

Autores colaboradores: **Sarah Moulton (NDI); Chris Doten (NDI)**

En el desarrollo de este Manual, nos gustaría agradecer especialmente a nuestros expertos revisores externos que nos proporcionaron valiosos comentarios, ediciones y sugerencias mientras elaborábamos este contenido, incluidos:

Fiona Krakenburger, Open Technology Fund; Bill Budington y Shirin Mori, Electronic Frontier Foundation; Jocelyn Woolbright, Cloudflare; Martin Shelton, Freedom of the Press Foundation; Dave Leichtman, Microsoft; Stephen Boyce, International Foundation for Electoral Systems; Amy Studdart, International Republican Institute; Emma Hollingsworth, Global Cyber Alliance; Caroline Sinders, Convocation Design + Research; Dhyta Caturani; Sandra Pepera, NDI; Aaron Azelton, NDI y Whitney Pfeifer, NDI.

También queremos agradecer todos los increíbles manuales, guías, libros de trabajo, módulos de capacitación y otros materiales desarrollados y mantenidos por la Comunidad de Seguridad Organizacional (OrgSec). Este Manual está diseñado para complementar esos materiales más profundos, combinando las lecciones clave en un recurso único y fácil de leer para las organizaciones de la sociedad civil que deseen comenzar con un plan de ciberseguridad.

Además de inspirarse de manera indirecta en muchos recursos maravillosos recopilados por la comunidad, hemos copiado directamente el lenguaje útil de un puñado de recursos existentes también a lo largo de este Manual, en particular la Guía de Autodefensa de Vigilancia de la **Electronic Frontier Foundation**, el Manual de Seguridad Holística de **Tactical Tech** y una serie de explicaciones del **Center for Democracy and Technology** y la **Freedom of the Press Foundation**. Puede encontrar citas específicas de estos recursos en las secciones siguientes, y los enlaces completos, el autor y la información de la licencia en el **Apéndice A**.

También recomendamos encarecidamente a quien lea este Manual que haga uso de la amplia **biblioteca** de guías y recursos de seguridad digital recopilada y actualizada por el Open Technology Fund.

¿Quiénes somos?

El Instituto Nacional para Asuntos Internacionales (NDI, por sus siglas en inglés) es una organización sin fines de lucro y no partidista, con sede en Washington D.C., que trabaja en asociación en todo el mundo para fortalecer y salvaguardar las instituciones, los procesos, las normas y los valores democráticos con el fin de garantizar una mejor calidad de vida para todos.

El NDI cree que todas las personas tienen derecho a vivir en un mundo que respete su dignidad, seguridad y derechos políticos, y que el mundo digital no es una excepción.

Dentro del NDI, el equipo de Democracia y Tecnología busca fomentar un ecosistema digital global en el que los valores democráticos estén protegidos, se promuevan y puedan prosperar; los gobiernos sean más transparentes e inclusivos; y todos los ciudadanos estén capacitados para hacer que su gobierno rinda cuentas. Llevamos a cabo esta labor apoyando a una red mundial de activistas comprometidos con la resiliencia digital, y mediante la colaboración con socios en herramientas y recursos como este Manual. Puede obtener más información sobre nuestro trabajo en nuestro **sitio web**, siguiéndonos en **Twitter** o comunicándose directamente con **cyberhandbook@ndi.org.** Siempre estamos encantados de saber de usted y de responder a sus preguntas sobre nuestro equipo y nuestro trabajo en materia de ciberseguridad, tecnología y democracia.

¿A quién va dirigido este Manual?

Este Manual se ha redactado con un objetivo sencillo: ayudar a su organización de la sociedad civil a desarrollar un plan de ciberseguridad comprensible y aplicable.

A medida que el mundo se mueve cada vez más en línea, la ciberseguridad no es sólo una palabra de moda, sino un concepto crítico para el éxito de una organización y la seguridad de un equipo. Especialmente para las organizaciones de la sociedad civil en los espacios de la democracia, la defensa, la rendición de cuentas y los derechos humanos, la seguridad de la información (tanto en línea como fuera de ella) es un desafío que requiere atención, inversión y vigilancia.

Es probable que su organización se encuentre, o haya estado ya, en la mira de un ataque de ciberseguridad. Esto no pretende ser alarmista; es una realidad incluso para las organizaciones que no se consideran objetivos particulares.

En un año normal, el Centro de Estudios Estratégicos e Internacionales, que mantiene una **lista continua** de lo que denominan "Incidentes Cibernéticos Significativos", cataloga cientos de ciberataques graves, muchos de los cuales tienen como objetivo docenas, y hasta cientos, de organizaciones a la vez. Además de estos ataques denunciados, es probable que cada año se produzcan cientos de otros ataques de menor envergadura que pasan desapercibidos o no se denuncian, muchos de ellos dirigidos a organizaciones de la sociedad civil que trabajan en apoyo de la democracia, la rendición de cuentas y los derechos humanos. Las organizaciones que representan a las mujeres o a otros grupos marginados suelen ser un objetivo especial.

Los ciberataques de este tipo tienen consecuencias importantes. Tanto si el objetivo de dichos ciberataques es quedarse con su dinero, reprimir su voz, interrumpir las operaciones de su organización, dañar su reputación o incluso robar información que pueda provocar daños psicológicos o físicos a sus socios o a su personal, estas amenazas deben tomarse en serio. Lo bueno es que no es necesario convertirse en un codificador o un técnico para defenderse a sí mismo y a su organización contra las amenazas comunes. Pero hay que estar preparado para invertir algo de esfuerzo, energía y tiempo en el desarrollo y la implementación de un sólido plan de seguridad organizacional. Si nunca ha pensado en la ciberseguridad en su organización, no ha tenido tiempo de dedicarle atención, o conoce algunos aspectos básicos sobre el tema pero cree que su organización podría mejorar su ciberseguridad, este Manual es para usted. Independientemente de su procedencia, este Manual pretende dar a su organización la información esencial que necesita para poner en marcha un sólido plan de seguridad. Un plan que va más allá de las palabras sobre el papel y le permite implementar las mejores prácticas.

¿Qué es un plan de seguridad y por qué debe tenerlo mi organización?

Un plan de seguridad es el conjunto de políticas, procedimientos e instrucciones escritas que su organización ha acordado para alcanzar el nivel de seguridad que usted y su equipo consideran adecuado para mantener la seguridad de su gente, sus socios y su información.

Un plan de seguridad organizativa bien elaborado y actualizado puede tanto mantenerlo a salvo como mejorar su eficacia al proporcionarle la tranquilidad necesaria para centrarse en el importante trabajo diario de su organización. Sin pensar en un plan integral, es muy fácil estar ciego ante algunos tipos de amenazas, centrándose demasiado en un riesgo o ignorando la ciberseguridad hasta que haya una crisis. Cuando se empieza a desarrollar un plan de seguridad, hay que hacerse algunas preguntas importantes que forman un proceso llamado **evaluación de riesgos**. Responder a estas preguntas ayuda a su organización a comprender las amenazas únicas a las que se enfrenta y le permite dar un paso atrás y pensar de forma exhaustiva en lo que necesita proteger y de quién debe protegerlo. Los asesores capacitados, con la ayuda de sistemas como la plataforma de auditoría **SAFETAG** de Internews, pueden ayudar a guiar a su organización a través de este proceso. Si puede acceder a ese nivel de experiencia profesional, merece la pena, pero incluso si no puede someterse a una evaluación completa, debería reunirse con su organización para considerar detenidamente estas cuestiones clave:

1 ¿Qué activos tiene su organización y qué quiere proteger?

Puede empezar a responder estas preguntas **creando un catálogo de todos los activos de su organización**. La información como mensajes, correos electrónicos, contactos, documentos, calendarios y ubicaciones son todos los posibles activos. Los teléfonos, las computadoras y otros dispositivos pueden ser activos. Y las personas, las conexiones y las relaciones también pueden ser activos. Haga una **lista de sus activos** y trate de catalogarlos por su importancia para la organización, dónde los guarda (quizás en varios lugares digitales o físicos) y qué impide que otros accedan a ellos, los dañen o los alteren. Tenga en cuenta que no todo es igual de importante. Si algunos de los datos de la organización son de dominio público, o información que se publica de todos modos, no son secretos que haya que proteger.

2 ¿Quiénes son sus adversarios y cuáles son sus capacidades y motivaciones?

"Adversario" es un término comúnmente utilizado en la seguridad de las organizaciones. En términos sencillos, los adversarios son los actores (individuos o grupos) que están interesados en atacar a su organización, interrumpir su trabajo y obtener acceso a su información o destruirla. En síntesis, los malos. Algunos ejemplos de adversarios potenciales podrían ser estafadores financieros, competidores, autoridades o gobiernos locales o nacionales, o piratas informáticos con motivaciones ideológicas o políticas. Es importante hacer una lista de sus adversarios y pensar críticamente en quién podría querer afectar negativamente a su organización y a su personal. Aunque es fácil imaginar que los actores externos (como un gobierno extranjero o un grupo político concreto) son adversarios, también hay que tener en cuenta que los adversarios pueden ser personas conocidas, como empleados descontentos, exempleados y familiares o parejas que no los apoyan. Diferentes adversarios plantean diferentes amenazas y tienen diferentes recursos y capacidades para interrumpir sus operaciones y obtener acceso a su información o destruirla.

Por ejemplo, los gobiernos suelen disponer de mucho dinero y de potentes capacidades que incluyen el cierre de internet o el uso de costosas tecnologías de vigilancia; las redes de telefonía móvil y los proveedores de internet probablemente tengan acceso a los registros de llamadas y a los historiales de navegación; los hackers expertos en redes wifi públicas tienen la capacidad de interceptar comunicaciones o transacciones financieras poco seguras. Incluso puede convertirlo en su propio adversario si, por ejemplo, borra accidentalmente archivos importantes o envía mensajes privados a la persona equivocada.

Es probable que los motivos de los adversarios difieran según su capacidad, intereses y estrategias. ¿Están interesados en desacreditar a su organización? ¿Quizás pretenden silenciar su mensaje? ¿O tal vez ven a su organización como competencia y quieren obtener una ventaja? Es importante entender la motivación de un adversario porque hacerlo puede ayudar a su organización a evaluar mejor las amenazas que podría plantear.

3 ¿A qué amenazas se enfrenta su organización? ¿Qué tan probables y de alto impacto son?

Al identificar las posibles amenazas, es probable que acabe con una larga lista que puede resultar abrumadora. Puede sentir que cualquier esfuerzo sería inútil, o no saber por dónde empezar. Para ayudar a su organización a dar los siguientes pasos productivos, es útil analizar cada amenaza basándose en dos factores: la probabilidad de que la amenaza tenga lugar y el impacto que puede tener si se produce.

Para medir la probabilidad de una amenaza (tal vez "Baja, Media o Alta" en función de si es poco probable que se produzca un evento determinado, si podría ocurrir o si sucede con frecuencia), puede utilizar la información que conoce sobre la capacidad y la motivación de sus adversarios, el análisis de incidentes de seguridad anteriores, las experiencias de otras organizaciones similares y, por supuesto, la presencia de cualquier estrategia de mitigación existente que su organización haya puesto en marcha.

Para medir el impacto de una amenaza, piense en cómo sería su mundo si la amenaza se produjera realmente. Hágase preguntas como "¿cómo nos ha perjudicado la amenaza como organización y como personas, tanto física como mentalmente?", "¿cuán duradero es el efecto?", "¿crea esto otras situaciones perjudiciales?" y "¿cómo obstaculiza nuestra capacidad de alcanzar nuestros objetivos organizativos ahora y en el futuro?". Al responder a estas preguntas, considere si la amenaza es de impacto bajo, medio o alto.

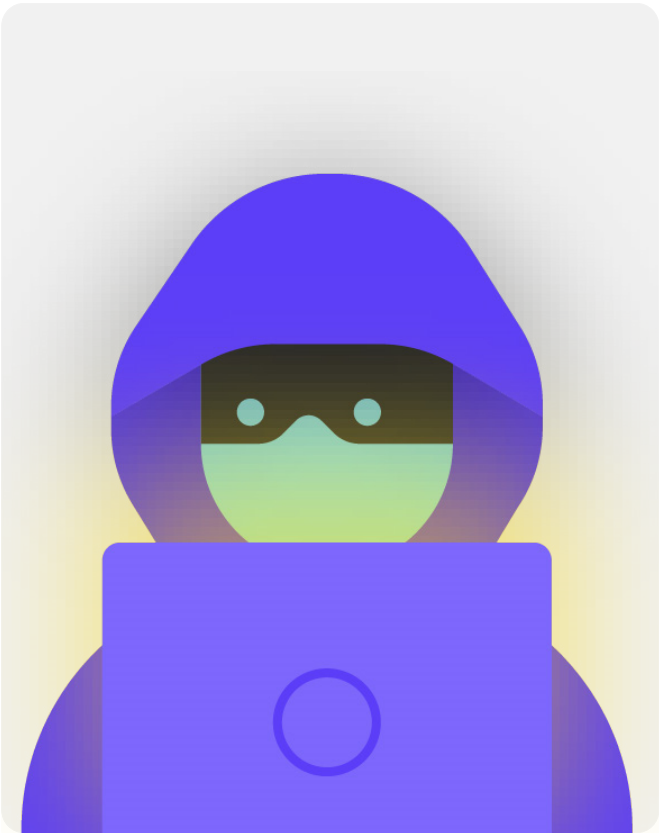
Una vez que haya clasificado sus amenazas por probabilidad e impacto, podrá empezar a elaborar un plan de acción más informado. Al centrarse en las amenazas más probables

Y que tendrán importantes repercusiones negativas, estará canalizando sus limitados recursos de la manera más eficiente y eficaz posible.

Su objetivo es siempre mitigar el mayor riesgo posible, pero nadie –ni el gobierno o la empresa con más recursos del mundo– puede eliminar por completo el riesgo. Y eso está bien: puede hacer mucho para protegerse a sí mismo, proteger a sus colegas y a su organización ocupándose de las mayores amenazas.



Para ayudarle a gestionar este proceso de evaluación de riesgos, considere la posibilidad de utilizar una hoja de trabajo como ésta desarrollada por la Electronic Frontier Foundation. Tenga en cuenta que la información que desarrolle como parte de este proceso (como una lista de sus adversarios y las amenazas que representan) podría ser en sí misma sensible. Por lo tanto, es importante mantener la seguridad.



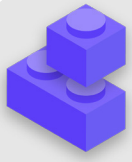
Creación del Plan de Ciberseguridad de su Organización

Si bien el plan de seguridad de cada organización será un poco diferente en función de su evaluación de riesgos y de la dinámica de la organización, algunos conceptos básicos son casi universales.

Este Manual aborda estos conceptos esenciales de manera que ayude a su organización a elaborar un plan de seguridad concreto basado en soluciones prácticas y aplicaciones del mundo real.

Este Manual trata de ofrecer opciones y sugerencias gratuitas o de muy bajo costo. Pero tenga en cuenta que el costo más importante asociado a la implantación de un plan de seguridad eficaz será el tiempo que usted y su organización necesiten para hablar, aprender y aplicar su nuevo plan. Sin embargo, dados los riesgos a los que probablemente se enfrente su organización, esta inversión merecerá la pena con creces.

En cada sección, encontrará una explicación de un tema clave que su organización y su personal deben conocer: qué es y por qué es importante. Cada tema va acompañado de estrategias esenciales, enfoques y herramientas recomendadas para limitar el riesgo, así como de consejos y enlaces a recursos adicionales que pueden ayudarle a aplicar dichas recomendaciones en toda su organización.



Kit de Inicio del Plan de Seguridad

Para ayudar a su organización a procesar las lecciones del Manual y convertirlas en un plan real, utilice este kit de inicio. Puede imprimir el kit o rellenarlo digitalmente mientras lee el Manual en línea. A medida que tome notas y comience a actualizar o elaborar su plan de seguridad, asegúrese de hacer referencia a los “Bloques del Plan de Seguridad” detallados también en cada sección. Ningún plan de seguridad está completo si no aborda, como mínimo, estos elementos esenciales.



Aproveche también otros recursos que pueden ayudarle a elaborar y aplicar su plan. Como organización de la sociedad civil, la aplicación gratuita SOAP (“Securing Organizations with Automated Policymaking”) puede ayudarle a simplificar y automatizar la creación de su plan de seguridad.

Utilice también recursos de capacitación gratuitos, como el Planificador de Seguridad de Consumer Reports, la aplicación Umbrella de Security First, el Proyecto Totem de Free Press Unlimited y Greenhost, las Guías de Herramientas de Conexo, y la ciberhigiene para organizaciones basadas en misiones de Global Cyber Alliance, que incluyen recursos sobre muchas de las mejores prácticas mencionadas en este Manual y enlaces a docenas de herramientas de capacitación que lo ayudarán a aplicar muchos aspectos básicos.



Crear una cultura de seguridad

Crear una cultura de seguridad

Cimientos Sólidos: Protección de Cuentas y Dispositivos

Comunicar y almacenar los datos de manera segura

Mantenerse seguro en internet

Proteger la seguridad física

Qué hacer cuando las cosas van mal

La seguridad tiene que ver con las personas, y para proteger su organización debe asegurarse de que todos los implicados se tomen en serio la ciberseguridad. Cambiar la cultura es difícil, pero unos sencillos pasos y unas conversaciones importantes pueden contribuir en gran medida a crear una atmósfera que fomente la resistencia de su personal y su organización frente a las amenazas a la seguridad. Uno de los pasos más sencillos, pero más importantes, para construir esta cultura de seguridad organizativa es comunicarla dentro de la organización, y que los líderes sean siempre un modelo de buen comportamiento.

Integre la Seguridad en su Estructura Operativa Habitual

Como se describe en detalle en la Guía de Seguridad Holística de Tactical Tech, es esencial crear espacios regulares y seguros para hablar de los diferentes aspectos de la seguridad.

De este modo, si los miembros del equipo están preocupados por la seguridad, estarán menos ansiosos por parecer paranoicos o por hacer perder el tiempo a los demás. **Programar charlas periódicas sobre seguridad** también normaliza la frecuencia de la interacción y reflexión sobre asuntos relacionados con la seguridad, de modo que los temas no se olviden, y es más probable que los miembros del equipo lleven al menos una conciencia pasiva de la seguridad a su trabajo continuo. No es necesario que sea cada semana, pero sí que sea un recordatorio recurrente. Estos debates no sólo deben dejar espacio para los temas de seguridad técnica, sino también para las cuestiones que afectan la comodidad y seguridad del personal, como los conflictos con la comunidad, el acoso en línea (y fuera de ella) o los problemas relacionados con el uso y la aplicación de las herramientas digitales. Las conversaciones pueden incluir incluso temas como los hábitos de intercambio de información fuera de línea y las formas en que el personal asegura o no la información fuera del trabajo. Después de todo, es importante recordar que la seguridad de una organización es tan fuerte como su eslabón más débil. Una forma de lograr un compromiso constante es añadir la seguridad al orden del día de una reunión ordinaria. También puede rotar la responsabilidad de organizar y facilitar un debate sobre la seguridad entre los miembros de la organización, lo que puede ayudar a desarrollar la idea de que la seguridad es responsabilidad de todos y no solo de unos pocos. A medida que se empiece a formalizar el debate sobre la seguridad, es probable que el personal se sienta más cómodo discutiendo estas cuestiones importantes entre ellos también en entornos menos formales.

También es importante incorporar elementos de seguridad en el funcionamiento normal de la organización, por ejemplo, durante la incorporación de los empleados, y pensar en cortar el acceso para la desvinculación de la empresa. La seguridad no debe ser una "cosa extra" de la que preocuparse, sino una ***parte integral de su estrategia y sus operaciones*.**

Recuerde que todos los planes de seguridad deben ser considerados documentos vivos, y deben ser reevaluados y discutidos regularmente, especialmente cuando se incorporan a la organización nuevos empleados o voluntarios o su contexto de seguridad cambia.

Planifique la revisión de su estrategia y las actualizaciones anuales, o si se producen cambios importantes en la estrategia, las herramientas o las amenazas a las que se enfrenta.

Consiga el Apoyo de la Organización

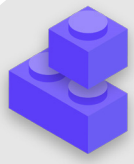
Parte de una cultura de seguridad exitosa es también asegurarse la aceptación de su plan de seguridad en toda la organización.

Es fundamental que esto incluya un apoyo y una orientación firmes y explícitos por parte de la dirección de la organización, que en muchos casos será la que tome la decisión final de asignar tiempo, recursos y energía al desarrollo y la aplicación de un plan de seguridad eficaz. Si ellos no se lo toman en serio, nadie más lo hará. Para lograr esta aceptación en toda la organización, piense cuidadosamente cuándo y cómo presentar su plan, hágalo de forma clara, asegúrese de que los líderes refuercen los mensajes y guíe a todos a través de todos los elementos y pasos del plan para que no haya ningún misterio o confusión sobre lo que está tratando de lograr. Muchos donantes exigen ahora a los beneficiarios que mantengan una seguridad sólida, por lo que insistir en ello al personal puede ser una buena manera de generar un mayor apoyo de la organización. Cuando hable de seguridad, evite las tácticas de miedo. A veces, las amenazas a las que se enfrentan su organización y su personal pueden dar miedo, pero intente centrarse en compartir los hechos y crear un espacio de calma para las preguntas y preocupaciones. Hacer que los peligros parezcan demasiado amenazantes puede provocar que la gente los descarte por sensacionalista o simplemente se dé por vencida, pensando que nada de lo que haga importa, y nada podría estar más lejos de la realidad.

Establezca un Plan de Capacitación

Una vez que haya desarrollado un plan y se haya comprometido con él, piense en cómo va a capacitar a todo el personal (y a los voluntarios) en estas nuevas buenas prácticas.

Puede ser una táctica útil exigir una capacitación periódica y hacer que la asistencia a la capacitación sea obligatoria y un punto de evaluación para las revisiones del rendimiento del personal. Evite crear consecuencias duras y negativas para el personal que tenga problemas con los conceptos de seguridad. Tenga en cuenta que algunos miembros del personal pueden adaptarse y aprender sobre la tecnología de forma diferente a otros, en función de los distintos niveles de familiaridad con las herramientas digitales e internet. El miedo al fracaso no hace más que desanimar al personal a la hora de informar los problemas o buscar ayuda. Sin embargo, la creación de una responsabilidad positiva y de recompensas por el éxito de la capacitación y la adopción de políticas puede ayudar a incentivar la mejora en toda la organización. Puede encontrar un valioso apoyo adicional a través de las redes locales o internacionales de capacitación en seguridad digital y los recursos de capacitación gratuitos, como la **aplicación Umbrella de Security First**, el **proyecto Totem** de Free Press Unlimited y Greenhost y el **portal de aprendizaje** de Global Cyber Alliance.



Crear una cultura de seguridad

- **Programe conversaciones y capacitaciones periódicas sobre la seguridad y su plan de seguridad.**
- **Involucre a todo el mundo: distribuya la responsabilidad de la aplicación de su plan de seguridad entre toda la organización.**
- **Asegúrese de que el liderazgo muestre un buen comportamiento de seguridad y un compromiso con su plan.**
- **Evite las tácticas de miedo o el castigo: recompense las mejoras y cree un espacio cómodo para que el personal informe los problemas y busque ayuda.**
- **Actualice su plan de seguridad anualmente o después de cambios importantes en la organización.**



Cimientos Sólidos: Protección de Cuentas y Dispositivos

¿Por qué centrarse en las cuentas y los dispositivos? Porque constituyen la base de todo lo que su organización hace digitalmente.

Es casi seguro que usted accede a información sensible, se comunica interna y externamente y guarda información privada en ellos. Si no son seguros, entonces todas estas cosas y más pueden ponerse en riesgo. Por ejemplo, si los hackers observan las pulsaciones de su teclado o escuchan su micrófono, sus conversaciones serán captadas por muy seguras que sean sus aplicaciones de mensajería. O si un adversario accede a las cuentas de las redes sociales de su organización, podría dañar fácilmente su reputación y credibilidad, socavando el éxito de su trabajo. Por lo tanto, es esencial, como organización, asegurarse de que todo el mundo esté tomando algunas medidas simples pero eficaces para mantener sus dispositivos y cuentas seguras. Es importante señalar que estas recomendaciones incluyen también las cuentas y los dispositivos personales, ya que suelen ser objetivos fáciles para los adversarios. Los hackers irán gustosamente por el objetivo más fácil y entrarán en una cuenta personal o en una computadora hogareña si su equipo los utiliza para comunicarse y acceder a información importante.



Cuentas Seguras y Sociedad Civil

La ampliamente publicitada piratería de SolarWinds revelada a finales de 2020, que comprometió a más de 250 organizaciones, incluidos la mayoría de los departamentos del gobierno de los Estados Unidos, proveedores de tecnología como Microsoft y Cisco, y ONG, fue en parte el resultado de que los piratas informáticos adivinaron contraseñas deficientes que se utilizaban en importantes cuentas de administrador. En general, alrededor del 80 % de las infracciones relacionadas con la piratería informática se producen debido a contraseñas débiles o reutilizadas.

Con la creciente prevalencia de violaciones de contraseñas como ésta y el acceso más fácil de todo tipo de adversarios a sofisticadas herramientas de piratería de contraseñas, la autenticación de dos factores es una necesidad de seguridad para las organizaciones de la sociedad civil. Un ejemplo de cuentas de la sociedad civil atacadas fue denunciado por Facebook en 2020.

Según su **informe**, los grupos de hackers en Bangladesh tenían como objetivo las cuentas de activistas de la sociedad civil local, periodistas y minorías religiosas. Desgraciadamente, los hackers lograron comprometer algunas de estas cuentas de Facebook, incluida la de un administrador de la página de Facebook de un grupo local. Con acceso a la cuenta de administrador, los hackers eliminaron a los restantes administradores, tomaron el control y desactivaron la página, impidiendo que el grupo compartiera información clave y se comunicara con su público. La investigación de Facebook descubrió que las cuentas se vieron comprometidas probablemente por varios medios, incluido el abuso de su proceso de recuperación de cuentas. Si todas las cuentas hubieran utilizado la autenticación de dos factores, estos ataques habrían sido mucho más difíciles de ejecutar para los hackers.



Cuentas Seguras: Contraseñas y Autenticación de Dos Factores

En el mundo actual, es probable que su organización y su personal tengan docenas, y hasta cientos, de cuentas que, en caso de ser violadas, podrían exponer información sensible o incluso hacer que personas en riesgo resulten heridas.

Piense en las diferentes cuentas que puede tener el personal individual y la organización en su conjunto: correo electrónico, aplicaciones de chat, redes sociales, banca en línea, almacenamiento de datos en la nube... y tiendas de ropa, la pizzería local, periódicos y cualquier otro sitio web o aplicación en la que se conecte. Una buena seguridad en el mundo actual requiere un enfoque diligente para proteger todas estas cuentas de los ataques. Eso empieza por garantizar una buena higiene de las contraseñas y el uso de la autenticación de dos factores en toda la organización.

¿CUÁL ES UNA BUENA CONTRASEÑA?

Hay tres claves para una buena contraseña: longitud, aleatoriedad y singularidad.

LONGITUD	Cuanto más larga sea la contraseña, más difícil será para un adversario adivinarla. Hoy en día, la mayoría de la piratería de contraseñas es realizada por programas informáticos, y esos nefastos programas descifran rápidamente una contraseña corta. Por ello, es esencial que sus contraseñas tengan como mínimo 16 caracteres, o al menos 5 palabras, y preferentemente más.
ALEATORIEDAD	Aunque una contraseña sea larga, no es muy buena si es algo que un adversario puede adivinar fácilmente sobre usted. Evite incluir información como su fecha de nacimiento, ciudad natal, actividades favoritas u otros datos que alguien podría averiguar sobre usted en una rápida búsqueda por internet.
SINGULARIDAD	Tal vez la "peor práctica" en materia de contraseñas sea utilizar la misma contraseña para varios sitios. La repetición de contraseñas es un gran problema porque significa que cuando una sola de esas cuentas se ve comprometida, cualquier otra cuenta que utilice esa misma contraseña también es vulnerable. Si utiliza la misma frase de acceso en varios sitios, puede aumentar en gran medida el impacto de un error o una violación de datos. Aunque a usted no le importe su contraseña para la biblioteca local, si la piratean y usted utiliza la misma contraseña en una cuenta más delicada, podrían robarle información importante.



Una forma fácil de lograr estos objetivos de longitud, aleatoriedad y singularidad es elegir tres o cuatro palabras comunes pero aleatorias. Por ejemplo, su contraseña podría ser "lámpara flor oso verde", que es fácil de recordar pero difícil de adivinar. Puede echar un vistazo a **este sitio web** de Better Buys para ver una estimación de lo rápido que se pueden descifrar las contraseñas malas.

USE UN ADMINISTRADOR DE CONTRASEÑAS PARA AYUDAR

Así que sabe que es importante que todos los miembros de la organización utilicen una contraseña larga, aleatoria y diferente para cada una de sus cuentas personales y de la organización, pero ¿cómo lo hace realmente? Memorizar una buena contraseña para docenas (y hasta cientos) de cuentas es imposible, así que todo el mundo tiene que hacer trampas. La forma incorrecta de hacerlo es reutilizar las contraseñas. Por suerte, podemos recurrir a los administradores de contraseñas digitales para hacernos la vida mucho más fácil (y nuestras prácticas de contraseñas mucho más seguras). Estas aplicaciones (a muchas de las cuales se puede acceder a través de una computadora o un dispositivo móvil) pueden crear, almacenar y gestionar contraseñas para usted y toda su organización. Adoptar un administrador de contraseñas seguro significa que solo tendrá que recordar una contraseña muy fuerte y larga, llamada contraseña principal (históricamente conocida como contraseña "maestra"), y al mismo tiempo podrá obtener las ventajas de seguridad que supone utilizar contraseñas buenas y únicas en todas sus cuentas. Utilizará esta contraseña principal [y posiblemente un segundo factor de autenticación (2FA), del que hablaremos en la siguiente sección] para abrir su administrador de contraseñas y desbloquear el acceso a todas sus otras contraseñas. Los administradores de contraseñas también pueden compartirse entre varias cuentas para facilitar el intercambio seguro de contraseñas en toda la organización.

¿Por qué tenemos que usar algo nuevo? ¿No podemos anotarlas en un papel o en una planilla de cálculo en la computadora?

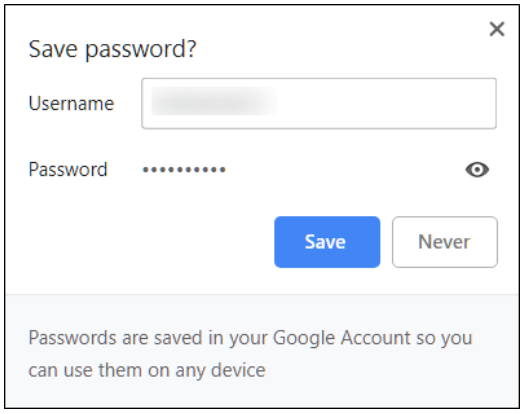
Lamentablemente, hay muchos enfoques comunes para la administración de contraseñas que no son seguros. Almacenar las contraseñas en hojas de papel (a menos que las guarde bajo llave en una caja fuerte) puede exponerlas a robos físicos, a miradas indiscretas y a su fácil pérdida y deterioro. Guardar las contraseñas en un documento en su computadora hace que sea mucho más fácil para un hacker, o para alguien que robe su computadora, no solo tener su dispositivo sino también acceso a todas sus cuentas. Utilizar un buen administrador de contraseñas es tan fácil como ese documento, pero mucho más seguro.

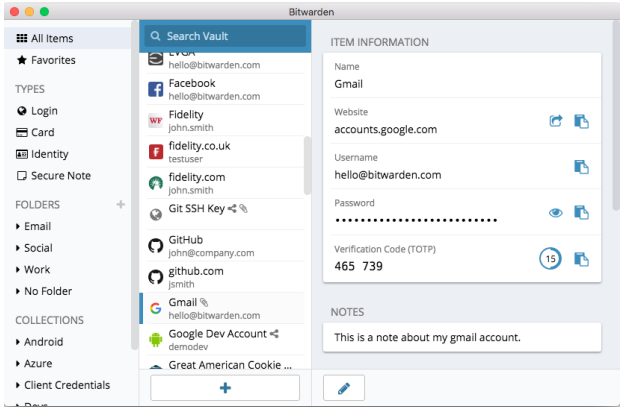
¿Por qué debemos confiar en un administrador de contraseñas?

Los administradores de contraseñas de calidad hacen esfuerzos extraordinarios (y emplean excelentes equipos de seguridad) para mantener sus sistemas seguros. Las buenas aplicaciones de administración de contraseñas (a continuación se recomiendan algunas) también están configuradas para que no tengan la capacidad de "desbloquear" sus cuentas. Esto significa que, en la mayoría de los casos, incluso si fueran pirateados u obligados legalmente a entregar información, no podrían perder o entregar sus contraseñas. También es importante recordar que es infinitamente más probable que un adversario adivine una de sus contraseñas débiles o repetidas, o que encuentre una en una **violación de datos pública**, que violen los sistemas de seguridad de un buen administrador de contraseñas. Es importante ser escéptico, y definitivamente no debe confiar ciegamente en todos los programas y las aplicaciones, pero los administradores de contraseñas de buena reputación tienen todos los incentivos necesarios para hacer lo correcto.



En lugar de utilizar su navegador (como Chrome, mostrado a la izquierda) para guardar sus contraseñas, utilice un administrador de contraseñas exclusivo (como Bitwarden, mostrado a la derecha). Los administradores de contraseñas tienen características que hacen la vida más segura y práctica para su organización.





¿Qué pasa con el almacenamiento de contraseñas en el navegador?

Guardar las contraseñas en el navegador no es lo mismo que utilizar un administrador de contraseñas seguro. En resumen, no debe utilizar Chrome, Firefox, Safari ni ningún otro navegador como administrador de contraseñas. Aunque sin duda es una mejora con respecto a escribirlas en papel o a guardarlas en una planilla de cálculo, las funciones básicas para guardar contraseñas de su navegador web dejan que desear desde el punto de vista de la seguridad. Estas deficiencias también le roban gran parte de la comodidad que un buen administrador de contraseñas aporta a su organización. La pérdida de esta comodidad hace más probable que las personas de su organización continúen con las malas prácticas de crear y compartir contraseñas.

Por ejemplo, a diferencia de los administradores de contraseñas exclusivos, las funciones integradas de "guardar esta contraseña" o "recordar esta contraseña" de los navegadores no ofrecen compatibilidad móvil sencilla, funcionalidad entre navegadores y herramientas de generación ni auditoría de contraseñas sólidas. Estas características son una gran parte de lo que hace que un administrador de contraseñas exclusivo sea tan útil y beneficioso para la seguridad de su organización. Los administradores de contraseñas también incluyen funciones específicas de la organización (como el uso compartido de contraseñas) que no solo aportan valor a la seguridad individual, sino a la organización en su conjunto. Si ha estado guardando contraseñas con su navegador (intencionalmente o no), tómese un momento para eliminarlas.

¿Qué administrador de contraseñas debemos utilizar?

Existen muchas buenas herramientas de administración de contraseñas que se pueden configurar en menos de treinta minutos. Si busca una opción de confianza en línea para su organización a la que se pueda acceder desde múltiples dispositivos en cualquier momento, 1Password (a partir de 2.99 dólares mensuales por usuario) o la gratuita y de código abierto BitWarden están bien respaldadas y son recomendables. Una opción en línea como BitWarden puede ser excelente tanto por la seguridad como por la comodidad. BitWarden, por ejemplo, le ayudará a crear contraseñas únicas y sólidas y acceder a ellas desde múltiples dispositivos a través de extensiones del navegador y una aplicación móvil. Con la

versión paga (10 dólares por un año completo), BitWarden también proporciona informes sobre contraseñas reutilizadas, débiles y posiblemente violadas para ayudarlo a estar al tanto de todo. Una vez que haya configurado su contraseña principal (conocida como contraseña maestra), también debería activar la autenticación de dos factores para mantener el banco de datos de su administrador de contraseñas lo más seguro posible.

Es esencial **practicar una buena seguridad cuando se utiliza el administrador de contraseñas**, también. Por ejemplo, si utiliza la extensión del navegador de su administrador de contraseñas o inicia sesión en BitWarden (o en cualquier otro administrador de contraseñas) en un dispositivo, recuerde cerrar la sesión después de utilizarlo si comparte ese dispositivo o cree que puede correr un mayor riesgo de robo físico. Esto incluye cerrar la sesión de su administrador de contraseñas si deja la computadora o el dispositivo móvil desatendido. Si se comparten contraseñas en toda la organización, asegúrese también de revocar el acceso a las contraseñas (y de cambiar las propias contraseñas) cuando la gente deje la organización. No quiere que un exempleado tenga acceso a la contraseña de Facebook de su organización, por ejemplo.

¿Qué pasa si alguien olvida su contraseña principal?

Es esencial que recuerde su contraseña principal. Los buenos sistemas de administración de contraseñas, como los recomendados anteriormente, no recordarán su contraseña principal por usted ni le permitirán restablecerla directamente por correo electrónico, como podría hacer con los sitios web. Esta es una buena función de seguridad, pero también hace que sea esencial memorizar la contraseña principal cuando se configura por primera vez el administrador de contraseñas. Como ayuda, considere la posibilidad de establecer un recordatorio diario para recordar su contraseña principal cuando cree por primera vez una cuenta de administrador de contraseñas.



Uso de un Administrador de Contraseñas para su Organización

Puede reforzar las prácticas de contraseñas de toda su organización y asegurarse de que todo el personal tenga acceso (y utilice) a un administrador de contraseñas implementando uno en toda la organización. En lugar de que cada miembro del personal establezca el suyo propio, considere la posibilidad de invertir en un plan "de equipo" o "de empresa". Por ejemplo, el plan "organización de equipos" de BitWarden cuesta 3 dólares mensuales por usuario. Con él (u otros planes de equipo de administradores de contraseñas, como 1Password), tiene la posibilidad de administrar todas las contraseñas compartidas en toda la organización. Las funciones de un administrador de contraseñas para toda la organización no solo proporcionan mayor seguridad, sino también comodidad para el personal. Dentro del propio administrador de contraseñas, puede compartir credenciales de forma segura con diferentes cuentas de usuario. Y BitWarden, por ejemplo, también ofrece dentro de su plan de equipo una práctica función de intercambio de texto y archivos cifrados de extremo a extremo, llamada "BitWarden Send". Ambas funciones brindan a su organización más control sobre quién puede ver y compartir qué contraseñas, y proporcionan una opción más segura para compartir credenciales en cuentas de todo el equipo o de grupos. Si se establece un administrador de contraseñas para toda la organización, hay que asegurarse de que alguien se encargue específicamente de eliminar las cuentas del personal y de cambiar las contraseñas compartidas cuando alguien se desvincula del equipo.

¿QUÉ ES LA AUTENTICACIÓN DE DOS FACTORES?

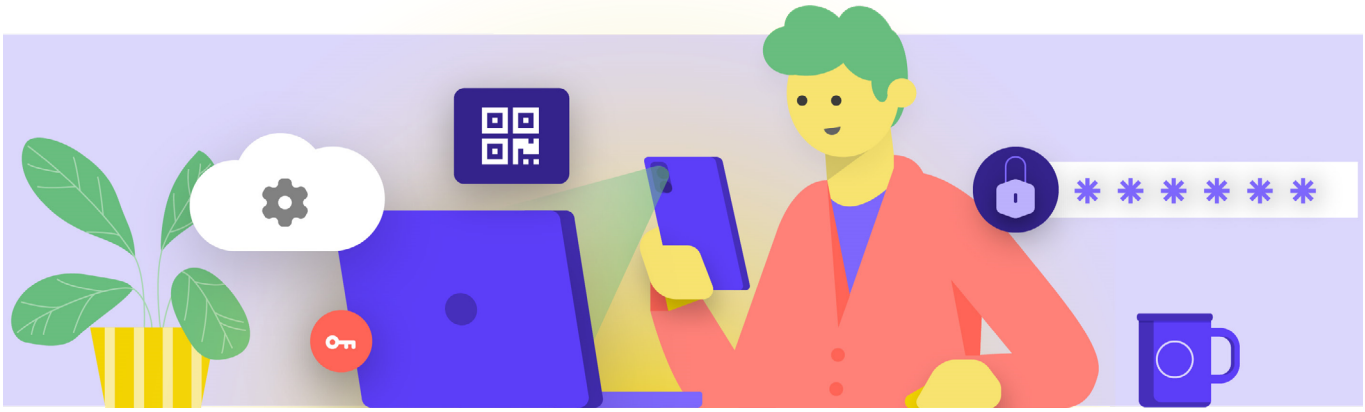
Por muy buena que sea la higiene de sus contraseñas, es muy común que los hackers la eludan. En el mundo actual, mantener sus cuentas seguras frente a algunos actores de amenazas comunes requiere otra capa de protección. Aquí es donde entra en juego la autenticación multifactorial o de dos factores, conocida como 2FA. Hay muchas guías y recursos excelentes que explican la autenticación de dos factores, como el artículo Two Factor Authentication for Beginners de Martin Shelton y Election Cybersecurity 101 Field Guide del Center for Democracy and Technology. Esta sección se basa, en gran medida, en esos dos recursos para ayudar a explicar por qué es tan importante implementar la 2FA en su organización. En resumen, la 2FA refuerza la seguridad de las cuentas al requerir un segundo dato (algo más que una contraseña) para acceder a ellas. El segundo dato suele ser algo que usted tiene, como un código de una aplicación en su teléfono o un token o llave física. Este segundo dato de información actúa como una segunda capa de defensa. Si un hacker roba su contraseña o accede a ella a través de la descarga de contraseñas de una gran filtración de datos, una 2FA eficaz puede impedirle el acceso a su cuenta (y por tanto, a la información privada y sensible). Es de vital importancia asegurarse de que todos los miembros de la organización pongan la 2FA en sus cuentas.

¿CÓMO SE PUEDE CONFIGURAR LA 2FA?

Hay tres métodos comunes para la 2FA: llaves de seguridad, aplicaciones de autenticación y códigos SMS de un solo uso.

Llaves de Seguridad

Las **llaves de seguridad son la mejor opción**, en parte porque son casi completamente a prueba de phishing. Estas "llaves" son tokens de hardware (piense en miniunidades USB) que pueden unirse a su llavero (o permanecer en su computadora) para facilitar el acceso y la protección. Cuando llegue el momento de utilizar la llave para desbloquear una cuenta determinada, solo tiene que introducirla en su dispositivo y tocarla físicamente cuando se le pida durante el inicio de sesión. Hay una amplia gama de modelos que puede comprar en línea (entre 20 y 50 dólares estadounidenses), incluido el estimado Yubikeys. El Wirecutter del New York Times tiene una guía útil con algunas recomendaciones sobre qué llaves comprar. Tenga en cuenta que la misma llave de seguridad puede utilizarse para tantas cuentas como desee. Aunque las llaves de seguridad son caras para muchas organizaciones, iniciativas como el Programa de Protección Avanzada de Google o AccountGuard de Microsoft proporcionan estas llaves de forma gratuita a algunos grupos de riesgo que cumplen los requisitos. Comuníquese con las personas que le entregaron el Manual para ver si pueden ponerse en contacto con esos programas o envíe un correo electrónico a cyberhandbook@ndi.org.



Aplicaciones de Autenticación

La **segunda mejor opción para la 2FA son las aplicaciones de autenticación.** Estos servicios le permiten recibir un código temporal de inicio de sesión de dos factores a través de una aplicación móvil o una notificación push (notificación de inserción) en su teléfono inteligente. Algunas opciones populares y de confianza son Google Authenticator, Authy y Duo Mobile. Las aplicaciones de autenticación también son estupendas porque funcionan cuando no se tiene acceso a la red celular y son de uso gratuito para los particulares. Sin embargo, las aplicaciones de autenticación son más susceptibles al phishing que las llaves de seguridad, ya que los usuarios pueden ser engañados para que introduzcan los códigos de seguridad de una aplicación de autenticación en un sitio web falso. Procure introducir los códigos de acceso solo en sitios web legítimos. Y no "acepte" las notificaciones push de inicio de sesión, a menos que esté seguro de que es usted quien ha hecho la solicitud de inicio de sesión. Cuando se utiliza una aplicación de autenticación, también es esencial estar preparado con códigos de respaldo (que se comentan a continuación) en caso de que pierda o le roben el teléfono.

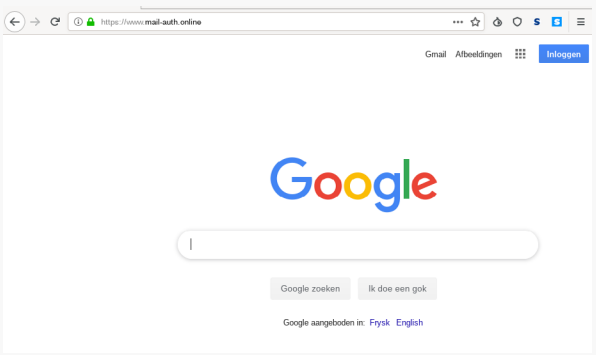
Códigos por SMS

La forma menos segura, pero desgraciadamente aún más común de la 2FA, son los códigos enviados por SMS. Dado que los SMS pueden ser interceptados y los números de teléfono pueden ser suplantados o pirateados a través de su operador de telefonía móvil, los SMS dejan mucho que desear como método para solicitar códigos de 2FA. Es mejor que usar solo una contraseña, pero se recomiendan aplicaciones de autenticación o una llave de seguridad física siempre que sea posible. Un adversario decidido puede obtener acceso a los códigos 2FA de los SMS, normalmente solo llamando a la compañía telefónica y cambiando su tarjeta SIM. Cuando esté listo para empezar a activar la 2FA para todas las cuentas de su organización, utilice este sitio web (https://2fa.directory/) para buscar rápidamente información e instrucciones de servicios específicos (como Gmail, Office 365, Facebook, Twitter, etc.) y para ver qué servicios permiten qué tipos de 2FA.



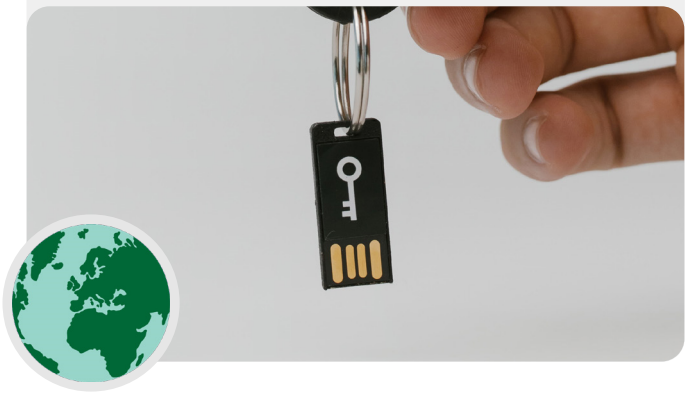
2FA y Sociedad Civil

Según un reciente informe de Amnistía Internacional, los hackers que tienen como objetivo a los defensores de los derechos humanos en Uzbekistán utilizaron ataques phishing para engañar a los usuarios a fin de que compartieran las contraseñas *y* los códigos de autenticación de dos factores de sus cuentas de correo electrónico a través de páginas de inicio de sesión de Gmail falsas. Estos ataques son una forma cada vez más común de "omitir" la autenticación de dos factores. Es importante, incluso con la 2FA implementada, tener cuidado con el lugar donde se escriben los códigos. Mejor aún, puede eliminar este riesgo adoptando llaves de seguridad física.



Llaves de Seguridad en el Mundo Real

Al proporcionar llaves de seguridad física para la autenticación de dos factores a sus más de 85,000 empleados, Google (una organización de muy alto riesgo y muy selectiva) **eliminó de forma efectiva cualquier ataque exitoso de phishing** contra la organización. Este caso demuestra lo eficaces que pueden ser las llaves de seguridad, incluso para las organizaciones de mayor riesgo.



¿QUÉ PASA SI ALGUIEN PIERDE UN DISPOSITIVO 2FA?

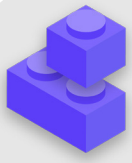
Si utiliza una llave de seguridad, trátela de la misma manera que trataría la llave de su casa o apartamento, si tiene una. En resumen, no la pierda. Sin embargo, al igual que las llaves de su casa, siempre es una buena idea tener una copia de seguridad de la llave registrada en su cuenta que permanezca guardada en un lugar seguro (como una caja fuerte en casa o una caja de seguridad) en caso de pérdida o robo. Alternativamente, debería (para las cuentas que lo permiten) crear códigos de copia de seguridad. Debería guardar estos códigos en un lugar muy seguro, como su administrador de contraseñas o una caja de seguridad física. Dichos códigos de copia de seguridad pueden ser generados dentro de la configuración 2FA de la mayoría de los sitios (el mismo lugar donde se habilita la 2FA en primer lugar), y pueden actuar como una copia de seguridad de la llave en caso de emergencia. El percance más común de la 2FA ocurre cuando la gente reemplaza o pierde los teléfonos que utiliza para las aplicaciones de autenticación. Si utiliza Google Authenticator, no tendrá suerte si le roban el teléfono, a menos que guarde los códigos de copia de seguridad que se generan en el momento de conectar una cuenta a Google Authenticator. Por lo tanto, si utiliza Google Authenticator como aplicación 2FA, asegúrese de guardar los códigos de copia de seguridad de todas las cuentas que conecte en un lugar seguro. Si utiliza Authy o Duo, ambas aplicaciones tienen funciones de copia de seguridad integradas con una fuerte configuración de seguridad que puede habilitar. Si elige cualquiera de esas aplicaciones, puede configurar esas opciones de copia de seguridad en caso de avería, pérdida o robo del dispositivo. Vea las instrucciones de Authy **aquí**, y las de Duo **aquí**. Asegúrese de que todos los miembros de su organización conozcan estos pasos cuando empiecen a activar la 2FA en todas sus cuentas.



2FA en Toda la Organización

Si su organización proporciona cuentas de correo electrónico a todo el personal a través de Google Workspace (antes conocido como GSuite) o Microsoft 365 utilizando su propio dominio (por ejemplo, @ndi.org), puede implementar la 2FA y una configuración de seguridad fuerte para todas las cuentas. Esta aplicación no solo ayuda a proteger estas cuentas, sino que también actúa como una forma de introducir y normalizar la 2FA con su personal para que se sientan más cómodos adoptándola también para las cuentas personales. Como administrador de Google Workspace, puede seguir **estas instrucciones** para aplicar la 2FA a su dominio. Puede hacer algo similar en Microsoft 365 siguiendo **estos pasos** como administrador del dominio.

Considere también la posibilidad de inscribir las cuentas de su organización en el **Programa de Protección Avanzada** (Google) o **AccountGuard** (Microsoft) para implementar controles de seguridad adicionales y exigir llaves de seguridad física para la autenticación de dos factores.



Cuentas Seguras

- **Exija contraseñas seguras para todas las cuentas de la organización; fomente lo mismo para las cuentas personales del personal y los voluntarios.**
- **Implemente un administrador de contraseñas de confianza para la organización (y fomente su uso también en la vida personal del personal).**
  - Exija una contraseña principal fuerte y la 2FA para todas las cuentas del administrador de contraseñas.
  - Recuérdeles a todos que deben cerrar la sesión de un administrador de contraseñas en los dispositivos compartidos o cuando corran un mayor riesgo de robo o confiscación del dispositivo.
- **Cambie las contraseñas compartidas cuando el personal se desvincula de la organización.**
- **Comparta únicamente las contraseñas de forma segura, por ejemplo, a través del administrador de contraseñas de su organización o de aplicaciones cifradas de extremo a extremo.**
- **Exija la 2FA en todas las cuentas de la organización, y aliente al personal a establecer la 2FA en todas las cuentas personales, también.**
  - Si es posible, proporcione llaves de seguridad física a todo el personal.
  - Si las llaves de seguridad no entran en su presupuesto, fomente el uso de aplicaciones de autenticación en lugar de SMS o llamadas telefónicas para la 2FA.
- **Imparta capacitación periódica para garantizar que el personal conozca las mejores prácticas en materia de contraseñas y 2FA, incluido qué hace que una contraseña sea sólida y la importancia de no reutilizar nunca las contraseñas, de aceptar únicamente solicitudes legítimas de 2FA y de generar códigos de 2FA de copia de seguridad.**

Dispositivos Seguros

Además de las cuentas, es esencial mantener todos los dispositivos – computadoras, teléfonos, USB, discos duros externos, etc.– bien protegidos.

Esta protección empieza por tener cuidado con el tipo de dispositivos que su organización y su personal compran y utilizan. Los proveedores o fabricantes que elija deben tener un historial demostrado de cumplimiento de las normas mundiales relativas al desarrollo seguro de dispositivos de hardware (como teléfonos y computadoras). Todos los dispositivos que adquiera deben ser fabricados por empresas de confianza que no tengan incentivos para entregar datos e información a un adversario potencial. Es importante señalar que el gobierno chino exige a las empresas chinas que proporcionen datos al gobierno central. Así que, a pesar de la presencia omnipresente y barata de teléfonos inteligentes como Huawei o ZTE, deberían evitarse. Aunque el costo de un equipo barato puede ser muy atractivo para una organización, debido a los posibles riesgos de seguridad para las organizaciones que defienden la democracia, los derechos humanos o la rendición de cuentas, deberían orientarse hacia otras opciones de dispositivos, ya que este acceso a los datos ha contribuido a facilitar la persecución de determinadas personas y comunidades por parte del gobierno chino y otros gobiernos. Sus adversarios pueden comprometer la seguridad de sus dispositivos (y todo lo que usted hace desde esos dispositivos) obteniendo acceso físico o "remoto" a su dispositivo.

Seguridad de los Dispositivos y la Sociedad Civil

Algunos de los programas maliciosos más avanzados del mundo se han desarrollado y desplegado en todo el planeta para atacar a las organizaciones de la sociedad civil y a los defensores de los derechos humanos. En India, por ejemplo, Amnistía Internacional informó que al menos nueve defensores de los derechos humanos fueron objeto en 2020 de spyware (un tipo de software malicioso) en sus dispositivos móviles y computadoras. El spyware se distribuyó a través de una serie de correos electrónicos de phishing con enlaces a archivos infectados compartidos a través de Firefox Send (un programa de intercambio de archivos suspendido). En el caso de los objetivos que abrieron los archivos, sus dispositivos se infectaron con un software que grababa el audio, interceptaba las pulsaciones del teclado y los mensajes y, de hecho, los ponía bajo la total vigilancia de los atacantes. Este tipo de ataques, que con frecuencia se dirigen a grupos de la sociedad civil y a su personal individual, son una forma desgraciadamente común de que los atacantes obtengan acceso "remoto" a un dispositivo.



ACCESO AL DISPOSITIVO FÍSICO POR PÉRDIDA O ROBO

Para evitar un compromiso físico, es esencial mantener sus dispositivos físicamente seguros. En resumen, no facilite que un adversario le robe o incluso le quite temporalmente su dispositivo. Mantenga los dispositivos bajo llave si los deja en casa o en la oficina. O si considera que es más seguro, llévelos consigo. Por supuesto, esto significa que parte de la seguridad de los dispositivos es la seguridad física de sus espacios de trabajo (ya sea en un entorno de oficina o en casa). Es posible que tenga que instalar cerraduras sólidas, cámaras de seguridad u otros sistemas de vigilancia, especialmente si su organización corre un alto riesgo. Recuerde al personal que debe tratar los dispositivos de la misma manera que trataría una gran cantidad de dinero en efectivo: no los deje tirados, desatendidos o desprotegidos.

¿Qué pasa si me roban un dispositivo?

Para limitar el impacto si alguien consigue robar un dispositivo (o si solo acceden a él durante un breve período de tiempo), asegúrese de **imponer el uso de contraseñas o códigos de acceso en las computadoras y teléfonos de todos**. Los mismos consejos sobre contraseñas de la sección Contraseñas de este Manual se aplican a una buena contraseña para una computadora de escritorio o portátil. A la hora de bloquear el teléfono, utilice códigos de al menos seis u ocho dígitos y evite utilizar "patrones de deslizamiento" para desbloquear la pantalla. Para obtener más consejos sobre los bloqueos de pantalla, consulte el Data Detox Kit de Tactical Tech. El uso de buenas contraseñas para los dispositivos hace mucho más difícil que un adversario pueda acceder rápidamente a la información de su dispositivo en caso de robo o confiscación. Con un código de acceso seguro, activar el Face ID o el desbloqueo por huella dactilar puede estar bien, pero asegúrese de desactivarlo (dejando habilitado su código de acceso seguro) antes de cualquier actividad de alto riesgo, como protestas o cruces de fronteras, si usted y su personal están preocupados por la confiscación del dispositivo por parte de las autoridades. Si alguno de los dispositivos entregados por la organización tiene una función "Find my Device" (Encontrar mi dispositivo), como Find My iPhone de iPhone y Find My Device de Android, considere la posibilidad de exigir al personal que la active. Anime al personal a utilizar estas funciones también en sus dispositivos personales. Con estas funciones activadas, el propietario del dispositivo (o un contacto de confianza) puede localizarlo o borrar a distancia su contenido en caso de robo, pérdida o confiscación. En el caso de los teléfonos iPhone, también puede configurar el dispositivo para borrar automáticamente después de varios intentos fallidos de inicio de sesión. Estas funciones de gestión de dispositivos adquieren una importancia fundamental para una organización cuando un dispositivo con información sensible se pierde o cae en manos equivocadas.

¿Y el cifrado de los dispositivos?

Es importante utilizar el cifrado, codificando los datos para que sean ilegibles e inutilizables, en todos los dispositivos, especialmente en computadoras y teléfonos inteligentes. Si es posible, debería configurar todos los dispositivos de su organización con algo llamado cifrado de disco. El cifrado de disco significa que la totalidad de un dispositivo está cifrada, de modo que un adversario, si lo robara físicamente, no podría extraer el contenido del dispositivo sin conocer la contraseña o la clave que se utilizó para cifrarlo. Muchos teléfonos inteligentes y computadoras ofrecen cifrados de disco. Los dispositivos de Apple, como los iPhone y los iPads, activan convenientemente el cifrado de disco cuando se establece un código de acceso normal del dispositivo. Las computadoras Apple que utilizan macOS ofrecen una función llamada FileVault que usted puede activar para el cifrado de disco. Las computadoras Windows con licencias Pro, Enterprise o Education ofrecen una función llamada BitLocker que puede activar para el cifrado de todo el disco. Puede activar BitLocker siguiendo estas instrucciones de Microsoft; probablemente tenga que ser activado primero por el administrador de su organización. Si el personal solo tiene una licencia doméstica para sus computadoras Windows, BitLocker no está disponible. Sin embargo, aún pueden activar el cifrado de disco completo yendo a "Update & Security" (Actualización y seguridad) > "Device encryption" (Cifrado de dispositivos) en la configuración del sistema operativo Windows.

Los dispositivos Android, a partir de la versión 9.0, vienen con el cifrado de archivos activado de manera predeterminada. El cifrado basado en archivos de Android funciona de forma diferente al cifrado de disco, pero sigue proporcionando una gran seguridad. Si utiliza un teléfono Android relativamente nuevo y ha establecido un código de acceso, el cifrado basado en archivos debería estar activado. Sin embargo, es una buena idea comprobar la configuración para estar seguro, especialmente si el teléfono tiene más de un par de años. Para comprobarlo, vaya a "Settings" > "Security" (Ajustes > Seguridad) en su dispositivo Android. Dentro de la configuración de seguridad, debería ver una subsección de "cifrado" o "cifrado y credenciales", que le indicará si su teléfono está cifrado y, si no, le permitirá activar el cifrado.

En el caso de las computadores (ya sean Windows o Mac), es especialmente importante guardar las claves de cifrado (denominadas claves de recuperación) en un lugar seguro. En la mayoría de los casos, estas "claves de recuperación" son esencialmente contraseñas largas o frases de contraseña. En caso de que olvide la contraseña normal de su dispositivo o de que ocurra algo inesperado (como una falla del dispositivo), las claves de recuperación son la única forma de recuperar sus datos cifrados y, si es necesario, trasladarlos a un nuevo dispositivo. Así que cuando active el cifrado de disco, asegúrese de guardar estas claves o contraseñas en un lugar seguro, como una cuenta segura en la nube o el administrador de contraseñas de su organización.

ACCESO REMOTO A DISPOSITIVOS, TAMBIÉN CONOCIDO COMO PIRATERÍA

Además de mantener los dispositivos físicamente seguros, es importante mantenerlos libres de malware. La publicación Security-in-a-Box de Tactical Tech ofrece una descripción útil de lo que es el malware y por qué es importante evitarlo, lo que se adapta ligeramente en el resto de esta sección.

Entender y evitar el malware

Hay muchas maneras de clasificar el malware (que es un término que significa software malicioso). Los virus, el spyware, los gusanos, los troyanos, los rootkits, el ransomware y los cryptojackers son todos tipos de malware. Algunos tipos de malware se propagan por internet a través del correo electrónico, los mensajes de texto, las páginas web maliciosas y otros medios. Algunos se propagan a través de dispositivos como las memorias USB que se utilizan para intercambiar y robar datos. Y, mientras que algunos tipos de malware requieren que un objetivo desprevenido cometa un error, otros pueden infectar silenciosamente los sistemas vulnerables sin que usted haga nada malo.

Además del malware general (que se libera ampliamente y está dirigido al público en general), el malware selectivo suele utilizarse para interferir o espiar a una persona, organización o red en particular. Los delincuentes habituales utilizan estas técnicas, pero también lo hacen los servicios militares y de inteligencia, los terroristas, los acosadores en línea, los cónyuges maltratadores y los actores políticos sospechosos.

Se llamen como se llamen y se distribuyan como se distribuyan, los programas maliciosos pueden arruinar las computadoras, robar y destruir datos, llevar a las organizaciones a la bancarrota, invadir la privacidad y poner en peligro a los usuarios. En resumen, el malware es realmente peligroso. Sin embargo, hay algunas medidas sencillas que su organización puede tomar para protegerse contra esta amenaza común.

¿Nos protegerá una herramienta contra el malware?

Lamentablemente, las herramientas contra el malware no son una solución completa. Pero es una muy buena idea utilizar algunas herramientas básicas y gratuitas como base. Con nuevos riesgos en el mundo real con tanta frecuencia, el malware cambia tan rápido que confiar en cualquier herramienta de este tipo no puede ser su única defensa.

Si utiliza Windows, debería echar un vistazo al Windows Defender incorporado. Las computadoras Mac y Linux no llevan incorporado un software contra el malware, ni tampoco los dispositivos Android e iOS. Puede instalar una herramienta de confianza y de uso gratuito como Bitdefender o Malwarebytes para esos dispositivos (y también para las computadoras con Windows). **Pero no confíe en eso como su única línea de defensa**, ya que seguramente no resistirán algunos de los nuevos ataques más específicos y peligrosos.

Además, tenga mucho cuidado de descargar únicamente herramientas contra malware o antivirus de buena reputación de fuentes legítimas (como los sitios web con enlaces mencionados anteriormente). Por desgracia, existen muchas versiones falsas o comprometidas de herramientas contra malware que hacen mucho más daño que bien.

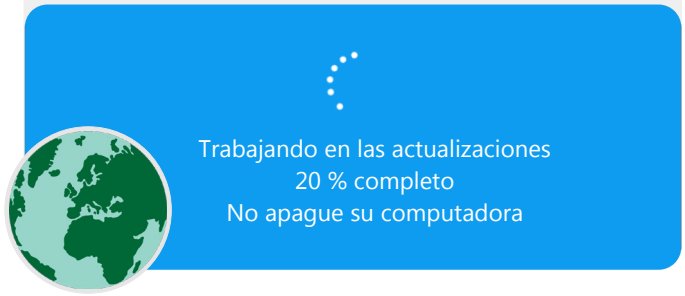
Si utiliza Bitdefender u otra herramienta contra malware en su organización, asegúrese de no ejecutar dos de ellas al mismo tiempo. Muchas de ellas identificarán el comportamiento de otro programa contra el malware como sospechoso y detendrán su ejecución, dejando a ambos en mal funcionamiento. Bitdefender u otros programas contra el malware de buena reputación pueden actualizarse gratuitamente, y el Windows Defender incorporado recibe actualizaciones junto con su computadora. Asegúrese de que su software contra malware se actualice con regularidad (algunas versiones de prueba del software comercial que se entrega con la compra de una computadora se desactivan después de que expira el período de prueba, volviendo al software más peligroso que útil). Cada día se escriben y distribuyen nuevos programas de malware, y su computadora se volverá rápidamente más vulnerable si no se mantiene al día con las nuevas definiciones de malware y las técnicas contra el malware. Si es posible, debería configurar su software para que instale las actualizaciones automáticamente. Si su herramienta contra malware tiene una función opcional "siempre activa", debería activarla y considerar la posibilidad de escanear ocasionalmente todos los archivos de su computadora.

Mantener los dispositivos actualizados

Las actualizaciones son esenciales. Utilice la última versión de cualquier sistema operativo que se ejecute en un dispositivo (Windows, Mac, Android, iOS, etc.), y mantenga ese sistema operativo actualizado. Mantenga también actualizado el resto del software, el navegador y los complementos del mismo. Instale las actualizaciones tan pronto como estén disponibles, idealmente activando las actualizaciones automáticas. Cuanto más actualizado esté el sistema operativo de un dispositivo, menos vulnerabilidades tendrá. Piense en las actualizaciones como si pusiera un apósito sobre un corte abierto. Sella una vulnerabilidad y reduce en gran medida la posibilidad de que su computadora se infecte. Desinstale también el software que ya no utilice. El software obsoleto suele tener problemas de seguridad, y es posible que haya instalado una herramienta que ya no es actualizada por el desarrollador, lo que la hace más vulnerable a los hackers.

El Malware en el Mundo Real: Las Actualizaciones son Esenciales

En 2017, los ataques de ransomware WannaCry infectaron millones de dispositivos en todo el mundo, dejando fuera de servicio hospitales, entidades gubernamentales, organizaciones grandes y pequeñas y empresas en decenas de países. ¿Por qué fue tan efectivo el ataque? Debido a los sistemas operativos Windows desactualizados y "sin parches", muchos de los cuales fueron inicialmente pirateados. Gran parte de los daños (humanos y financieros) podrían haberse evitado con mejores prácticas de actualización automatizada y el uso de sistemas operativos legítimos.



Cuidado con los USB

Tenga cuidado al abrir los archivos que le envíen como adjuntos, a través de enlaces de descarga o por cualquier otro medio. Además, piénselo dos veces antes de insertar en su computadora elementos extraíbles, como memorias USB, tarjetas de memoria flash, DVD y CD, ya que pueden ser un vector de malware. Los dispositivos USB que han sido compartidos durante un tiempo son muy propensos a tener virus. Para conocer opciones alternativas para compartir archivos de forma segura en toda la organización, eche un vistazo a la sección de intercambio de archivos del Manual.

Tenga también cuidado con los dispositivos que conecta a través de Bluetooth. Está bien sincronizar el teléfono o la computadora con un altavoz Bluetooth conocido y de confianza para reproducir su música favorita, pero tenga cuidado con vincular o aceptar solicitudes de cualquier dispositivo que no reconozca. Permita solo las conexiones con dispositivos de confianza y recuerde apagar Bluetooth cuando no esté en uso.

Sea inteligente mientras navega

Nunca acepte ni ejecute aplicaciones que provengan de sitios web que no conozca y en los que no confíe. En lugar de aceptar una "actualización" ofrecida en una ventana emergente del navegador, por ejemplo, compruebe si hay actualizaciones en el sitio web oficial de la aplicación correspondiente. Tal y como se comenta en la sección sobre phishing del Manual, es esencial mantenerse alerta cuando se navega por sitios web. Compruebe el destino de un enlace (pasando el mouse por encima) antes de hacer clic, eche un vistazo a la dirección del sitio web después de seguir un enlace y asegúrese de que parezca adecuada antes de introducir información sensible, como su contraseña. No haga clic en los mensajes de error o las advertencias, esté atento a las ventanas del navegador que aparezcan automáticamente y léalas detenidamente en lugar de limitarse a hacer clic en Sí o en Aceptar.

¿Qué sucede con los teléfonos inteligentes?

Al igual que en el caso de las computadoras, mantenga actualizados el sistema operativo y las aplicaciones de su teléfono, y active las actualizaciones automáticas. Realice instalaciones solo desde fuentes oficiales o de confianza, como la Play Store de Google y la App Store de Apple (o F-droid, una tienda de aplicaciones gratuita y de código abierto para Android). Las aplicaciones pueden tener malware insertado y seguir pareciendo que funcionan con normalidad, por lo que no siempre sabrá si una es maliciosa. Asegúrese también de que está descargando la versión legítima de una aplicación. Especialmente en los Android, existen versiones "fake"o falsas de aplicaciones populares. Así que asegúrese de que una aplicación esté creada por la empresa o el desarrollador adecuados, tenga buenas críticas y tenga el número de descargas esperado (por ejemplo, una versión falsa de WhatsApp podría tener solo unas cuantas miles de descargas, pero la versión real tiene más de 5,000 millones). Preste atención a los permisos que solicitan sus aplicaciones. Si parecen excesivas (como una calculadora que pide acceso a su cámara o Angry Birds que pide acceso a su ubicación, por ejemplo), niegue la petición o desinstale la aplicación. Desinstalar las aplicaciones que ya no use también puede ayudar a proteger su teléfono inteligente o tableta. Los desarrolladores a veces venden la propiedad de sus aplicaciones a otras personas. Estos nuevos propietarios pueden intentar ganar dinero añadiendo código malicioso.

El Malware en el Mundo Real: Aplicaciones Móviles Maliciosas

Durante años, los hackers de múltiples países han estado utilizando aplicaciones falsas en la tienda Google Play para distribuir malware. Un caso concreto dirigido a usuarios de Vietnam salió a la luz en abril de 2020. Esta campaña de espionaje utilizaba aplicaciones falsas, que supuestamente ayudaban a los usuarios a encontrar pubs cercanos o a buscar información sobre las iglesias locales. Una vez instaladas por los usuarios involuntarios de Android, las aplicaciones maliciosas recopilaban registros de llamadas, datos de localización e información sobre contactos y mensajes de texto. Esta es solo una de las muchas razones para tener cuidado con las aplicaciones que se descargan en los dispositivos.



Ahorre dinero y aumente la seguridad de los dispositivos con Tails para su organización

Una opción muy segura, pero que requiere un poco de habilidad técnica para configurarla, es el sistema operativo Tails. Este sistema operativo portátil es de uso gratuito y puede activarse directamente desde un dispositivo USB, evitando la necesidad de depender de sistemas operativos con licencia de Windows o Mac. Tails también es una buena opción para aquellos que corren un riesgo extremadamente alto, ya que incorpora una amplia gama de funciones que mejoran la privacidad. Estas funciones incluyen la integración de Tor (de la que hablaremos más adelante) para asegurar su tráfico web, y el borrado completo de la memoria cada vez que apaga el sistema operativo. Estas funciones le permiten esencialmente comenzar con un estado original cada vez que reinicie su computadora. Tails también tiene un "modo de persistencia", que permite guardar archivos y configuraciones importantes en varias sesiones, si lo desea.

Otra opción para un sistema operativo gratuito y seguro es Qubes OS. Aunque no es la opción más sencilla para los usuarios no técnicos, Qubes está diseñado para limitar la amenaza del malware y es otra opción a tener en cuenta para los usuarios más avanzados y con alto riesgo de su organización, especialmente si los costos de las licencias son un desafío.

¿Y si no podemos costear un software legal?

Puede resultar caro comprar versiones con licencia de programas populares como Microsoft Office (Word, PowerPoint, Excel) para toda la organización, pero un presupuesto limitado no es excusa para descargar versiones piratas de software o no mantenerlas actualizadas. No se trata de una cuestión de moral, sino de seguridad. El software pirata suele estar repleto de malware y, a menudo, no se pueden cubrir con parches las vulnerabilidades de seguridad. Si no puede hacer frente al software que necesita su organización, existe una amplia gama de programas gratuitos de código abierto, como **LibreOffice** (un sustituto de las aplicaciones estándar de Microsoft Office) o **GIMP** (un sustituto de Photoshop), que pueden satisfacer sus necesidades. Considere también la posibilidad de registrarse a través de **Tech Soup**, una organización que ofrece grandes descuentos en software popular para organizaciones sin fines de lucro. Incluso si puede adquirir software y aplicaciones legítimos, su dispositivo sigue estando en peligro si el sistema operativo subyacente no es legítimo.

Así que si su organización no puede adquirir licencias de Windows, considere alternativas más baratas como los Chromebooks, que son una opción excelente y fácil de proteger si su organización trabaja principalmente en la nube. Si utiliza Google Docs o Microsoft 365, no necesita muchas aplicaciones de escritorio: los editores gratuitos de documentos y planillas de cálculo en el navegador son más que suficientes para casi cualquier uso. Si tiene personal con conocimientos técnicos, otra opción es instalar en cada computadora un sistema operativo gratuito basado en Linux (una alternativa de código abierto a los sistemas operativos Windows y Mac). Una opción de Linux popular y bastante fácil de usar es **Ubuntu**. Independientemente del sistema operativo que elija, asegúrese de que alguien en la organización sea responsable de comprobar regularmente con el personal que han aplicado las últimas actualizaciones.

Cuando está tomando una decisión sobre una nueva herramienta o sistema, considere cómo su organización puede respaldarlo técnicamente y financieramente a largo plazo. Hágase preguntas como: ¿Puede pagar y retener al personal necesario para mantenerlo de manera segura? ¿Se pueden pagar suscripciones recurrentes? ¿Tienes acceso a descuentos de grupos como el mencionado TechSoup? Responder a estas preguntas puede ayudar a garantizar que sus estrategias de software y tecnología sean más exitosas con el tiempo.



Mantener la Seguridad de los Dispositivos

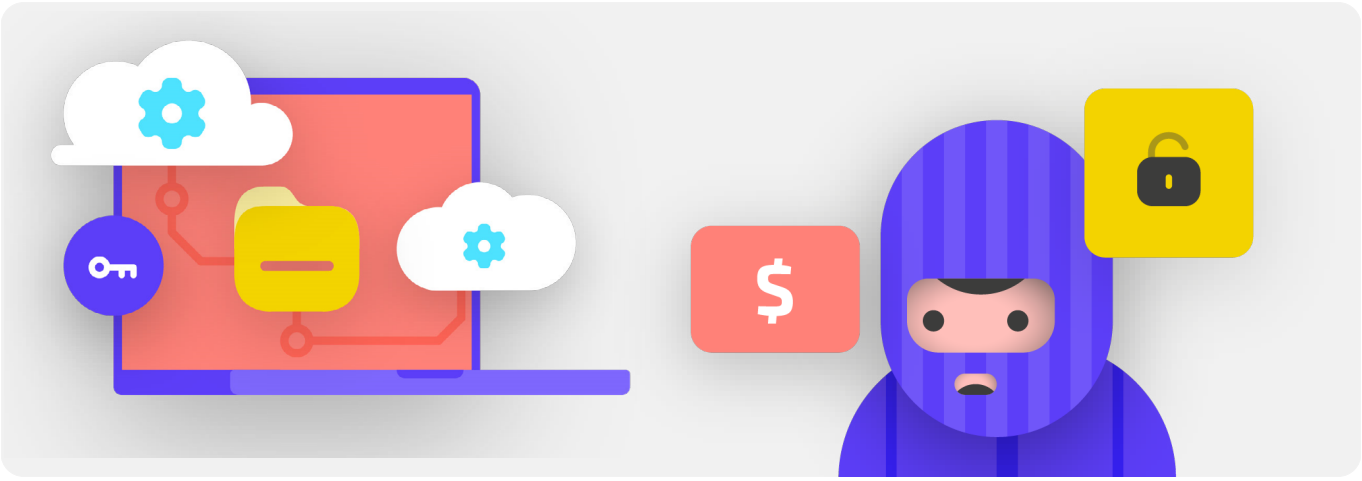
- **Capacite al personal sobre los riesgos del malware y las mejores prácticas para evitarlo.**
  - Proporcione políticas sobre la conexión de dispositivos externos, el cliqueo de enlaces, la descarga de archivos y aplicaciones, y la comprobación de los permisos de software y aplicaciones.
- **Ordene que los dispositivos, el software y las aplicaciones se mantengan totalmente actualizados.**
  - Active las actualizaciones automáticas siempre que sea posible.
- **Asegúrese de que todos los dispositivos utilicen software con licencia. Si el costo es prohibitivo, cambie a una alternativa gratuita.**
- **Exija la protección con contraseña de todos los dispositivos de la organización, incluidos los dispositivos móviles personales que se utilizan para las comunicaciones relacionadas con el trabajo.**
- **Habilite el cifrado de disco completo en los dispositivos.**
- **Recuerde con frecuencia al personal que mantenga sus dispositivos físicamente seguros, y gestione la seguridad de su oficina con cerraduras adecuadas y formas de proteger las computadoras.**
- **No comparta archivos utilizando dispositivos USB ni conecte dispositivos USB a sus computadoras.**
  - Utilice opciones alternativas para compartir archivos de forma segura.

Suplantación de Identidad: Una Amenaza Común para los Dispositivos y las Cuentas

El phishing o suplantación de identidad es el ataque más común y eficaz contra las organizaciones de todo el mundo. Esta técnica es utilizada por los más sofisticados ejércitos de los estados-nación, así como por los estafadores de poca monta.

En términos sencillos, la suplantación de identidad consiste en que un adversario intenta engañarle para que comparta información que podría utilizarse contra usted o su organización. La suplantación de identidad puede producirse a través de correos electrónicos, mensajes de texto/SMS (a menudo denominado phishing por SMS o "smishing"), aplicaciones de mensajería como WhatsApp, mensajes o publicaciones en redes sociales, o llamadas telefónicas (a menudo denominado phishing por voz o "vishing"). Los mensajes de phishing pueden intentar que escriba información sensible (como contraseñas) en un sitio web falso para obtener acceso a una cuenta, pedirle que comparta información privada

(como el número de una tarjeta de crédito) a través de voz o de un mensaje de texto, o convencerlo de que descargue malware (software malicioso) que puede infectar su dispositivo. Para poner un ejemplo no técnico, cada día millones de personas reciben llamadas telefónicas automatizadas falsas en las que se les informa que su cuenta bancaria ha quedado comprometida o que su identidad ha sido robada, todo ello con el fin de engañar a los desprevenidos para que compartan información sensible.



¿CÓMO PODEMOS IDENTIFICAR LA SUPLANTACIÓN DE IDENTIDAD?

La suplantación de identidad puede parecer siniestra e imposible de atrapar, pero hay algunas medidas sencillas que todos los miembros de su organización pueden tomar para protegerse contra la mayoría de los ataques. Los siguientes consejos de defensa contra la suplantación de identidad se han modificado y ampliado a partir de la guía de phishing en profundidad elaborada por The Freedom of the Press Foundation, y deben compartirse en su organización (y otros contactos) e integrarse en su plan de seguridad:

A veces, el campo "de" le miente

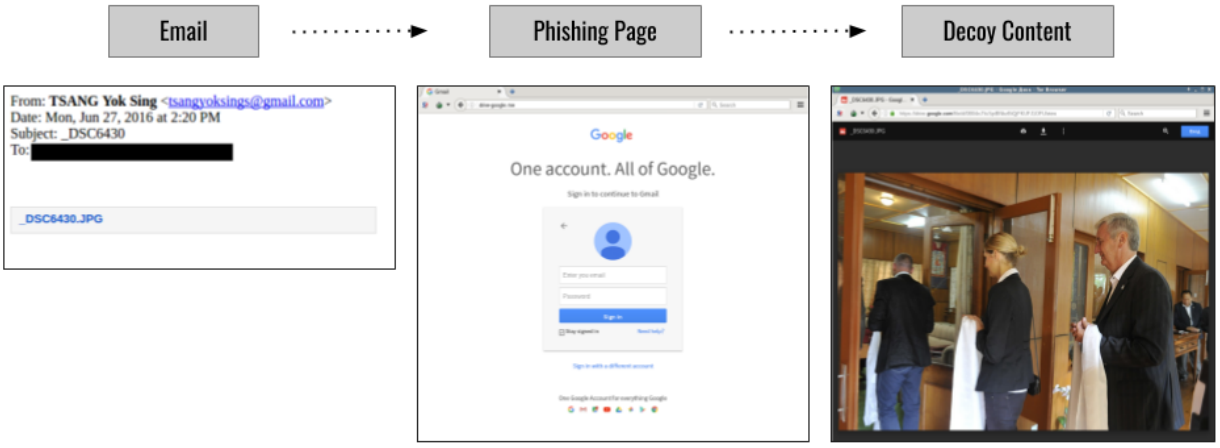
Tenga en cuenta que el campo "de" en sus correos electrónicos puede ser falsificado o manipulado para engañarle. Es habitual que los suplantadores de identidad creen una dirección de correo electrónico que se parece mucho a una legítima con la que usted está familiarizado, pero con un pequeño error ortográfico para engañarle. Por ejemplo, puede recibir un correo electrónico de alguien con la dirección "john@ gooogle.com" en lugar de "john@google.com". Fíjese en la "O" extra en Google. También es posible que conozca a alguien con una dirección de correo electrónico "john@gmail.com", pero que reciba un correo electrónico de phishing de un suplantador que haya creado "johm@gmail.com", con la única diferencia de un sutil cambio de letras al final. Asegúrese siempre de comprobar que conoce la dirección de envío de un correo electrónico antes de continuar. Un concepto similar se aplica al phishing a través de mensajes de texto, llamadas o aplicaciones de mensajería. Si recibe un mensaje de un número desconocido, piénselo dos veces antes de responder o interactuar con el mensaje.



Suplantación de Identidad y Sociedad Civil

Los sofisticados ataques de phishing personalizados se dirigen cada día a grupos de la sociedad civil de todo el mundo.

Un ejemplo de este tipo de ataque se destaca en el informe de 2018 de The Citizen Lab, Spying on a Budget: Inside a Phishing Operation with Targets in the Tibetan Community (Espionaje con presupuesto: dentro de una operación de suplantación de identidad con objetivos de la comunidad tibetana). Este ataque de phishing, muy barato y sencillo, pero increíblemente eficaz, estaba dirigido a los defensores de los derechos humanos del Tíbet y a otros activistas. El ataque comenzó con un correo electrónico de phishing (a la izquierda) desde una dirección estándar de Gmail que solo contenía un enlace a un archivo de imagen. Al hacer clic, el enlace llevaba al objetivo a una página falsa de acceso al correo electrónico de Google (en el centro) que se utilizaba para robar las credenciales de la cuenta. Si las víctimas proporcionaban credenciales a la página falsa, sus cuentas se verían fácilmente comprometidas. Tras proporcionar su nombre de usuario y contraseña en el sitio falso, las víctimas eran redirigidas a una imagen (a la derecha) que muestra a los delegados en una reunión tibetana. La imagen se incluyó como señuelo para hacer creer a los objetivos de la suplantación de identidad que realmente habían iniciado sesión en su cuenta real de Google y reducir cualquier posible sospecha sobre la verdadera naturaleza maliciosa del correo electrónico.



Cuidado con los Archivos Adjuntos

Los archivos adjuntos pueden llevar malware y virus, y suelen acompañar a los correos electrónicos de suplantación de identidad. **La mejor manera de evitar el malware de los archivos adjuntos es no descargarlos nunca**. Como norma, no abra inmediatamente ningún archivo adjunto, especialmente si procede de personas que no conoce. Si es posible, pida a la persona que le ha enviado el documento que copie y pegue el texto en un correo electrónico o que comparta el documento a través de un servicio como Google Drive o Microsoft OneDrive, que llevan incorporado el escaneo de virus de la mayoría de los documentos subidos a sus plataformas. Construya una cultura organizativa en la que se desaconsejen los archivos adjuntos. Si es absolutamente necesario abrir el archivo adjunto, solo debería abrirse en un entorno seguro (vea la sección Avanzado más adelante), donde no pueda implementarse un potencial malware en su dispositivo.

Si utiliza Gmail y recibe un archivo adjunto en un correo electrónico, en lugar de descargarlo y abrirlo en su computadora, simplemente haga clic en el archivo adjunto y léalo en "vista previa" dentro de su navegador. Este paso le permite ver el texto y el contenido de un archivo sin descargarlo ni permitir que cargue posible malware en su computadora. Esto funciona bien para los documentos de texto, pdf e incluso presentaciones de diapositivas. Si necesita editar el documento, considere la posibilidad de abrir el archivo en un programa en la nube, como Google Drive, y convertirlo en un Google Doc o Google Slides.

Si utiliza Outlook, también puede previsualizar los archivos adjuntos sin necesidad de descargarlos desde el cliente web de Outlook. Si necesita editar el archivo adjunto, considere la posibilidad de abrirlo en OneDrive, si está disponible. Si utiliza Yahoo Mail, se aplica el mismo concepto. No descargue los archivos adjuntos, previsualícelos desde el navegador web.

Independientemente de las herramientas que tenga a su disposición, lo mejor es simplemente no descargar nunca archivos adjuntos que no conozca o en los que no confíe. E independientemente de lo importante que pueda parecer un archivo adjunto, nunca abra algo con un tipo de archivo que no reconozca o que no tenga intención de utilizar nunca.



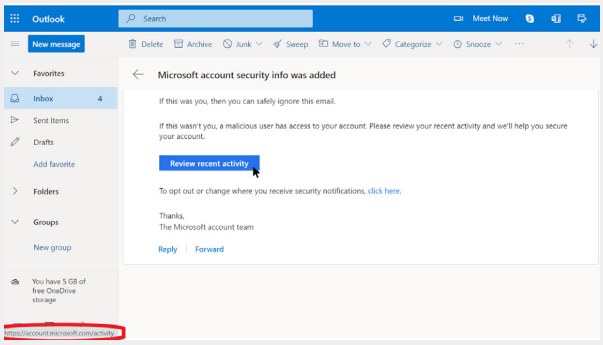
Defensa contra la Suplantación de Identidad para su Organización

Si su organización utiliza Microsoft 365 empresarial para el correo electrónico y otras aplicaciones, el administrador del dominio debe configurar la política de Archivos Adjuntos Seguros para protegerse de los archivos adjuntos peligrosos. Si se utiliza el Google Workspace para empresas (antes conocido como GSuite), existe una opción igualmente eficaz que el administrador debe configurar, denominada Google Security Sandbox. Los usuarios individuales más avanzados pueden considerar la configuración de sofisticados programas de Sandbox, como DangerZone o, para aquellos con la versión Pro o Enterprise de Windows 10, Windows Sandbox. Otra opción avanzada que debe considerar implementar en su organización es un servicio de filtrado seguro del sistema de nombres de dominio (DNS, por sus siglas en inglés). Las organizaciones pueden utilizar esta tecnología para bloquear al personal y evitar que acceda o interactúe accidentalmente con contenidos maliciosos, proporcionando una capa adicional de protección contra la suplantación de identidad. Aunque históricamente dicha tecnología requería un equipo exclusivo de personal informático interno, los nuevos servicios como Gateway de Cloudflare proporcionan dichas capacidades a organizaciones menos sofisticadas técnicamente, sin requerir grandes sumas de dinero (Gateway, por ejemplo, es gratuito para hasta 50 usuarios). Otras herramientas gratuitas, como Quad9 del Global Cyber Alliance Toolkit, le ayudarán a bloquear el acceso a sitios conocidos que tienen virus u otros programas maliciosos y pueden implementarse en menos de cinco minutos.

Haga clic con precaución

No se fíe de los enlaces que aparecen en los correos electrónicos u otros mensajes de texto. Los enlaces pueden estar disfrazados para descargar archivos maliciosos o llevarlo a sitios falsos que pueden pedirle que proporcione contraseñas u otra información confidencial. En una computadora, hay un sencillo truco para asegurarse de que un enlace en un correo electrónico o un mensaje lo enviará adonde se supone que debe hacerlo: utilice el mouse para pasar por encima de cualquier enlace antes de hacer clic en él, y mire en la parte inferior de la ventana del navegador para ver cuál es la URL real (vea la imagen siguiente).

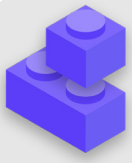
Es más difícil comprobar los enlaces de un correo electrónico en un dispositivo móvil sin hacer clic accidentalmente en ellos, así que tenga cuidado. Pero puede comprobar el destino de un enlace en la mayoría de los teléfonos inteligentes pulsando prolongadamente (manteniéndolo pulsado) sobre un enlace hasta que aparezca la URL completa. En la suplantación de identidad a través de SMS y aplicaciones de mensajería, los enlaces acortados son una práctica muy común utilizada para disfrazar el destino de una URL. Si ve un enlace corto (como bit.ly o tinyurl.com, por ejemplo) en lugar de la URL completa, no haga clic en él. Si el enlace es importante, cópielo en un expansor de URL, como https://www.expandurl.net/, para ver el destino real de una URL acortada. Además, no haga clic en enlaces a sitios web con los que no esté familiarizado. En caso de duda, realice una búsqueda del sitio, con el nombre del sitio entre comillas (por ejemplo: "www.badwebsite.com") para ver si es un sitio web legítimo. También puede verificar enlaces potencialmente sospechosos a través del escáner de las URL de VirusTotal. Esto no es 100 % exacto, pero es una buena precaución.



Por último, si hace clic en algún enlace de un mensaje y se le pide que inicie sesión en algo, no lo haga, a menos que esté 100 % seguro de que el correo electrónico es legítimo y lo está enviando al sitio apropiado. Muchos ataques de suplantación de identidad proporcionan enlaces que lo envían a páginas de inicio de sesión falsas para Gmail, Facebook u otros sitios populares. No caiga en la trampa. Siempre puede abrir un nuevo navegador e ir directamente a un sitio conocido, como Gmail.com, Facebook.com, etc. si quiere o necesita iniciar sesión. Eso también lo llevará al contenido de forma segura, si era legítimo en primer lugar.

¿Qué debemos hacer cuando recibimos un mensaje de phishing?

Si alguien en su organización recibe un archivo adjunto no solicitado, un enlace, una imagen, o un mensaje o una llamada sospechosos, es importante que lo comunique inmediatamente al responsable de seguridad informática de su organización. Si aún no cuenta con esta persona, debe identificarla como parte del desarrollo de su plan de seguridad. El personal también puede denunciar el correo electrónico como spam o phishing directamente en Gmail o Outlook.
Es crucial contar con un plan sobre lo que el personal o los voluntarios deben hacer si/cuando reciben un posible mensaje de suplantación de identidad. Además, le recomendamos que adopte estas buenas prácticas de phishing: no hacer clic en enlaces sospechosos, evitar los archivos adjuntos y comprobar la dirección del remitente, y que las comparta con otras personas con las que trabaja, preferiblemente a través de un canal de comunicación muy utilizado. Esto demuestra que se preocupa por las personas con las que se comunica y fomenta una cultura en sus redes de que está alerta y es consciente de los peligros de la suplantación de identidad. Su seguridad depende de las organizaciones en las que confía, y viceversa. Las mejores prácticas protegen a todos. Además de compartir los consejos anteriores con todo el personal y los voluntarios, también puede practicar la identificación de la suplantación de identidad con el Cuestionario sobre Suplantación de Identidad de Google. También recomendamos encarecidamente que se organice una capacitación periódica sobre suplantación de identidad con el personal para comprobar el conocimiento sobre el tema y mantener a la gente alerta. Dicha capacitación puede formalizarse en el marco de las reuniones periódicas de la organización, o celebrarse de manera más informal. Lo importante es que todos los miembros de la organización se sientan cómodos haciendo preguntas sobre la suplantación de identidad, denunciando el phishing (incluso si creen que pueden haber cometido un error, como hacer clic en un enlace), y que todos estén capacitados para ayudar a defender su organización contra esta amenaza de alto impacto y alta probabilidad.



Suplantación de Identidad

- **Capacite periódicamente al personal sobre qué es la suplantación de identidad, cómo detectarla y defenderse de ella, incluido el phishing en mensajes de texto, aplicaciones de mensajería y llamadas telefónicas, no solo en el correo electrónico.**
- **Recuerde con frecuencia al personal las mejores prácticas, por ejemplo:**
  - No descargue archivos adjuntos desconocidos o potencialmente sospechosos.
  - Compruebe la URL de un enlace antes de hacer clic en ella. No haga clic en enlaces desconocidos o potencialmente sospechosos.
  - No proporcione información sensible o privada por correo electrónico, texto o llamada telefónica a direcciones o personas desconocidas o no confirmadas.
- **Fomente la denuncia del phishing.**
  - Establezca un mecanismo de notificación y un responsable de suplantación de identidad dentro de su organización.
  - Premie los informes y no castigue los fracasos.



Comunicar y almacenar los datos de manera segura

Comunicaciones e Intercambio de Datos

Para tomar las mejores decisiones en su organización sobre cómo comunicarse, es esencial entender los diferentes tipos de protección que pueden tener nuestras comunicaciones, y por qué es importante dicha protección.

Uno de los aspectos más importantes para la mayoría de las comunicaciones es mantener en secreto el contenido de los mensajes, de lo que en la era moderna se encarga en gran medida el cifrado. Sin un cifrado adecuado, las comunicaciones privadas pueden ser vistas por cualquier número de adversarios. Las comunicaciones inseguras pueden exponer información y mensajes sensibles, revelar contraseñas u otros datos privados, y posiblemente poner en riesgo a su personal y a su organización, según la naturaleza de sus comunicaciones y el contenido que comparta.

Comunicaciones Seguras y Sociedad Civil

Miles de activistas y organizaciones por la democracia y los derechos humanos confían cada día en los canales de comunicación seguros para mantener la confidencialidad de las conversaciones en entornos políticos difíciles. Sin estas prácticas de seguridad, los mensajes sensibles pueden ser interceptados y utilizados por las autoridades para atacar a los activistas y disolver las protestas. Un ejemplo destacado y bien documentado de esto ocurrió tras las elecciones de 2010 en Bielorrusia. Como se detalla en este informe de Amnistía Internacional, el gobierno interceptó grabaciones telefónicas y otras comunicaciones no codificadas y las utilizó en los tribunales contra destacados políticos y activistas de la oposición, muchos de los cuales pasaron años en prisión. En 2020, otra oleada de protestas poselectorales en Bielorrusia hizo que miles de manifestantes adoptaran aplicaciones de mensajería seguras y fáciles de usar que no estaban disponibles tan fácilmente diez años antes para proteger sus comunicaciones sensibles.



¿QUÉ ES EL CIFRADO Y POR QUÉ ES IMPORTANTE?

El cifrado es un proceso matemático que se utiliza para codificar un mensaje o un archivo de manera que solo una persona o entidad con la clave pueda "descifrarlo" y leerlo. La Guía de Autoprotección Digital contra la Vigilancia de la Electronic Frontier Foundation ofrece una explicación práctica (con gráficos) de lo que significa el cifrado:

Mensajería No Cifrada

Sin ningún tipo de cifrado, todos los que participan en la transmisión del mensaje, y cualquiera que pueda echar un vistazo a su paso, puede leer su contenido. Esto puede no importar mucho si todo lo que está diciendo es "hola", pero podría ser un gran problema si está comunicando algo más privado o sensible que no quiere que su empresa de telecomunicaciones, el ISP, un gobierno hostil o cualquier otro adversario vea. Por ello, es esencial evitar el uso de herramientas no cifradas para enviar cualquier mensaje sensible (e idealmente cualquier tipo de mensaje). Tenga en cuenta que algunos de los métodos de comunicación más populares (como los SMS y las llamadas telefónicas) prácticamente funcionan sin ningún tipo de cifrado (como en esta imagen).



Como se puede ver en la imagen de arriba, un teléfono inteligente envía un mensaje de texto verde y sin cifrar ("hola") a otro teléfono inteligente situado en el extremo derecho. En el trayecto, una torre de telefonía móvil (o en el caso de algo enviado por internet, su ISP) pasa el mensaje a los servidores de la empresa. Desde allí, salta a través de la red hasta otra torre de telefonía móvil, que puede ver el mensaje de "hola" sin cifrar, y finalmente se dirige al destino. Es importante señalar que, sin ningún tipo de cifrado, todos los que participan en la transmisión del mensaje, y cualquiera que pueda echar un vistazo a su paso, puede leer su contenido. Esto puede no importar mucho si todo lo que está diciendo es "hola", pero podría ser un gran problema si está comunicando algo más privado o sensible que no quiere que su empresa de telecomunicaciones, el ISP, un gobierno hostil o cualquier otro adversario vea. Por ello, es esencial evitar el uso de herramientas no cifradas para enviar cualquier mensaje sensible (e idealmente cualquier tipo de mensaje). Tenga en cuenta que algunos de los métodos de comunicación más populares (como los SMS y las llamadas telefónicas) prácticamente funcionan sin ningún tipo de cifrado (como en la imagen de arriba).

Hay dos formas de cifrar los datos en movimiento: el ***cifrado de la capa de transporte*** y ***el cifrado de extremo a extremo***. Para adoptar prácticas de comunicación más seguras, es importante conocer el tipo de cifrado que admite un proveedor de servicios a medida que su organización toma decisiones. Estas diferencias se describen bien en la guía de Autoprotección Digital contra la Vigilancia, que se adapta de nuevo aquí:

Cifrado en la Capa de Transporte

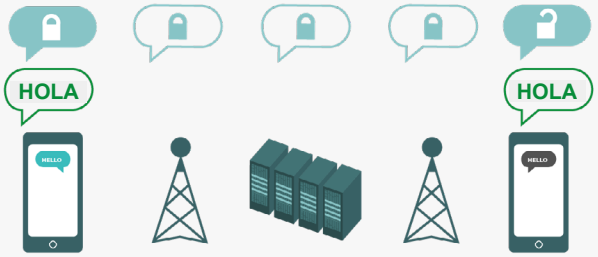
El cifrado de la capa de transporte, también conocido como seguridad de la capa de transporte (TLS, por sus siglas en inglés), protege los mensajes cuando viajan desde su dispositivo a los servidores de la aplicación/servicio de mensajería y desde allí al dispositivo de su destinatario. Esto los protege de las miradas indiscretas de los piratas informáticos que se encuentran en su red o en sus proveedores de servicios de internet o telecomunicaciones. Sin embargo, en el medio, su proveedor de servicios de mensajería/correo electrónico, el sitio web por el que navega o la aplicación que utiliza pueden ver copias no cifradas de sus mensajes. Como sus mensajes pueden ser vistos por los servidores de la empresa (y a menudo se almacenan en ellos), pueden ser vulnerables a las solicitudes de la policía o al robo si los servidores de la empresa se ven comprometidos.



La imagen de arriba muestra un ejemplo de cifrado de la capa de transporte. A la izquierda, un teléfono inteligente envía un mensaje verde sin cifrar: "Hola". Ese mensaje se cifra y luego se transmite a una torre de telefonía móvil. En el medio, los servidores de la empresa son capaces de descifrar el mensaje, leer el contenido, decidir dónde enviarlo, volver a cifrarlo y enviarlo a la siguiente torre de telefonía móvil hacia su destino. Al final, el otro teléfono inteligente recibe el mensaje cifrado y lo descifra para leer "Hola".

Cifrado de Extremo a Extremo

El cifrado de extremo a extremo protege los mensajes en tránsito desde el emisor hasta el receptor. Garantiza que la información sea convertida en un mensaje secreto por su emisor original (el primer "extremo") y descifrada solo por su destinatario final (el segundo "extremo"). Nadie, ni siquiera la aplicación o el servicio que está utilizando, puede "escuchar" ni espiar su actividad.



La imagen de arriba muestra un ejemplo de cifrado de extremo a extremo. A la izquierda, un teléfono inteligente envía un mensaje verde sin cifrar: "Hola". Ese mensaje se cifra y se transmite a una torre de telefonía móvil y, a continuación, a los servidores de la aplicación/servicio, que no pueden leer el contenido, sino que transmitirán el mensaje secreto a su destino. Al final, el otro teléfono inteligente recibe el mensaje cifrado y lo descifra para leer "Hola". A diferencia del cifrado de la capa de transporte, su ISP o el host de mensajería no pueden descifrar el mensaje. Solo los puntos finales (los dispositivos originales que envían y reciben mensajes cifrados) tienen las claves para descifrar y leer el mensaje.

¿QUÉ TIPO DE CIFRADO NECESITAMOS?

A la hora de decidir si su organización necesita un cifrado de la capa de transporte o un cifrado de extremo a extremo para sus comunicaciones, las grandes preguntas que debe plantearse tienen que ver con la confianza. Por ejemplo, ¿confía en la aplicación o el servicio que está utilizando? ¿Confía en su infraestructura técnica? ¿Le preocupa la posibilidad de que un gobierno hostil pueda obligar a la empresa a entregar sus mensajes y, en ese caso, confía en las políticas de la empresa para protegerse de las peticiones de la policía?
Si responde "no" a alguna de estas preguntas, entonces necesita un cifrado de extremo a extremo. Si responde "sí", entonces puede ser suficiente un servicio que solo admita el cifrado de la capa de transporte, pero en general es mejor optar por servicios que admitan el cifrado de extremo a extremo cuando sea posible.

Cuando envíe mensajes a grupos, tenga en cuenta que la seguridad de sus mensajes es solo tan buena como la de todos los que los reciben. Por eso, además de elegir cuidadosamente las aplicaciones seguras, es importante que todos los miembros del grupo sigan otras buenas prácticas en relación con la seguridad de las cuentas y los dispositivos. Basta con una persona mal intencionada o un dispositivo infectado para que se filtre el contenido de todo un chat o una llamada de grupo.

¿QUÉ HERRAMIENTAS DE MENSAJERÍA CIFRADA DE EXTREMO A EXTREMO DEBEMOS UTILIZAR (A PARTIR DE 2021)?

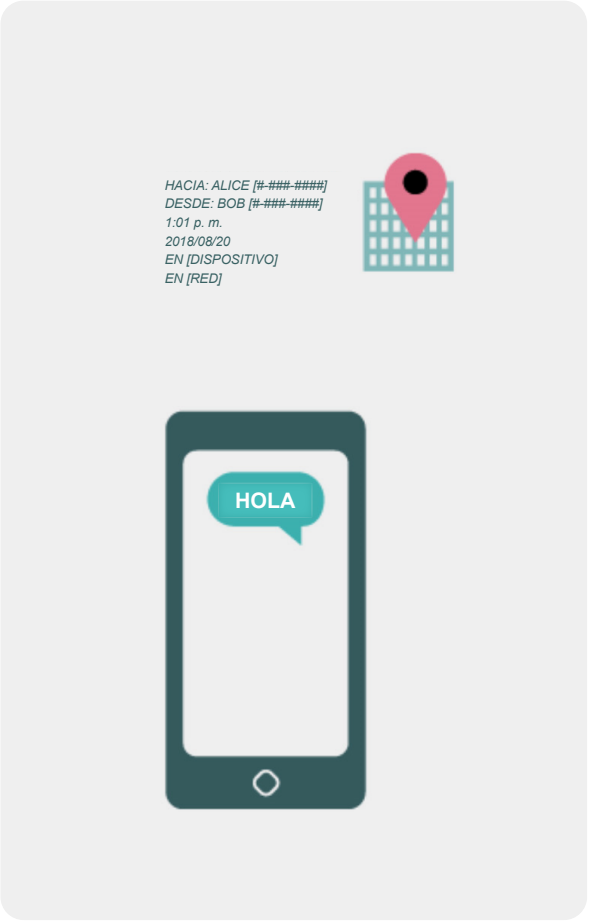
Si necesita utilizar el cifrado de extremo a extremo, o simplemente quiere adoptar la mejor práctica independientemente del contexto de amenazas de su organización, aquí tiene algunos ejemplos de servicios de confianza que, a partir de 2021, ofrecen mensajería y llamadas cifradas de extremo a extremo. Esta sección del Manual se actualizará periódicamente en línea, pero tenga en cuenta que todo cambia rápidamente en el mundo de la mensajería segura, por lo que es posible que estas recomendaciones no estén actualizadas en el momento en que usted lea esta sección. Tenga en cuenta también que sus comunicaciones son tan seguras como su dispositivo. Por ello, además de adoptar prácticas de mensajería segura, es esencial aplicar las mejores prácticas descritas en la sección de seguridad de los dispositivos de este Manual.

Herramientas Recomendadas para las Comunicaciones Cifradas de Extremo a Extremo

MENSAJES DE TEXTO (INDIVIDUALES O DE GRUPO)	• **Signal** • **WhatsApp (solo con configuraciones específicas detalladas a continuación)**
LLAMADAS DE AUDIO Y VIDEO	• **Signal (hasta 40 personas)** • **WhatsApp (hasta 32 personas en audio, y 8 personas en video)**
USO COMPARTIDO DE ARCHIVOS	• **Signal** • **Keybase/Keybase Teams** • **OnionShare + una aplicación de mensajería cifrada de extremo a extremo como Signal**

¿QUÉ SON LOS METADATOS Y QUÉ NOS DEBE PREOCUPAR?

Las personas con quienes usted y su personal hablan, y cuándo y dónde lo hacen, a menudo puede ser tan delicado como lo que se habla. Es importante recordar que el cifrado de extremo a extremo solo protege el contenido (el "qué") de sus comunicaciones. Aquí es donde entran en juego los metadatos. La Guía de Autoprotección Digital contra la Vigilancia de la EFF ofrece una visión general de los metadatos y de por qué son importantes para las organizaciones (incluida una ilustración de cómo son los metadatos):



Los metadatos suelen describirse como todo lo que no es el contenido de sus comunicaciones. Puede pensar en los metadatos como el equivalente digital de un sobre. Al igual que un sobre contiene información sobre el remitente, el destinatario y el destino de un mensaje, también lo hacen los metadatos. Los metadatos son información sobre las comunicaciones digitales que se envían y reciben.

Algunos ejemplos de metadatos son:

- con quién se comunica
- la línea de asunto de sus correos electrónicos
- la extensión de sus conversaciones
- la hora en la que tuvo lugar una conversación
- su ubicación cuando se comunica

Incluso una pequeña muestra de metadatos puede proporcionar una visión íntima de las actividades de su organización. Echemos un vistazo a lo reveladores que pueden ser los metadatos para los hackers, las agencias gubernamentales y las empresas que los recopilan:

Saben que usted llamó a un periodista y habló con él durante una hora antes de que ese periodista publicara una noticia con una cita anónima. Pero no saben de qué habló usted.

Saben que varios miembros del personal de su organización enviaron un mensaje a un destacado capacitador en seguridad digital local. Pero el tema de los mensajes sigue siendo un secreto.

Saben que recibió un correo electrónico de un servicio de pruebas de COVID, luego llamó a su médico y después visitó el sitio web de la Organización Mundial de la Salud a la misma hora. Pero no saben lo que había en el correo electrónico ni lo que ha hablado por teléfono.

Saben que ha recibido un correo electrónico de un grupo local de defensa de los derechos humanos con el asunto: "Dígale al gobierno: dejen de abusar de su poder". Pero el contenido del correo electrónico es invisible para ellos.

Los metadatos no están protegidos por el cifrado que ofrece la mayoría de los servicios de mensajes. Así que, por ejemplo, si envía un mensaje en WhatsApp, tenga en cuenta que aunque el contenido de su mensaje esté cifrado de extremo a extremo, sigue siendo posible que otros sepan con quién se está comunicando, con qué frecuencia y (con llamadas telefónicas) durante cuánto tiempo. En consecuencia, debe tener en cuenta qué riesgos existen (si los hubiera) si ciertos adversarios son capaces de averiguar con quién habla su organización, cuándo ha hablado con ellos y (en el caso del correo electrónico) las líneas de asunto generales de las comunicaciones de su organización.

Una de las razones por las que **Signal** es tan recomendable es que, además de proporcionar cifrado de extremo a extremo, ha **introducido funciones y ha asumido compromisos para reducir la cantidad de metadatos que registra y almacena**. Por ejemplo, la función "Sealed Sender" (Remitente sellado) de Signal cifra los metadatos sobre quién habla con quién, de modo que Signal solo conoce el destinatario de un mensaje, pero no el remitente. De manera predeterminada, esta función solo se activa cuando se comunica con contactos o perfiles existentes (personas), con los que ya se ha comunicado o que tiene almacenados en su lista de contactos. Sin embargo, puede habilitar esta configuración de "Sealed Sender" en "Allow from anyone" (Permitir de cualquier persona) si es importante para usted eliminar dichos metadatos en todas las conversaciones de Signal, incluso en aquellas con personas desconocidas para usted.

¿Qué pasa con el correo electrónico?

La mayoría de los proveedores de correo electrónico, por ejemplo, Gmail, Microsoft Outlook y Yahoo Mail, emplean cifrado de capa de transporte. Por lo tanto, si debe comunicar contenido confidencial a través del correo electrónico y le preocupa que su proveedor de correo electrónico pueda estar legalmente obligado a proporcionar información sobre sus comunicaciones a un gobierno u otro adversario, puede considerar usar una opción de correo electrónico encriptado de extremo a extremo. Tenga en cuenta, sin embargo, que incluso las opciones de correo electrónico cifrado de extremo a extremo dejan algo que desear desde una perspectiva de seguridad, por ejemplo, no cifran las líneas de asunto de los correos electrónicos y no protegen los metadatos. Si necesita comunicar información particularmente sensible, el correo electrónico no es la mejor opción. En su lugar, opte por opciones de mensajería segura como Signal.

Si su organización continúa utilizando el correo electrónico, es fundamental adoptar un sistema para toda la organización. Esto lo ayuda a limitar los riesgos comunes que surgen cuando el personal usa su correo electrónico personal para su trabajo, como las malas prácticas de seguridad de la cuenta. Por ejemplo, si el personal tiene cuentas de correo electrónico oficiales de la organización, se puede aplicar mejores prácticas como contraseñas seguras y 2FA en cualquier cuenta que administre su organización. Si, según su análisis anterior, el cifrado de extremo a extremo es necesario para su correo electrónico, tanto Protonmail como Tutanota ofrecen planes para organizaciones. Si el cifrado de la capa de transporte es adecuado para el correo electrónico de su organización, las opciones como Google Workspace (Gmail) o Microsoft 365 (Outlook) pueden ser útiles.

¿REALMENTE PODEMOS CONFIAR EN WHATSAPP?

WhatsApp es una opción popular para la mensajería segura, y puede ser una buena opción, dada su amplia difusión. A algunos les preocupa que sea propiedad de y esté controlada por Facebook, que ha estado trabajando para integrarla con sus otros sistemas. La gente también está preocupada por la cantidad de metadatos (es decir, información sobre con quién se comunica y cuándo) que recoge WhatsApp. Si decide utilizar WhatsApp como opción de mensajería segura, asegúrese de leer la sección anterior sobre los metadatos. También hay algunos ajustes que debe verificar para que estén configurados correctamente. Lo más importante es asegurarse de desactivar las copias de seguridad en la nube, o, por lo menos, activar la nueva función de **copias de seguridad cifradas de extremo a extremo** de WhatsApp usando una clave de encriptación de 64 dígitos o una contraseña larga, aleatoria y única guardada en un lugar seguro (como en su administrador de contraseñas). También asegúrese de encender las notificaciones de seguridad y verificar los códigos de seguridad. Puede encontrar guías sencillas para configurar estos ajustes para teléfonos Android **aquí** y para iPhone, **aquí**. Si su personal *y aquellos con los que todos se comunican* no configuran adecuadamente estas opciones, entonces no debería considerar que WhatsApp es una buena opción para las comunicaciones confidenciales que requieren cifrado de extremo a extremo. Signal sigue siendo la mejor opción para este tipo de necesidades de mensajería cifrada de extremo a extremo, dada su configuración segura predeterminada y la protección de los metadatos.

¿QUÉ SUCEDE CON LOS MENSAJES DE TEXTO?

Los mensajes de texto básicos son muy inseguros (los SMS estándar no están cifrados) y deben evitarse para cualquier cosa que no esté destinada al conocimiento público. Aunque los mensajes de iPhone a iPhone de Apple (conocidos como iMessages) están cifrados de extremo a extremo, si hay una persona que no es de iPhone en la conversación, los mensajes no están protegidos. Es mejor estar seguro y evitar los mensajes de texto para **cualquier cosa remotamente sensible, privada o confidencial.**

¿POR QUÉ NO SE RECOMIENDAN TELEGRAM, FACEBOOK MESSENGER O VIBER PARA CHATS SEGUROS?

Algunos servicios, como Facebook Messenger y Telegram, solo ofrecen cifrado de extremo a extremo si usted los activa deliberadamente (y solo para chats individuales), por lo que no son buenas opciones para la mensajería sensible o privada, especialmente para una organización. No confíe en estas herramientas si necesita utilizar el cifrado de extremo a extremo, porque es bastante fácil olvidarse de cambiar la configuración predeterminada menos segura. Viber afirma que ofrece cifrado de extremo a extremo, pero no ha puesto su código a disposición de investigadores de seguridad externos para que lo revisen. El código de Telegram tampoco se ha puesto a disposición de una auditoría pública. Por ello, muchos expertos temen que el cifrado de Viber (o los "chats secretos" de Telegram) sea deficiente y, por lo tanto, no sea adecuado para las comunicaciones que requieren un verdadero cifrado de extremo a extremo.

NUESTROS CONTACTOS Y COLEGAS UTILIZAN OTRAS APLICACIONES. ¿CÓMO PODEMOS CONVENCERLOS DE QUE DESCARGUEN UNA NUEVA APLICACIÓN?

A veces hay que elegir entre seguridad y comodidad, pero un poco de esfuerzo extra merece la pena para las comunicaciones sensibles. Dé un buen ejemplo a sus contactos. Si tiene que utilizar otros sistemas menos seguros, sea muy consciente de lo que dice. Evite hablar de temas delicados. En algunas organizaciones, pueden utilizar un sistema para el chat general y otro con la gerencia para las conversaciones más confidenciales. Por supuesto, lo más sencillo es que todo se cifre automáticamente en todo momento: no hay que recordar ni pensar en nada.

Por suerte, las aplicaciones cifradas de extremo a extremo, como Signal, son cada vez más populares y fáciles de usar, por no mencionar que se han adaptado a docenas de idiomas para su uso mundial. Si sus socios u otros contactos necesitan ayuda para cambiar las comunicaciones a una opción cifrada de extremo a extremo, como Signal, tómese un tiempo para explicarles por qué es tan importante proteger adecuadamente sus comunicaciones. Cuando todo el mundo comprenda su importancia, los pocos minutos necesarios para descargar una nueva aplicación y el par de días que puede llevar acostumbrarse a usarla no parecerán un gran problema.

¿HAY OTROS AJUSTES PARA LAS APLICACIONES CIFRADAS DE EXTREMO A EXTREMO QUE DEBAMOS CONOCER?

En la aplicación Signal, también es importante la verificación de los códigos de seguridad (denominados Números de Seguridad). Para ver un número de seguridad y verificarlo en Signal, puede abrir el chat con un contacto, tocar su nombre en la parte superior de la pantalla y desplazarse hacia abajo para tocar "View Safety Number" (Ver número de seguridad). Si su número de seguridad coincide con el de su contacto, puede marcarlo como "verificado" desde esa misma pantalla. Es especialmente importante prestar atención a estos números de seguridad y verificar sus contactos si recibe una notificación en un chat de que su número de seguridad con un determinado contacto ha cambiado. Si usted o el resto del personal necesita ayuda para configurar estos ajustes, Signal **proporciona instrucciones útiles**. Si utiliza Signal, ampliamente considerada como la mejor opción para la mensajería segura y las llamadas individuales, asegúrese de establecer también un pin seguro. Utilice al menos seis dígitos, y no algo fácil de adivinar, como su fecha de nacimiento. Para obtener más consejos sobre cómo configurar correctamente **Signal** y **WhatsApp**, puede consultar las **guías de herramientas** para ambos desarrolladas por la EFF en su Guía de Autoprotección Digital contra la Vigilancia.

Uso de Aplicaciones de Chat en el Mundo Real

Para limitar los daños en caso de pérdida, robo o confiscación del teléfono, es una buena práctica minimizar el historial de mensajes que se guardan en el teléfono. Una forma sencilla de hacerlo es activar **la función "disappearing messages"** (mensajes que se borran automáticamente) en los chats de grupo de su organización, y animar al personal a hacerlo también en sus chats personales.

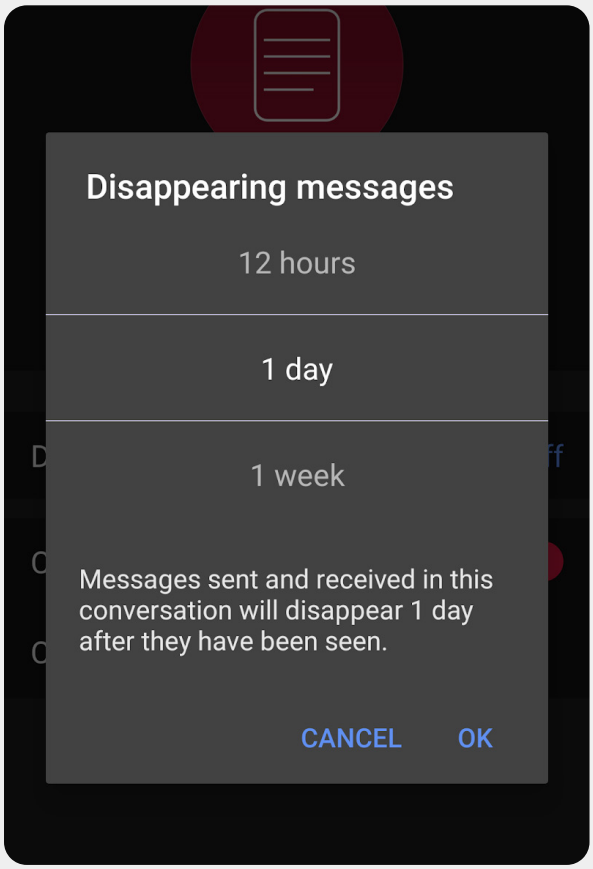
En Signal y otras aplicaciones de mensajería populares, puede establecer un temporizador para que los mensajes se borren en un determinado número de minutos u horas después de ser leídos. Esta configuración se puede personalizar en función del chat individual o de grupo. Para la mayoría de nosotros, establecer una ventana de eliminación automática de una semana nos brinda mucho tiempo para buscar cosas y, al mismo tiempo, no conserva mensajes que nunca necesitará, pero que podrían ser utilizados en su contra en el futuro. Recuerde que lo que no tiene no se lo pueden robar.

Para activar la eliminación automática de mensajes en Signal, abra un chat, pulse el nombre de la persona/grupo con el que está chateando, pulse la función "disappearing messages", elija un temporizador y pulse "ok". Existe una configuración similar en WhatsApp.

En situaciones más graves en las que sea necesario eliminar inmediatamente un mensaje, quizás porque le hayan robado el teléfono a alguien o porque usted ha enviado un mensaje a la persona equivocada, tenga en cuenta que Signal le permite a un grupo o a una persona eliminar un mensaje del teléfono de alguien dentro de las tres horas siguientes al envío, simplemente borrándolo de su chat. A pesar de sus limitaciones de cifrado, Telegram sigue siendo popular en muchos países por una función similar, que permite a los usuarios borrar mensajes entre dispositivos sin restricciones.



Dicho esto, si su organización está preocupada por la seguridad del personal como resultado de las comunicaciones que podrían verse en sus teléfonos, entonces el uso de mensajes que se borran automáticamente con temporizadores cortos es probablemente la opción más sencilla y sostenible.



¿QUÉ PASA CON LAS VIDEOLLAMADAS DE GRUPOS MÁS GRANDES? ¿HAY OPCIONES DE CIFRADO DE EXTREMO A EXTREMO?

Con el aumento del trabajo remoto, es importante tener una opción segura para las videollamadas de los grupos grandes de su organización. Desgraciadamente, actualmente no existen grandes opciones que cumplan todos los requisitos: que sean fáciles de usar, que admitan un gran número de asistentes y funciones de colaboración, y que permitan el cifrado predeterminado de extremo a extremo.

Para grupos de hasta 40 personas, Signal es una opción de cifrado de extremo a extremo muy recomendado. Se puede unirse a las videollamadas en grupo desde un teléfono inteligente o desde la aplicación de escritorio de Signal en una computadora, el cual permite la función de compartir pantalla. Sin embargo, tenga en cuenta que solo sus contactos que ya utilizan Signal pueden ser añadidos a un grupo de Signal.

Si está buscando otras opciones, una plataforma que recientemente ha añadido una opción de cifrado de extremo a extremo es **Jitsi Meet.** Jitsi Meet es una solución de audio y videoconferencia en la web que puede funcionar para grandes audiencias (hasta 100 personas) y no requiere la descarga de una aplicación o un software especial. Tenga en cuenta que si utiliza esta función con grupos grandes (más de 15 a 20 personas), la calidad de la llamada puede disminuir. Para organizar una reunión en Jitsi Meet, puede ir a **meet.jit.si**, escribir un código de reunión y compartir ese enlace (a través de un canal seguro como Signal) con los participantes que desee. Para utilizar el cifrado de extremo a extremo, eche un vistazo a estas **instrucciones** indicadas por Jitsi. Tenga en cuenta que todos los usuarios individuales tendrán que activar ellos mismos el cifrado de extremo a extremo para que funcione. Cuando utilice Jitsi, asegúrese también de crear nombres aleatorios para las salas de reuniones y de utilizar contraseñas fuertes para proteger sus llamadas.

Si esta opción no funciona para su organización, puede considerar el uso de una opción comercial popular, como WebEx o Zoom, con cifrado de extremo a extremo activado. Hace tiempo que WebEx permite el cifrado de extremo a extremo, pero esta opción no está activada de manera predeterminada y requiere que los participantes descarguen WebEx para unirse a la reunión. Para obtener la opción de cifrado de extremo a extremo para su cuenta de WebEx, debe abrir un caso de asistencia de WebEx y seguir **estas instrucciones** para asegurarse de que el cifrado de extremo a extremo esté configurado. Solo el anfitrión de la reunión tiene que activar el cifrado de extremo a extremo. Si los participantes lo hacen, toda la reunión estará cifrada de extremo a extremo. Si utiliza WebEx para reuniones de grupo y talleres seguros, asegúrese de habilitar también contraseñas seguras en sus llamadas.

Tras meses de prensa negativa, Zoom desarrolló una **opción de cifrado de extremo a extremo** para sus llamadas. Sin embargo, esa opción no está activada de manera predeterminada, requiere que el anfitrión de la llamada asocie su cuenta con un número de teléfono y solo funciona si todos los participantes se unen a través de la aplicación de escritorio o móvil de Zoom en lugar de marcar. Debido a que es fácil desconfigurar accidentalmente estos ajustes, no recomendamos confiar en Zoom como opción de cifrado de extremo a extremo. Sin embargo, si requiere un cifrado de extremo a extremo y Zoom es su única opción, puede seguir las **instrucciones** de Zoom para configurarlo. Solo asegúrese de comprobar cualquier llamada antes de que se inicie para asegurarse de que realmente está cifrada de extremo a extremo haciendo clic en el candado verde del extremo superior izquierdo de la pantalla de Zoom y viendo que aparece “de extremo a extremo” junto a la configuración de cifrado. También debe establecer un código de acceso fuerte para cualquier reunión de Zoom.

Además de las herramientas mencionadas anteriormente, **este diagrama de flujo** desarrollado por Frontline Defenders destaca algunas opciones de videollamada y conferencia que, según su contexto de riesgo, podrían tener sentido para su organización.

Sin embargo, vale la pena señalar que ciertas características populares de las herramientas anteriores solo funcionan con el cifrado de la capa de transporte. Por ejemplo, activar el cifrado de extremo a extremo en Zoom desactiva las salas de reuniones, las capacidades de sondeo y la grabación en la nube. En Jitsi Meet, las salas de reuniones pueden desactivar la función de cifrado de extremo a extremo, lo que provoca una disminución involuntaria de la seguridad.

¿Y SI REALMENTE NO NECESITAMOS EL CIFRADO DE EXTREMO A EXTREMO PARA TODAS NUESTRAS COMUNICACIONES?

Si no es necesario el cifrado de extremo a extremo para todas las comunicaciones de su organización según su evaluación de riesgos, puede considerar el uso de aplicaciones protegidas por el cifrado de la capa de transporte. Recuerde que este tipo de cifrado requiere que confíe en el proveedor del servicio, como Google para Gmail, Microsoft para Exchange o Facebook para Messenger, porque ellos (y cualquier persona con la que puedan verse obligados a compartir información) pueden ver/escuchar sus comunicaciones. Una vez más, las mejores opciones dependerán de su modelo de amenaza (por ejemplo, si no confía en Google o si el gobierno de los Estados Unidos es su adversario, entonces Gmail no es una buena opción), pero algunas opciones populares y generalmente confiables incluyen:

CORREO ELECTRÓNICO	• **Gmail (a través de Google Workspace)** • **Outlook (a través de Office 365)** • No aloje su propio servidor de Microsoft Exchange para el correo electrónico de su organización. Si lo está haciendo actualmente, debería migrar a Office 365.
MENSAJES DE TEXTO (INDIVIDUALES O DE GRUPO)	• **Google Hangouts** • **Slack** • **Microsoft Teams** • **Mattermost** • **Line** • **KaKao Talk** • **Telegram**
CONFERENCIAS DE GRUPO, LLAMADAS DE AUDIO Y VIDEO	• **Jitsi Meet** • **Google Meet** • **Microsoft Teams** • **WebEx** • **GotoMeeting** • **Zoom**
USO COMPARTIDO DE ARCHIVOS	• **Google Drive** • **Microsoft Sharepoint** • **Dropbox** • **Slack** • **Microsoft Teams**

NOTA SOBRE EL INTERCAMBIO DE ARCHIVOS

Además de compartir mensajes de forma segura, compartir archivos de forma segura es probablemente una parte importante del plan de seguridad de su organización. La mayoría de las opciones para compartir archivos están integradas en las aplicaciones de mensajería o en los servicios que ya utiliza. Por ejemplo, compartir archivos a través de Signal es una buena opción si se necesita un cifrado de extremo a extremo. Y si el cifrado de la capa de transporte es suficiente, el uso de Google Drive o Microsoft Sharepoint podría ser una buena opción para su organización. Tiene que asegurarse de configurar correctamente los ajustes de uso compartido para que solo las personas adecuadas tengan acceso a un determinado documento o carpeta, y asegurarse de que estos servicios estén conectados a las cuentas de correo electrónico de la organización (no a las personales). Si puede, prohíba que se compartan archivos sensibles a través de archivos adjuntos de correo electrónico o físicamente con USB. El uso de dispositivos como los USB dentro de su organización aumenta en gran medida la probabilidad de malware o de robo, y confiar en el correo electrónico u otras formas de archivos adjuntos debilita las defensas de su organización contra los ataques de phishing o suplantación de identidad.



Alternativas de la Organización para Compartir Archivos

Si está buscando una opción para su organización a fin de compartir archivos de forma segura, que no esté directamente integrada en una plataforma de mensajería (o tal vez se encuentre con límites de tamaño de archivo al compartir documentos grandes), considere OnionShare. OnionShare es una herramienta de código abierto que permite compartir un archivo de cualquier tamaño de forma segura y anónima. Funciona haciendo que el remitente descargue la aplicación OnionShare (disponible en computadoras Mac, Windows y Linux), suba los archivos que desea compartir y genere un enlace único. Este enlace, que solo puede ser procesado en el Navegador Tor, puede ser compartido a través de cualquier canal de mensajería seguro (Signal, por ejemplo) con el destinatario. El destinatario puede abrir el enlace en el Navegador Tor y descargar el/los archivo/s en su computadora. Tenga en cuenta que los archivos son tan seguros como el método a través del cual comparte el enlace. Tor se explicará con más detalle en una sección posterior "avanzada" del Manual, pero para los propósitos de compartir archivos dentro de su organización, tenga en cuenta a OnionShare como una alternativa más segura para compartir archivos grandes en USB de la oficina si no tiene una opción de proveedor de nube de confianza.

Si su organización ya está invirtiendo en un administrador de contraseñas, como se describe en la sección de este Manual sobre contraseñas, y elige la cuenta premium o de equipos de Bitwarden, la función Bitwarden Send es otra opción para compartir archivos de forma segura. Esta función permite a los usuarios crear enlaces seguros para compartir archivos cifrados a través de cualquier canal de mensajería segura (como Signal). El tamaño de los archivos está limitado a 100 MB, pero Bitwarden Send permite establecer una fecha de caducidad en los enlaces, proteger con contraseña el acceso a los archivos compartidos y limitar el número de veces que se puede abrir el enlace.



Comunicar y Compartir Datos de Forma Segura

- **Exija el uso de servicios de mensajería cifrados de extremo a extremo de confianza para las comunicaciones sensibles de su organización (e idealmente para todas las comunicaciones).**
  - Dedique tiempo a explicarle al personal y a los socios externos por qué son tan importantes las comunicaciones seguras; esto aumentará el éxito de su plan.
- **Establezca una política sobre el tiempo que conservará los mensajes y cuándo/si la organización utilizará comunicaciones que "se borran automáticamente".**
- **Asegúrese de que la configuración de las aplicaciones de comunicaciones seguras es la adecuada, incluido lo siguiente:**
  - Asegúrese de que todo el personal esté atento a las notificaciones de seguridad y, si utiliza WhatsApp, no haga copias de seguridad de los chats.
  - Si utiliza una aplicación en la que el cifrado de extremo a extremo no está activado de manera predeterminada (por ejemplo, Zoom o Webex), asegúrese de que los usuarios requeridos hayan activado la configuración adecuada al inicio de cualquier llamada o reunión.
- **Utilice servicios de correo electrónico en la nube, como Office 365 o Gmail, para su organización.**
  - No intente alojar su propio servidor de correo electrónico.
  - No permita que el personal utilice cuentas de correo electrónico personales para trabajar.
- **Recuerde con frecuencia a la organización las mejores prácticas de seguridad relacionadas con la mensajería y los metadatos de grupo.**
  - Esté atento a quién se incluye en los mensajes de grupo, chats e hilos de correo electrónico.

Almacenamiento Seguro de Datos

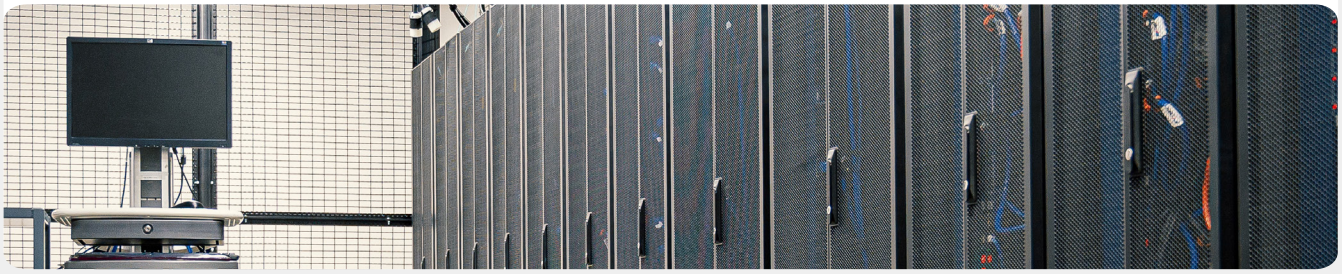
Para la mayoría de las organizaciones de la sociedad civil, una de las decisiones más importantes es dónde almacenar sus datos.

¿Es "más seguro" almacenar los datos en las computadoras del personal, en un servidor local, en dispositivos de almacenamiento externo o en la nube? En el 99 % de las situaciones, la opción más fácil y segura es mantener los datos almacenados en servicios de almacenamiento en la nube de confianza. Algunos ejemplos comunes son Microsoft 365, Google Drive o Dropbox. Sin un plan integral de almacenamiento en la nube, es probable que los datos de su organización se almacenen en diversos lugares, como las computadoras del personal, los discos duros externos e incluso un servidor local. Aunque es posible proteger los datos en todos estos dispositivos, es muy difícil hacerlo con éxito sin gastar mucho dinero y contratar a personal importante de TI

Al seleccionar una herramienta o servicio para almacenar sus datos, asegúrese que confía en la empresa o el grupo que lo respalda. Una búsqueda rápida en Google y una consulta con expertos en seguridad digital pueden ser de gran ayuda para verificar la confiabilidad de un posible proveedor de tecnología. Algunas preguntas a tener en cuenta incluyen: ¿Venden o comparten sus datos privados? ¿Tienen los recursos de seguridad apropiados en el personal? ¿Ofrecen funciones de seguridad (como 2FA) para ayudarlo a proteger su cuenta?

Almacenamiento de Datos y Sociedad Civil

La llegada del almacenamiento de datos asequible (a veces gratuito) basado en la nube ha facilitado la vida (y la seguridad) de muchas organizaciones de la sociedad civil con recursos limitados. Desafortunadamente, muchos siguen intentando alojar sus propios servidores con escasos conocimientos o soporte informáticos. En marzo de 2021, la amenaza de esa infraestructura organizativa se hizo real para decenas de miles de organizaciones de todo el mundo cuando un actor de amenazas afiliado al gobierno chino, llamado Hafnium, desató una catástrofe de ciberseguridad mundial con un sofisticado ataque a servidores de Microsoft Exchange autoalojados. El ataque comprometió los servidores locales, lo que permitió a los hackers obtener acceso a las cuentas de correo electrónico de la organización e instalar malware adicional en los servidores de las víctimas y los sistemas conectados. Aunque Microsoft publicó rápidamente una actualización e instrucciones para identificar y eliminar a los posibles intrusos, muchas organizaciones pequeñas carecían de la capacidad informática para aplicar rápidamente dichas actualizaciones, lo que las dejó expuestas durante largos períodos de tiempo. El alcance y la repercusión de este ataque informático mundial revelan el peligro que corren las organizaciones civiles, especialmente las más pequeñas con personal informático limitado, que optan por autoalojar los servidores de correo electrónico y otros tipos de datos sensibles.



BENEFICIOS DEL ALMACENAMIENTO EN LA NUBE

Aunque tome todas las medidas adecuadas para proteger sus computadoras contra el malware y los robos físicos, sigue siendo posible que un adversario decidido piratee su computadora o servidor local. Es mucho más difícil para ellos vencer las defensas de seguridad de, por ejemplo, Google o Microsoft. Las buenas empresas de almacenamiento en la nube cuentan con recursos de seguridad incomparables y tienen un fuerte incentivo comercial para ofrecer la máxima seguridad a sus usuarios. En resumen: una estrategia de almacenamiento en la nube de confianza será mucho más fácil y barata de implementar y mantener segura a lo largo del tiempo. Así, en lugar de preocuparse por intentar proteger su propio servidor, puede concentrar su energía en un puñado de tareas más sencillas. Mantener la mayor parte de la información en la nube también ayuda a evitar otros riesgos comunes. ¿Alguien ha olvidado su computadora o teléfono móvil en el autobús? ¿Su hijo ha volcado un vaso de zumo sobre su teclado, y dejó a su dispositivo inutilizable? ¿Un empleado tiene malware en su computadora y necesita eliminarlo y empezar de cero? Si la mayoría de los documentos y datos están en la nube, es fácil volver a sincronizarlos y empezar de cero en una computadora limpia o completamente nueva. Además, si un malware entra en una computadora o si un ladrón escanea un disco duro, no hay nada que robar si se accede a la mayoría de los documentos a través del navegador web.

¿QUÉ PROVEEDOR DE ALMACENAMIENTO EN LA NUBE DEBEMOS ELEGIR?

Las dos opciones más populares de almacenamiento en la nube son Google Workspace (antes conocido como GSuite) y Microsoft 365. Si usted y su personal ya utilizan Gmail, tiene mucho sentido registrar su organización en Google Workspace y almacenar los datos en Google Drive con sus aplicaciones integradas Google Docs, Sheets y Slides para el procesamiento de textos, planillas de cálculo y presentaciones. Del mismo modo, si se trata de una organización que depende de Excel y Word, la opción más fácil es registrarse en Microsoft 365, que brinda a su organización acceso a Outlook para el correo electrónico y versiones con licencia de Microsoft Word, Excel, PowerPoint y Teams. Independientemente del proveedor que elija, almacenar los datos de forma segura en la nube requiere aplicar una buena configuración de uso compartido y capacitar al personal para que entienda cómo y cuándo compartir (y no compartir) carpetas y documentos. En general, debe configurar carpetas dentro de su unidad de almacenamiento en la nube que limiten el acceso solo al personal que lo necesite para determinados archivos. Realice una auditoría rutinaria de su sistema para asegurarse de que no está "compartiendo en exceso" ningún archivo (por ejemplo, activando el uso compartido de enlaces universales para archivos que deberían estar limitados a unas pocas personas).

¿QUÉ PASA SI NO CONFIAMOS EN GOOGLE O MICROSOFT U OTROS PROVEEDORES DE ALMACENAMIENTO EN LA NUBE?

Si uno de sus adversarios (por ejemplo, un gobierno extranjero o local) puede obligar legalmente a Google o a Microsoft (o a otro proveedor de almacenamiento en la nube) a entregar datos, entonces podría no tener sentido elegirlos como opciones de almacenamiento de datos. Este riesgo puede ser mayor si su adversario es el gobierno de los Estados Unidos, por ejemplo, pero mucho menor si su adversario es un régimen autoritario. Tenga en cuenta que tanto Google como Microsoft tienen políticas sobre la entrega de datos solo cuando están legalmente obligados a hacerlo, y reconozca que su organización podría ser vulnerable al mismo tipo de demandas legales de su propio gobierno si aloja los datos localmente. En situaciones en las que el almacenamiento en la nube de Google o Microsoft no tiene sentido para su organización, una opción alternativa a considerar es Keybase. La función "teams" (equipos) de Keybase permite a su organización compartir archivos y mensajes mediante un cifrado de extremo a extremo en un entorno seguro en la nube sin tener que depender de un proveedor externo. Por ello, puede ser una buena opción para almacenar de forma segura documentos y archivos en toda la organización. Sin embargo, Keybase es menos familiar para la mayoría de los usuarios, por lo que hay que tener en cuenta que la adopción de esta herramienta probablemente requiera más capacitación y esfuerzo que las otras soluciones mencionadas. Dicho esto, si prefiere no adoptar estas recomendaciones y no utilizar el almacenamiento en la nube, es crucial que invierta tiempo y recursos en reforzar las defensas digitales de los dispositivos de su organización, y que se asegure de que los servidores locales estén correctamente configurados, cifrados y se mantengan físicamente seguros. Probablemente ahorre las cuotas mensuales de suscripción, pero le costará a su organización tiempo y recursos del personal, y serán mucho más vulnerables a los ataques.

COPIA DE SEGURIDAD DE LOS DATOS

Tanto si su organización almacena los datos en dispositivos físicos como en la nube, es importante tener una copia de seguridad. Especialmente si depende del almacenamiento en dispositivos físicos, es bastante fácil perder el acceso a sus datos. Podría derramar café sobre su computadora y destruir el disco duro. Las computadoras del

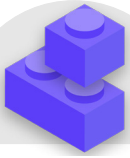
personal podrían ser pirateadas y todos los archivos locales bloqueados con un ransomware. Alguien podría perder un dispositivo en el tren o sufrir el robo del dispositivo junto con su bolso. Como se mencionó anteriormente, esta es otra razón por la que el uso del almacenamiento en la nube puede ser un beneficio, ya que no está atado a un dispositivo específico que puede ser infectado, robado o perderse. Las computadoras Mac vienen con un software de copia de seguridad integrado llamado Time Machine, que se utiliza junto con un dispositivo de almacenamiento externo; para los dispositivos de Windows, el Historial de Archivos ofrece una funcionalidad similar. Los teléfonos iPhone y Android pueden crear una copia de seguridad automática de sus contenidos más importantes en la nube si se activa en la configuración del teléfono. Si su organización utiliza el almacenamiento en la nube (como Google Drive), el riesgo de que Google se caiga o sus datos se destruyan en un desastre es bastante bajo, pero el error humano (como la eliminación accidental de archivos importantes) sigue siendo una posibilidad. Así que explorar una solución de copia de seguridad en la nube como Backupify o SpinOne Backup puede valer la pena. Si los datos se almacenan en un servidor local o en dispositivos, una copia de seguridad segura es aún más importante. Puede crear una copia de seguridad de los datos de su organización en un disco duro externo, pero asegúrese de cifrar ese disco duro con una contraseña segura. Time Machine puede cifrar los discos duros, o usted mismo puede utilizar herramientas de cifrado de confianza para todo el disco duro, como VeraCrypt o BitLocker. Asegúrese de mantener los dispositivos de copia de seguridad en un lugar separado de sus otros dispositivos y archivos. Recuerde que un incendio que destruya tanto sus computadoras como las copias de seguridad significa que no tiene ninguna copia de seguridad. Considere la posibilidad de guardar una copia en un lugar muy seguro, como una caja de seguridad.

Tenga en cuenta: si usa un proveedor de nube en un país con leyes específicas de localización de datos, consulte con expertos legales para comprender mejor cómo una solución de almacenamiento en la nube puede cumplir con los requisitos locales. Muchos proveedores de almacenamiento en la nube, incluidos Google y Microsoft, ahora ofrecen opciones que permiten a algunos clientes elegir la ubicación geográfica de sus datos en la nube, por ejemplo



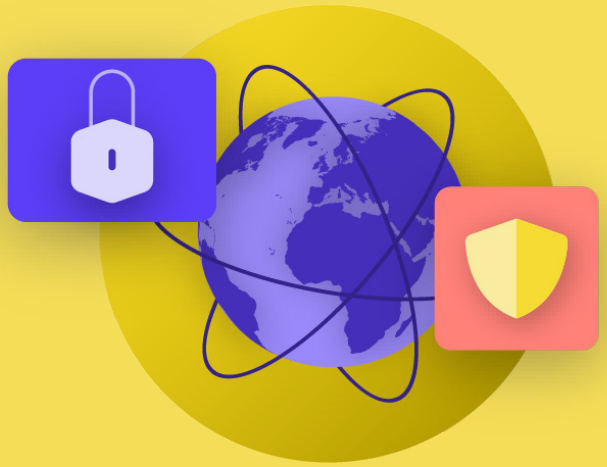
Mejora de la seguridad de las cuentas en la nube de la organización

Si su organización opta por configurar un dominio en Google Workspace o Microsoft 365, tenga en cuenta que ambas empresas ofrecen mayores niveles de seguridad (de forma gratuita en muchos casos) a las organizaciones de la sociedad civil. El Programa de Protección Avanzada de Google y AccountGuard de Microsoft proporcionan una seguridad aún más sólida a todas las cuentas en la nube de su organización, y lo ayudan a reducir en gran medida la probabilidad de que se produzca una suplantación de identidad efectiva y de que la cuenta se vea comprometida. Si cree que su organización cumple los requisitos y está interesado en inscribirla en cualquiera de los dos planes, visite los sitios web con los enlaces mencionados anteriormente o póngase en contacto con cyberhandbook@ndi.org para obtener más ayuda.



Comunicar y Compartir Datos de Forma Segura

- **Almacene los datos sensibles exclusivamente en un servicio de confianza de almacenamiento en la nube.**
  - Asegúrese de que cualquier cuenta conectada que se utilice para acceder a dicho servicio tenga contraseñas seguras y 2FA.
- **Establezca y aplique una política para limitar la configuración de uso compartido dentro de la nube.**
  - Capacite a todo el personal sobre cómo compartir correctamente (y no en exceso) los documentos.
- **Si su organización opta por almacenar los datos localmente, invierta en personal informático calificado.**
- **Mantenga las copias de seguridad de sus datos de forma segura: cifre los discos duros de las copias de seguridad u otros dispositivos de copia de seguridad.**



Mantenerse seguro en internet

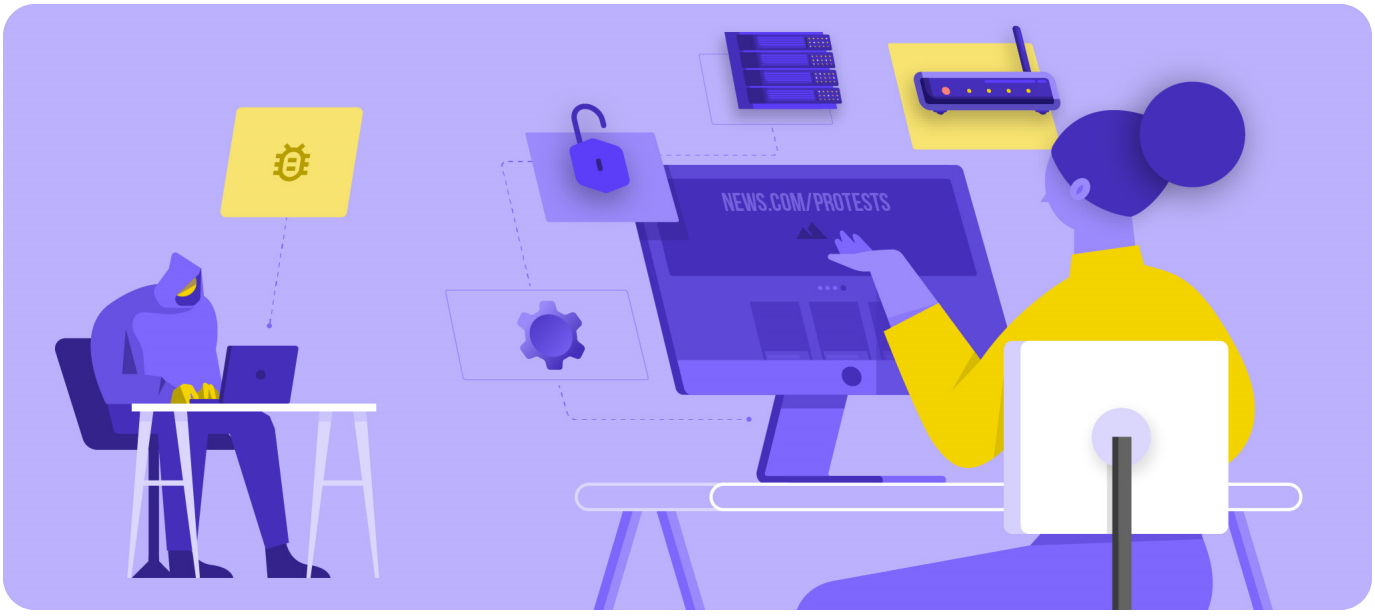
Al utilizar internet en su teléfono o computadora, su actividad puede decir bastante sobre usted y su organización.

Es importante mantener la información sensible –como los nombres de usuario y las contraseñas que se escriben en un sitio web, las publicaciones en las redes sociales o, en ciertos contextos, incluso los nombres de los sitios web que se visitan– fuera de la vista de ojos curiosos. El bloqueo o la restricción del acceso a determinados sitios o aplicaciones también es una preocupación común. Estos dos problemas –la vigilancia y la censura en internet– van de la mano, y las estrategias para reducir su impacto son similares.

Navegar de Manera Segura

USO DE HTTPS

El paso más importante para limitar la capacidad de un adversario de vigilar a su organización en línea es minimizar la cantidad de información disponible sobre su actividad en internet y la de sus colegas. Asegúrese siempre de conectarse a los sitios web de manera segura: compruebe que la URL (ubicación) comienza con "https" y muestra un pequeño ícono de candado en la barra de direcciones de su navegador. Cuando navega por internet sin cifrado, queda expuesta la información que se teclea en un sitio (como contraseñas, números de cuenta o mensajes), los detalles del sitio y las páginas que se visitan. Esto significa que (1) cualquier hacker en su red, (2) su administrador de red, (3) su ISP y cualquier entidad con la que puedan compartir datos (como las autoridades gubernamentales), (4) el ISP del sitio que está visitando y cualquier entidad con la que puedan compartir datos, y por supuesto (5) el sitio que está visitando, todos tienen acceso a bastante información potencialmente sensible.



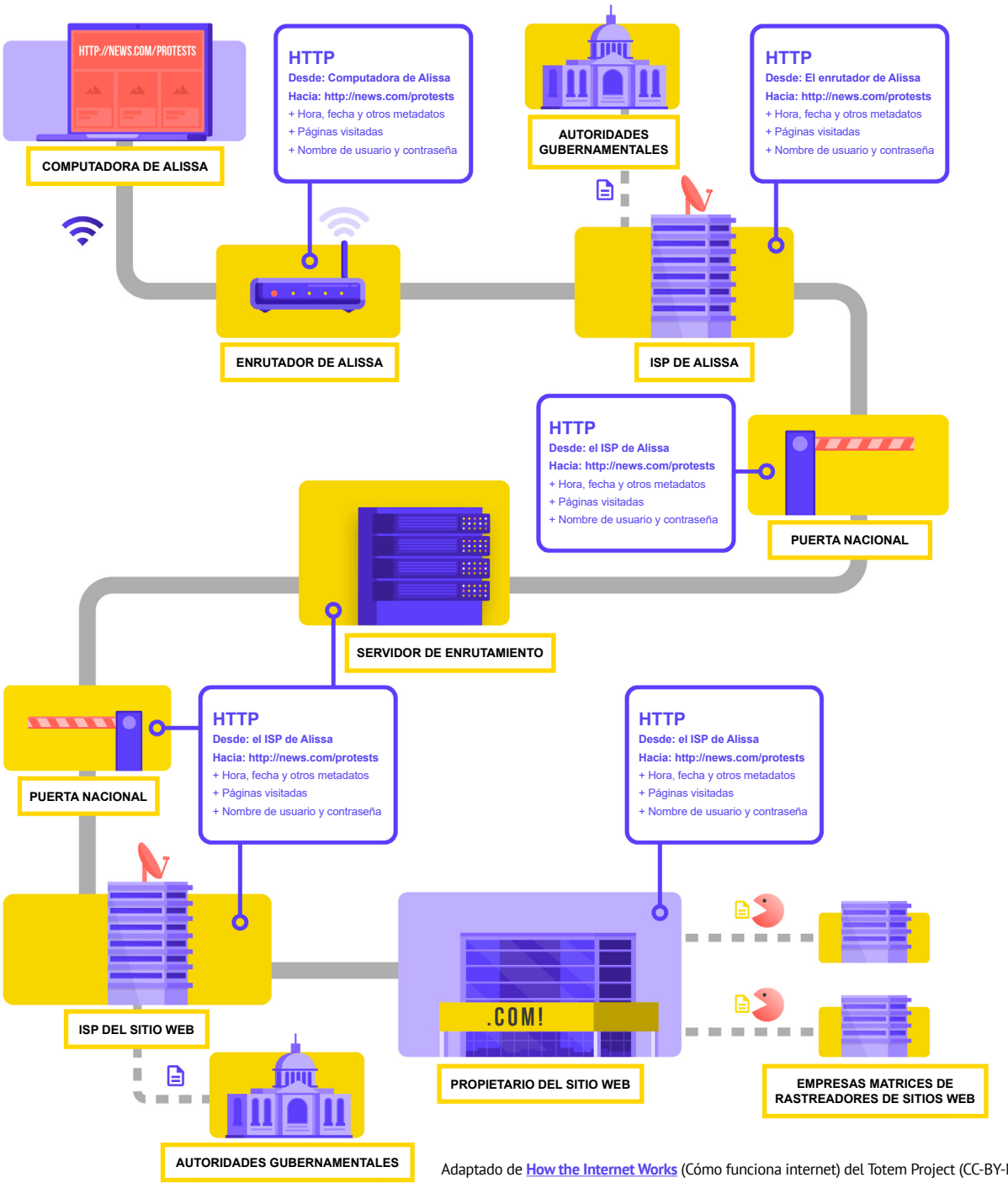
Vigilancia, Censura y Sociedad Civil

Los gobiernos utilizan cada vez más su influencia y autoridad sobre los proveedores de servicios de internet y otras infraestructuras locales de internet para impedir que las personas y los grupos de la sociedad civil accedan a la información en internet. En algunos casos, estas interrupciones de internet tienen como objetivo derribar las principales plataformas de comunicación e intercambio de información, incluidas las redes sociales y los sitios de noticias. Por ejemplo, en respuesta a las protestas derivadas de un golpe militar, los militares de Myanmar ordenaron a los operadores de telefonía móvil que cerraran temporalmente toda la red de datos móviles del país. Esto llegó poco después de un bloqueo más selectivo de Facebook, Twitter e Instagram. Además de bloquear el acceso a internet y a los sitios web, los gobiernos y otros agentes de amenazas de todo el mundo utilizan una tecnología de vigilancia cada vez más accesible para controlar la actividad de los ciudadanos en línea. Por ejemplo, según el informe Freedom on the Net 2020 de Freedom House, el gobierno ugandés se asoció con la empresa tecnológica china Huawei para **vigilar a figuras de la oposición y activistas civiles** en el período previo y posterior a unas polémicas elecciones presidenciales en el país.

La creciente frecuencia de este tipo de ataques a la libertad de información en línea pone de manifiesto lo esencial que es para los grupos de la sociedad civil comprender los riesgos de operar en internet y desarrollar planes para conectarse cuando la conectividad está restringida.



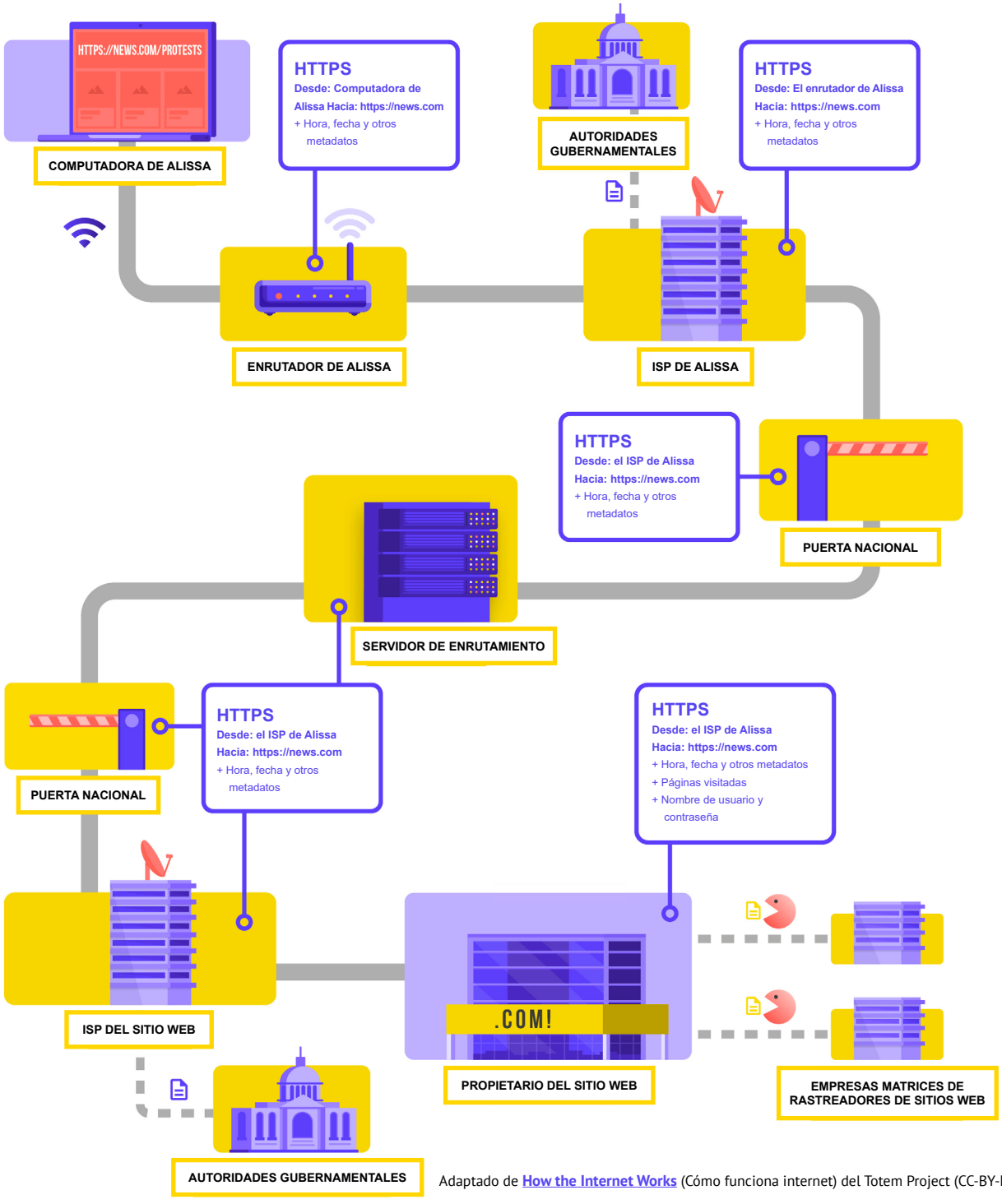
Veamos un ejemplo real de cómo es la navegación sin cifrado:



Adaptado de How the Internet Works (Cómo funciona internet) del Totem Project (CC-BY-NC-SA)

Como se muestra arriba, un adversario puede ver dónde está usted, que usted está navegando en news.com, mirando específicamente la página sobre las protestas en su país, y ver su contraseña, que usted comparte para entrar en el sitio. Esta información en manos equivocadas no solo expone a su cuenta, sino que también da a sus adversarios una buena idea de lo que usted podría estar haciendo o pensando.

El uso de HTTPS (la "s" significa "seguro" en inglés) significa que hay cifrado. Esto le ofrece mucha más protección. Veamos cómo es la navegación con HTTPS (es decir, con cifrado):



Adaptado de How the Internet Works (Cómo funciona internet) del Totem Project (CC-BY-NC-SA)

Al existir HTTPS, un adversario potencial ya no puede ver su contraseña u otra información sensible que usted podría compartir en un sitio web. Sin embargo, un adversario potencial puede seguir viendo qué dominios (por ejemplo, news.com) está visitando. Y aunque HTTPS también cifra la información sobre las páginas individuales de un sitio (por ejemplo, website.com/protests) que usted visita, los adversarios sofisticados pueden seguir viendo esta información al inspeccionar su tráfico de internet. Así que con la existencia de HTTPS, un adversario podría saber que usted va a news.com, pero no podría ver su contraseña, y sería más difícil (pero no imposible) para ellos ver que usted está buscando información sobre las protestas (para usar nuestro ejemplo). Esa es una diferencia importante. Compruebe siempre que existe la extensión HTTPS antes de navegar por un sitio web o de introducir información sensible. También puede utilizar la **extensión de navegador HTTPS Everywhere** para asegurarse de utilizar HTTPS en todo momento, o si es usuario de Firefox, activar el **modo solo HTTPS** en el navegador. Si su navegador le avisa de que un sitio web puede ser inseguro, no lo ignore. Algo está mal. Puede ser algo benigno –como que el sitio tenga un certificado de seguridad caducado– o que el sitio haya sido suplantado o falseado maliciosamente. En cualquier caso, es importante tener en cuenta la advertencia y no acceder al sitio. El HTTPS es esencial y el sistema de nombres de dominio cifrado proporciona cierta protección adicional contra el fisgoneo y el bloqueo de sitios, pero si su organización está preocupada por la vigilancia altamente selectiva con respecto a sus actividades en línea y se enfrenta a una sofisticada censura en línea (como el bloqueo de sitios web y aplicaciones), es posible que desee utilizar una red privada virtual (VPN, por sus siglas en inglés) de confianza.



Uso de un DNS Cifrado

Si, teniendo en cuenta su entorno de amenazas, quiere hacer más difícil (pero no imposible) para un ISP que pueda conocer los detalles de los sitios web que visita, puede utilizar un sistema de nombres de dominio (DNS, por sus siglas en inglés) cifrado.

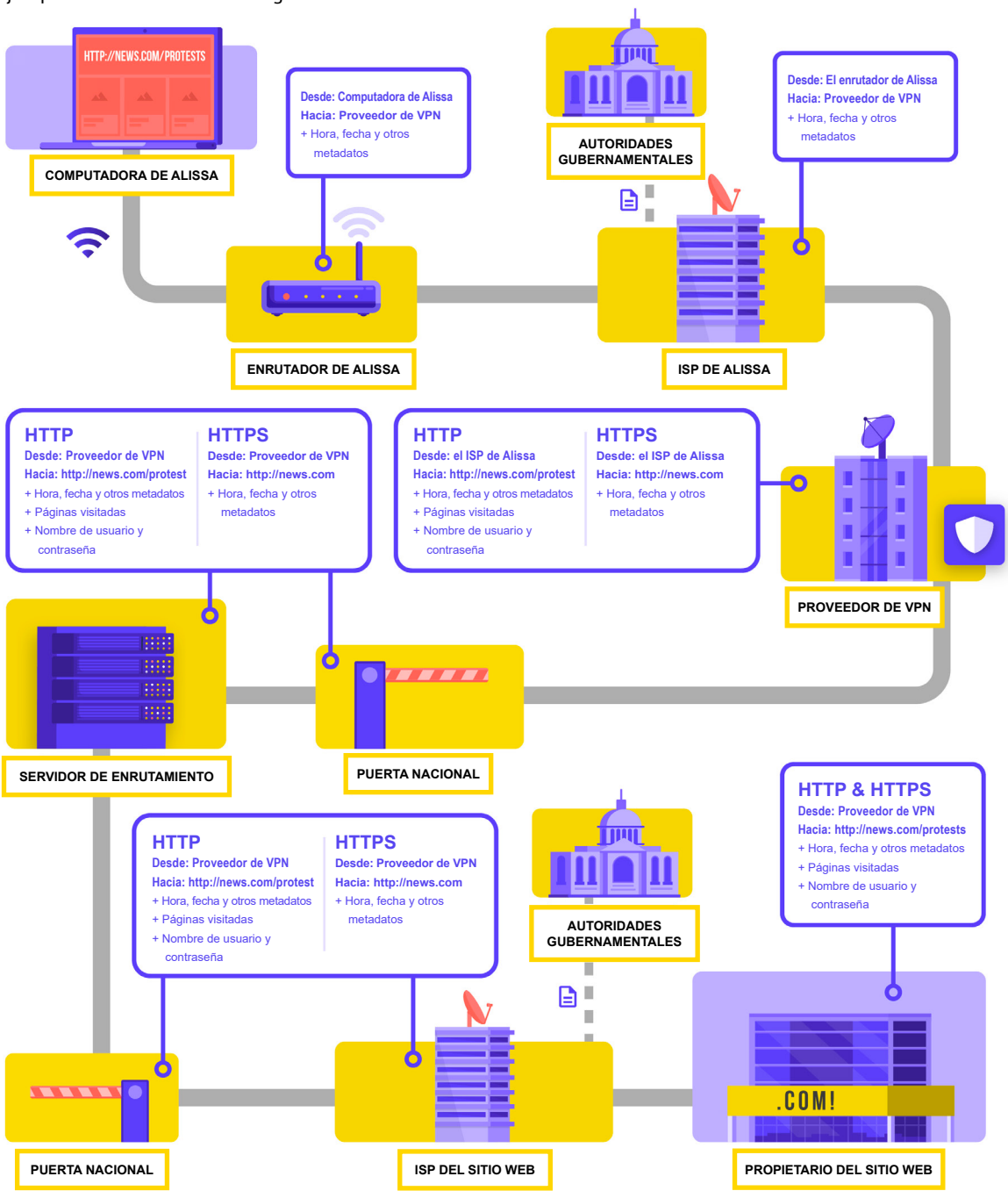
Si se lo **pregunta**, DNS significa Sistema de Nombres de Dominio. El sistema de nombres de dominio es esencialmente la guía telefónica de internet, que traduce los nombres de dominio aptos para las personas (como ndi.org) en direcciones de protocolo de internet (IP, por sus siglas en inglés) aptas para la web. Esto permite a las personas utilizar los navegadores para buscar y cargar fácilmente recursos de internet y visitar sitios web. Sin embargo, el DNS no está cifrado de manera predeterminada.

Para utilizar el DNS cifrado y al mismo tiempo añadir un poco de protección a su tráfico de internet, una opción fácil es descargar y activar **la aplicación 1.1.1.1 de Cloudflare** en su computadora y dispositivo móvil. Existen otras opciones de DNS cifrado, como el 8.8.8.8 de Google, pero requieren **más pasos técnicos** para su configuración. Si utiliza el navegador Firefox, el DNS cifrado está ahora activado de manera predeterminada. Los usuarios de los navegadores Chrome o Edge **pueden activar el DNS cifrado** también a través de la configuración de seguridad avanzada del navegador, activando "usar DNS seguro" y seleccionando "Con: Cloudflare (1.1.1.1)" o el proveedor de su elección.

1.1.1.1 de Cloudflare con WARP cifra su DNS y los datos de navegación, proporcionando un servicio similar a una VPN tradicional. Aunque WARP no protege completamente su ubicación de todos los sitios web que visita, es una función fácil de usar que puede ayudar al personal de su organización a aprovechar el DNS cifrado y la protección adicional de su ISP en situaciones en las que una VPN completa no es funcional o es necesaria dado el contexto de la amenaza. En la configuración avanzada del DNS de 1.1.1.1 con WARP, el personal también puede activar el 1.1.1.1 para Familias a fin de proporcionar una protección adicional contra el malware mientras se accede a internet.

¿QUÉ ES UNA VPN?

Una VPN es esencialmente un túnel que protege contra la vigilancia y el bloqueo de su tráfico de internet por parte de los hackers de su red, su administrador de red y su proveedor de servicios de internet y cualquier persona con la que puedan compartir datos. Este es un ejemplo de cómo se ve la navegación con una VPN:



Adaptado de [How the Internet Works](#) (Cómo funciona internet) del Totem Project (CC-BY-NC-SA)

Para describir las redes privadas virtuales en mayor profundidad, esta sección hace referencia a la [Guía de Autoprotección Digital contra la Vigilancia de EFF]:

Las VPN tradicionales están diseñadas para disfrazar su dirección IP real de la red y crear un túnel cifrado para el tráfico de internet entre su computadora (o teléfono o cualquier dispositivo "inteligente" conectado a la red) y el servidor de la VPN. Dado que el tráfico en el túnel se cifra y se envía a su VPN, es mucho más difícil para terceros (como los ISP o los hackers en la wifi pública) controlar, modificar o bloquear su tráfico. Después de pasar por el túnel desde su ubicación hasta la VPN, el tráfico sale de la VPN hacia su destino final, enmascarando su dirección IP original. Esto ayuda a disfrazar su ubicación física para cualquiera que mire el tráfico después de que abandone la VPN. Esto le ofrece más privacidad y seguridad, pero el uso de una VPN no lo hace a usted completamente anónimo en línea: su tráfico sigue siendo visible para el operador de la VPN. Su ISP también sabrá que está utilizando una VPN, lo que podría aumentar su perfil de riesgo.

Esto significa que **es esencial elegir un proveedor de VPN de confianza**. En algunos lugares como Irán, los gobiernos hostiles han creado sus propias VPN para poder rastrear lo que hacen los ciudadanos. Para encontrar la VPN adecuada para su organización y el personal, puede evaluar las VPN en función de su modelo de negocio y reputación, de los datos que recopilan o no y, por supuesto, de la seguridad de la propia herramienta.

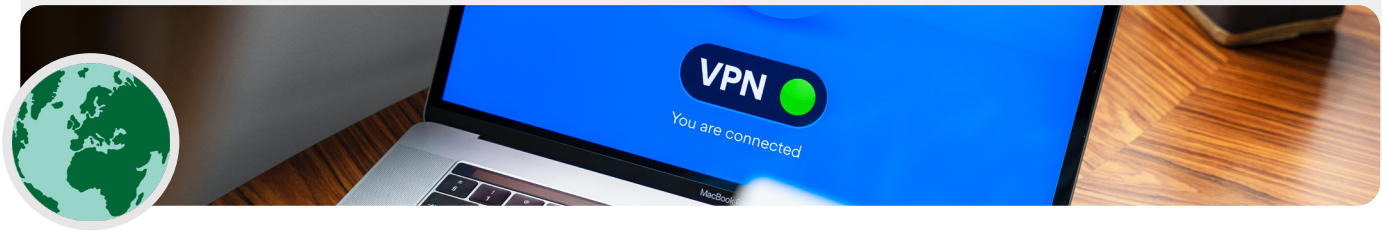
¿Por qué no debería utilizar una VPN gratuita? La respuesta corta es que la mayoría de las VPN gratuitas, incluidas las que vienen preinstaladas en algunos teléfonos inteligentes, vienen con una gran trampa. Al igual que todas las empresas y proveedores de servicios, las VPN tienen que sostenerse de alguna manera. Si la VPN no vende su servicio, ¿cómo mantiene su negocio a flote? ¿Solicita donaciones? ¿Cobra por los servicios premium? ¿Está respaldada por organizaciones benéficas o financiadores? Desafortunadamente, muchas VPN gratuitas ganan dinero recopilando y vendiendo sus datos.

Un proveedor de VPN que no recopila datos en primer lugar es la mejor opción. Si los datos no se recopilan, no pueden venderse ni entregarse a un gobierno si lo solicita. Al examinar la política de privacidad de un proveedor de VPN, compruebe si la VPN realmente recopila datos del usuario. Si no indica explícitamente que los datos de conexión del usuario no se registran, lo más probable es que sí los registre. Aunque una empresa afirme que no registra los datos de conexión, esto no siempre es una garantía de buen comportamiento.

Merece la pena hacer una búsqueda sobre la empresa que está detrás de la VPN. ¿Está avalada por profesionales independientes de la seguridad? ¿Se han escrito artículos sobre la VPN? ¿Se la ha encontrado alguna vez engañando o mintiendo a sus clientes? Si la VPN fue creada por personas conocidas en la comunidad de la seguridad de la información, es más probable que sea de confianza. Sea escéptico con respecto a una VPN que ofrezca un servicio por el que nadie quiera apostar su reputación personal, o que esté dirigida por una empresa que nadie conozca.

Falsas VPN en el Mundo Real

A finales de 2017, tras el aumento de las protestas en el país, [los iraníes comenzaron a descubrir una versión "gratuita" (pero falsa) de una popular VPN que se compartía a través de mensajes de texto]. La VPN gratuita (que en realidad no funcionaba) prometía dar acceso a Telegram, que en ese momento estaba bloqueado a nivel local. Lamentablemente, la aplicación falsa no era más que un malware que permitía a las autoridades rastrear los movimientos y vigilar las comunicaciones de quienes la descargaban.



Entonces, ¿qué VPN debemos utilizar?

Si el uso de una VPN tiene sentido para su organización, un par de opciones de confianza incluyen TunnelBear y ProtonVPN. Otra opción es configurar su propio servidor utilizando Outline de Jigsaw, donde no hay una empresa que gestione su cuenta, usted tiene que configurar su propio servidor. Si su organización es un poco más grande, puede considerar una VPN para empresas que ofrezca funciones de administración de cuentas, como el plan Teams de TunnelBear. Para determinadas organizaciones de la sociedad civil y de los derechos humanos que reúnan los requisitos necesarios, TunnelBear proporciona créditos para el uso gratuito de su VPN (que suele costar unos $3 al mes). Si cree que su organización cumple los requisitos y está interesado, póngase en contacto con cyberhandbook@ndi.org para obtener más información.

Aunque la mayoría de las VPN modernas han mejorado en lo que respecta al rendimiento y la velocidad, conviene tener en cuenta que el uso de una VPN podría reducir la velocidad de navegación si se encuentra en una red con un ancho de banda muy bajo, sufre una alta latencia o retrasos en la red, o experimenta cortes intermitentes de internet. Si está en una red más rápida, debería usar una VPN predeterminada todo el tiempo.

Si recomienda que el personal utilice una VPN, también es importante asegurarse de que la gente mantenga la VPN encendida. Puede parecer obvio, pero una VPN que está instalada pero no funciona no proporciona ninguna protección.



Anonimato a través de Tor

Además de las VPN, es posible que haya oído hablar de Tor como otra herramienta para utilizar internet de forma más segura. Es importante entender qué son ambos, por qué se puede utilizar uno u otro y cómo ambos pueden afectar a su organización.

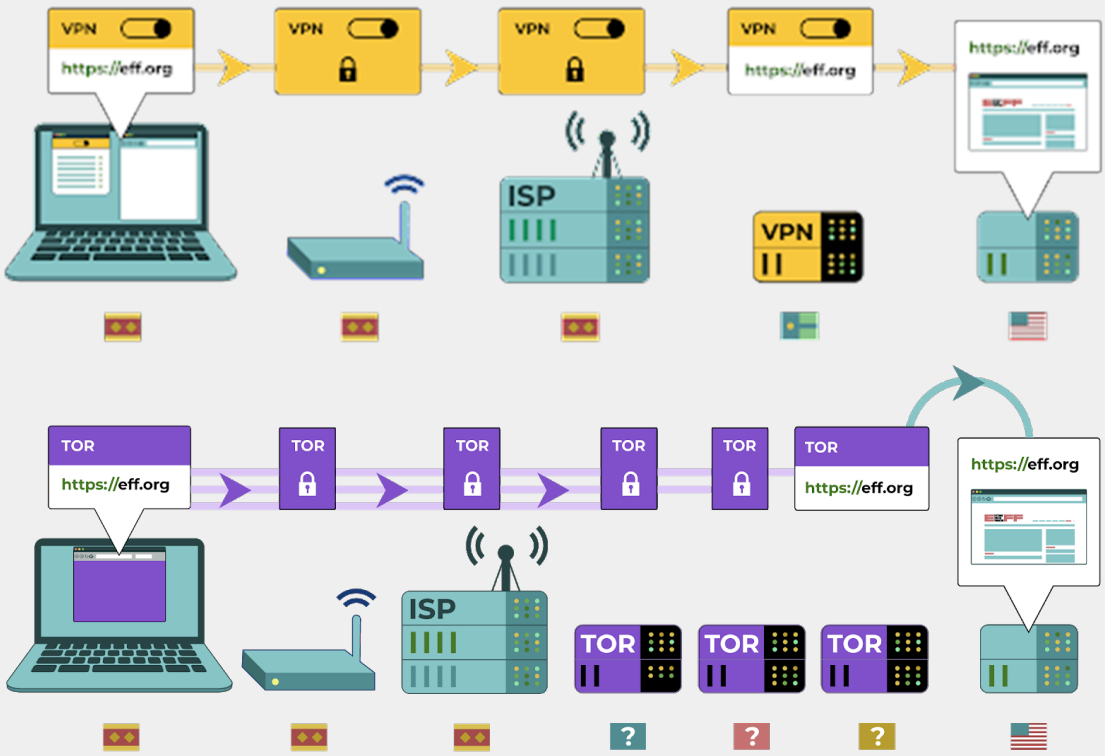
Tor es un protocolo para transmitir datos de forma anónima en internet mediante el enrutamiento de mensajes o datos a través de una red descentralizada. Puede obtener más información sobre cómo funciona Tor aquí, pero en resumen, enruta su tráfico a través de múltiples puntos a lo largo del camino hacia el destino para que ningún punto tenga suficiente información para exponer a la vez quién es usted y qué está haciendo en línea.

Tor es diferente a una VPN en algunos aspectos. Fundamentalmente, se diferencia porque no depende de la confianza de un punto específico (como un proveedor de VPN).

Este gráfico, desarrollado por la EFF, muestra la diferencia entre una VPN tradicional y Tor.

La forma más fácil de usar Tor es a través del navegador web Tor. Funciona como cualquier navegador normal, excepto que dirige su tráfico a través de la red Tor. Puede descargar el Navegador Tor en Windows, Mac, Linux o dispositivos Android. Tenga en cuenta que al usar el Navegador Tor, solo está protegiendo la información a la que accede **mientras está en el navegador**. No proporciona ninguna protección a otras aplicaciones o archivos descargados que pueda abrir por separado en su dispositivo. También tenga en cuenta que Tor no cifra su tráfico, por lo que, al igual que cuando se utiliza una VPN, sigue siendo esencial utilizar las mejores prácticas como HTTPS cuando navega.

Si quiere extender las protecciones de anonimato de Tor a toda su computadora, los usuarios más expertos en tecnología pueden instalar Tor como una conexión a internet en todo el sistema, o considerar el uso del sistema operativo Tails, que enruta todo el tráfico a través de Tor de manera predeterminada. Los usuarios de Android también pueden utilizar la aplicación Orbot para ejecutar Tor con todo el tráfico de internet y las aplicaciones de su dispositivo. Independientemente de cómo utilice Tor, es importante saber que cuando lo usa, su proveedor de servicios de internet no puede ver qué sitios web está visitando, pero *puede* ver que está utilizando Tor.



Al igual que cuando se utiliza una VPN, esto podría elevar el perfil de riesgo de su organización considerablemente, porque Tor no es una herramienta muy común y, por lo tanto, se destaca para los adversarios que pueden estar monitoreando su tráfico de internet.

Entonces, ¿debería su organización usar Tor? La respuesta es: depende. Para la mayoría de las organizaciones en riesgo, una VPN de confianza que sea utilizada adecuadamente por todo el personal en todo momento es lo más fácil, lo más práctico y, en la era del mayor uso de VPN a nivel mundial, es menos probable que surjan señales de peligro. Sin embargo, si no puede disponer de una VPN de confianza o si opera en un entorno en el que las VPN se bloquean habitualmente, Tor puede ser una buena opción para limitar el impacto de la vigilancia y evitar la censura en línea.

¿Hay alguna razón por la que no debamos usar una VPN o Tor?

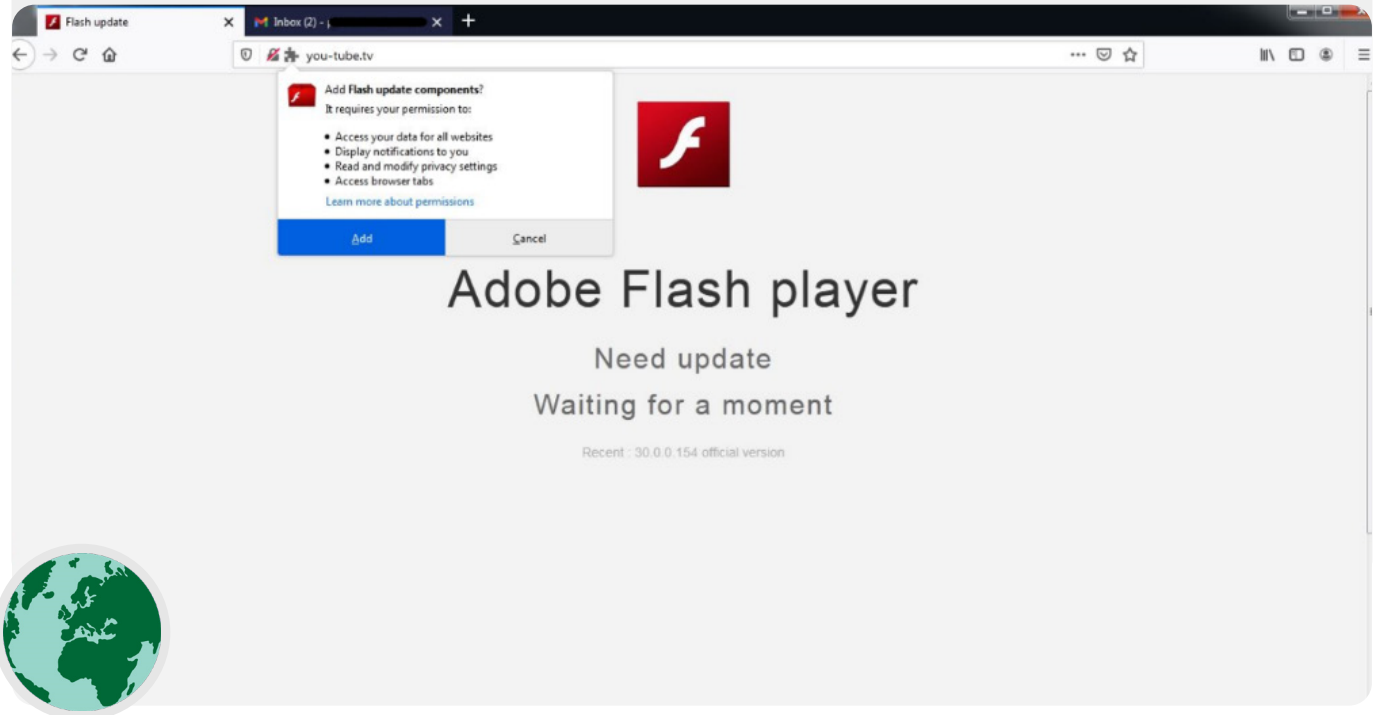
Aparte de las preocupaciones en torno a los servicios VPN de escasa reputación, lo más importante a tener en cuenta es si el uso de una VPN o Tor puede atraer atención no deseada o, en algunas jurisdicciones, ir en contra de la ley. Aunque su ISP no sabrá qué sitios está visitando mientras usa estos servicios, puede ver que está conectado a Tor o a una VPN. Así que si eso es ilegal donde su organización opera o podría atraer más atención o riesgo que simplemente navegar por la web con HTTPS estándar y DNS cifrado, tal vez una VPN o especialmente Tor (que es mucho menos comúnmente utilizado y, por lo tanto, una mayor "señal de alerta") no es la opción correcta para su organización. Sin embargo, a medida que el uso de la VPN se hace más común, este es un factor menos distintivo. Tener una VPN encendida todo el tiempo es la mejor opción si es legal y posible.

¿QUÉ NAVEGADOR DEBEMOS UTILIZAR?

Utilice un navegador de confianza, como Chrome, Firefox, Brave, Safari, Edge o el Navegador Tor. Tanto Chrome como Firefox son muy utilizados y hacen un buen trabajo con la seguridad. Algunas personas prefieren Firefox por su enfoque de privacidad. En cualquier caso, es importante que los reinicie y que reinicie la computadora con relativa frecuencia para mantener su navegador actualizado. Si le interesa comparar las características de los navegadores, consulte este recurso de la Freedom of the Press Foundation. Independientemente del navegador, también es una buena idea utilizar una extensión o complemento, como Privacy Badger, uBlock Origin o Privacy Essentials de DuckDuckGo, que impide que los anunciantes y otros rastreadores de terceros sepan adónde va y qué sitios visita. Y cuando navegue por internet, considere la posibilidad de cambiar sus búsquedas web predeterminadas de Google a DuckDuckGo, Startpage u otro motor de búsqueda que proteja la privacidad. Este cambio ayudará a limitar también a los anunciantes y rastreadores de terceros.

Seguridad de los Navegadores en el Mundo Real

Los activistas de la sociedad civil tibetana fueron atacados a principios de 2021 con un complemento del navegador malicioso inteligentemente diseñado, que robó su correo electrónico y datos de navegación. El complemento, denominado "Componentes de actualización de Flash", se presentaba a los usuarios que visitaban sitios web vinculados a correos electrónicos de suplantación de identidad. Estos ataques a las extensiones o complementos del navegador pueden ser tan dañinos como el malware compartido directamente a través de descargas de phishing u otro software.



Seguridad en las Redes Sociales

Su organización puede revelar mucho (y a veces más de lo que desea) al publicar y comentar en las redes sociales.

Ya sea en Facebook, Twitter, Instagram, YouTube o en sitios de redes sociales específicos de una región, como VKontakte y Odnoklassniki, siempre hay que pensar bien lo que se publica y configurar adecuadamente las opciones de privacidad que puedan estar disponibles. Esto es válido no solo para las páginas oficiales de su organización, sino también, en algunos casos, para las cuentas personales del personal y las de sus familiares y amigos.

Seguridad en las Redes Sociales y Sociedad Civil

Incluso las organizaciones de bajo riesgo pueden ser objeto de ataques y acoso en las redes sociales si no se aplican políticas de seguridad adecuadas. En este ejemplo de 2018, un refugio de animales sin fines de lucro perdió miles de dólares y se alejó de sus partidarios después de que un administrador de cuentas no autorizado creara una campaña de recaudación de fondos falsa, y aparecieran en la plataforma cuentas falsas que se hacían pasar por empleados. Si los hackers son capaces de llegar a esos extremos para sacar unos cuantos miles de dólares a un refugio de animales, puede imaginarse el daño que podrían infligir adversarios sofisticados si consiguieran acceder a las cuentas de su organización o se hicieran pasar por usted en línea. Además de la piratería de cuentas, los grupos de la sociedad civil y los usuarios individuales de muchos países también se enfrentan a repercusiones por los contenidos publicados en las redes sociales. En un ejemplo de Zambia de 2020, la policía detuvo a un estudiante de 15 años por haber difamado supuestamente al presidente en una publicación de Facebook. El adolescente, que realizó la publicación bajo un seudónimo, fue identificado por el número de teléfono utilizado para registrar la cuenta y su dirección de protocolo de internet (IP).



DESARROLLE UNA POLÍTICA DE REDES SOCIALES DE LA ORGANIZACIÓN

Asuma que todo lo que se publique en las redes sociales puede llegar a ser de dominio público, y elabore una política organizativa acorde para las redes sociales. Esta política debe responder a preguntas como: ¿Quién tiene acceso a sus cuentas de redes sociales? ¿Quién puede publicar y quién debe aprobar las publicaciones? ¿Qué información debe/no debe compartirse en las redes sociales? Si publica fotos, información sobre la ubicación u otros datos identificativos de su personal, socios o asistentes al evento; ¿les ha pedido su permiso y ha considerado los riesgos? Además de desarrollar su política y dejarla clara para el personal, asegúrese de configurar adecuadamente los parámetros de privacidad y seguridad (a menudo denominados "protección"). Algunas de las preguntas clave que debe hacerse para decidir qué configuraciones de privacidad y seguridad tienen más sentido para sus cuentas personales y de la organización son:

- ¿Quiere compartir sus publicaciones con el público, o solo con un grupo específico de personas a nivel interno o externo?
- ¿Debe alguien poder comentar, responder o interactuar con sus mensajes o publicaciones?
- ¿Debe la gente poder encontrarlo a usted o a su organización utilizando su dirección de correo electrónico o su número de teléfono (personal o profesional)?
- ¿Quiere que su ubicación se comparta automáticamente al realizar una publicación?
- ¿Quiere bloquear o silenciar cuentas hostiles?
- ¿Quiere bloquear palabras o hashtags específicos?

Cada sitio de redes sociales tendrá una configuración de privacidad y seguridad diferente, pero estos conceptos generales se aplican universalmente. Mientras considera estas cuestiones, aproveche las útiles guías de privacidad de las principales plataformas: **Facebook**, **Twitter**, **Instagram** y **YouTube**. En el caso de Facebook en particular, tenga cuidado con sus opciones de privacidad con respecto a Groups. Facebook Groups es un lugar popular para la participación, la defensa y el intercambio de información, pero cualquiera puede unirse a los grupos sin restricciones. No es raro que las cuentas "falsas" se hagan pasar por personas reales para intentar infiltrarse en grupos o páginas privadas de las redes sociales. Así que acepte las solicitudes de "amistad" y "seguimiento" con cuidado. Recuerde que las cuentas de redes sociales de su organización son tan seguras como las cuentas que están "vinculadas" a ella. Esto es especialmente importante de recordar en el caso de Facebook, donde la página de su organización puede ser administrada por la cuenta personal vinculada de alguien.

ACOSO EN LÍNEA

Por desgracia, muchas organizaciones se enfrentan a un importante acoso en línea, especialmente en las redes sociales. Este acoso **suele dirigirse con mayor intensidad a las mujeres y a las poblaciones marginadas.** La violencia en línea contra las mujeres, en particular, puede crear un entorno hostil que lleva a la autocensura o a la retirada del discurso político o cívico. Como se identificó en el informe **Tweets that Chill** del equipo del NDI, cuando los ataques contra las mujeres políticamente activas se canalizan en línea, el alcance expansivo de los medios sociales puede magnificar el efecto del acoso y el abuso psicológico, socavando la sensación de seguridad personal de las mujeres de maneras que no experimentan los hombres.

A medida que su organización desarrolla su política de redes sociales, es importante ser consciente de esta dinámica. Incluya en su plan de seguridad un apoyo estructurado para el personal que se enfrenta a mensajes negativos, insultos y amenazas en las redes sociales (como parte de su trabajo y en su vida personal). Desarrolle una infraestructura contra el acoso dentro de su organización, que incluya una encuesta a su personal para entender cómo les afecta el acoso en línea y cree un equipo de respuesta rápida para ayudar al personal a enfrentarse a situaciones difíciles. El **Manual de Campo contra el Acoso en Línea** de PEN América también ofrece recomendaciones detalladas sobre cómo puede apoyar al personal que se enfrenta a este tipo de acoso. Si su personal se siente cómodo, usted puede considerar la posibilidad de que puedan **denunciar incidentes** de acoso o cuentas problemáticas directamente en las plataformas.

Cuando se trata de personal que ha sido víctima de acoso en línea (y también de forma física), es importante ser sensible. Tal y como se indica en el programa de derechos de la mujer **¡Dominemos la tecnología!** de la Asociación para el Progreso de las Comunicaciones, hay que entender que una sobreviviente del hecho puede estar lidiando con un trauma, y reconocer que la violencia (en línea o fuera de ella) nunca es culpa de la víctima. Garantice que estas cuestiones puedan plantearse y discutirse (si el personal se siente cómodo haciéndolo) en un entorno confidencial y seguro, con la opción del anonimato. E incluya en el plan de seguridad de su organización una lista de profesionales locales, organizaciones y cuerpos de seguridad con los que pueda poner en contacto al personal para obtener asistencia legal, médica, de salud mental y técnica en caso de ser necesario. Para obtener más ideas, consulte la **Guía de Seguridad en Línea** de Feminist Frequency.

Mantenga sus Sitios Web en Línea

Además de proteger su capacidad de acceso a internet de forma segura, también es importante hacer lo posible para garantizar que otros puedan acceder a los sitios o propiedades web de su organización.

En el caso de las páginas de las redes sociales, esto significa proteger esas cuentas con contraseñas fuertes y únicas y una autenticación de dos factores. Para su sitio web, esto significa protegerlo contra la piratería y los ataques de denegación de servicio. Los ataques de denegación de servicio distribuido (DDoS, por sus siglas en inglés) consisten en que un gran grupo de computadoras sobrecargue simultáneamente su servidor con tráfico malicioso. Si usted es una organización de la sociedad civil u otra organización sin fines de lucro, lo más probable es que pueda optar por una protección DDoS gratuita (que dificulta considerablemente que un adversario derribe su sitio web) a través del Proyecto Galileo de Cloudflare, el Proyecto Shield de Google o el servicio Deflect de eQualitie.



Alojar el Sitio Web de su Organización de Forma Segura

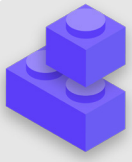
Los sitios web se alojan en computadoras, y éstas son vulnerables a la piratería informática, al igual que sus dispositivos. Si es posible, su organización debería aprovechar los servicios de alojamiento existentes, como Wordpress.com, Wix u otros, que gestionan toda la seguridad del sitio. Si está leyendo este manual, es probable que su organización también reúna los requisitos para el alojamiento seguro y gratuito de un sitio Wordpress por parte de eQualitie a través de su servicio de alojamiento eQPress. Esta es una buena opción para las organizaciones civiles con sitios Wordpress existentes o si su organización está buscando construir un sitio nuevo. Si necesita alojar su sitio web usted mismo, asegúrese de mantener el sistema operativo y el software de alojamiento web actualizados, al igual que lo haría con su computadora personal. Considere la posibilidad de utilizar proveedores de alojamiento en la nube bien establecidos, como Amazon Web Services (AWS), Microsoft Azure o Eclips.is de Greenhost, que ofrecen opciones de seguridad mejoradas para los sitios web alojados. Y, por supuesto, independientemente de las herramientas que utilice para alojar su sitio web, asegúrese de que todas las cuentas utilizadas para acceder a la edición de contenidos y a los ajustes de configuración estén protegidas con contraseñas seguras y una autenticación de dos factores.

Si su organización tiene los conocimientos técnicos necesarios para alojar su propio sitio web, también debería considerar la posibilidad de elegir un sitio web denominado "estático" o plano. A diferencia de los sitios web dinámicos, este tipo de sitios reduce la superficie de ataque para los hackers y hará que su sitio web sea más resistente a los ataques.

Proteja su Red Wifi

Todas estas medidas para proteger el tráfico web de la vigilancia y la censura son importantes, pero no sustituyen a la seguridad básica de la red en la oficina (y en casa).

No se olvide de lo más básico, como utilizar una contraseña fuerte (no la contraseña predeterminada) en su enrutador wifi, asegurarse de que solo los usuarios autorizados tengan acceso a su red cambiando frecuentemente la contraseña, y activar el cortafuegos integrado de sus enrutadores inalámbricos. Considere también la posibilidad de crear una red para invitados en su oficina si tiene visitantes que entran y salen del edificio y utilizan internet.



Mantenerse seguro en internet

- **Lleve a cabo una capacitación periódica para el personal sobre la importancia de seguir las medidas básicas de seguridad en la web.**
- **Recuerde al personal que debe navegar siempre con HTTPS y DNS cifrado.**
- **Exija al personal que reinicie regularmente sus navegadores para instalar las actualizaciones.**
- **Fomente el uso de navegadores y extensiones que protejan la privacidad.**
- **Si una VPN es apropiada dado el contexto de su organización, elija una VPN de buena reputación, capacite al personal en su uso y asegúrese de que se utilice de forma consistente.**
- **Desarrolle y distribuya una política organizativa clara sobre el uso de las redes sociales. o Habilite la configuración de privacidad y seguridad en todas las cuentas de las redes sociales.**
- **Comprenda las repercusiones del acoso en línea y esté preparado para apoyar al personal afectado.**
- **Elabore una lista de profesionales, organizaciones y cuerpos de seguridad locales con los que pueda poner en contacto al personal para obtener asistencia jurídica, de salud mental y técnica en respuesta al acoso en línea.**
- **Contrate una protección DDoS para sus sitios web.**
- **Utilice un proveedor de alojamiento web de confianza.**
- **Utilice una contraseña fuerte y una red de invitados para el wifi de su oficina.**



Proteger la seguridad física

Es esencial mantener sus dispositivos físicamente seguros. Pero la seguridad física va más allá de los dispositivos, y debe incluir estrategias para proteger todo lo demás en su mundo: los documentos en papel, la oficina de su organización o los espacios de trabajo y, por supuesto, usted, su personal y los voluntarios.

Vigilancia, Censura y Sociedad Civil

Los ataques físicos a las organizaciones de la sociedad civil son, desgraciadamente, algo habitual, y suelen tener importantes implicaciones para la seguridad tanto física como de la información. Una táctica habitual de los adversarios para suprimir la actividad de las CSO es el allanamiento y cierre de oficinas, tanto para intimidar al personal como, en algunos casos, para robar o confiscar información y equipos tecnológicos. Estas amenazas suelen dirigirse a los grupos de minorías y de derechos humanos y a las CSO que operan en el espacio de la democracia y la gobernabilidad. Por ejemplo, las oficinas de LGBT+ Rights Ghana, una organización civil que a principios de 2021 abrió el primer centro comunitario del país para la comunidad local LGBTQI+, fueron amenazadas con ser quemadas, y finalmente fueron allanadas y cerradas por la policía. Estos ataques no solo afectan a las operaciones físicas de una organización, sino que también pueden dañar la sensación de seguridad del personal.



Protección de los Activos Físicos

Un componente esencial de la seguridad de la información es la seguridad física de sus dispositivos.

Además de mitigar el impacto de un dispositivo robado mediante el uso de pantallas de bloqueo y contraseñas, la implementación del cifrado completo del disco y la activación de las funciones de borrado remoto, también debe considerar cómo evitar que esos dispositivos sean robados en primer lugar. Para dificultar los robos, asegúrese de instalar cerraduras fuertes (y cambiarlas cada vez que se desvincule un miembro del personal) en la oficina o en casa. Considere también la posibilidad de comprar una caja fuerte para computadoras portátiles o un armario con cerradura para mantener los dispositivos más protegidos durante la noche. Las cámaras de seguridad se han abaratado mucho, y las versiones sencillas diseñadas para uso doméstico son las más disponibles. Estos sistemas de cámaras o sensores de movimiento alrededor de las instalaciones pueden detectar y, con suerte, disuadir los robos físicos. Busque una opción que respete la privacidad disponible en su país, y asegúrese de seleccionar cámaras proporcionadas por empresas de confianza que no tengan un incentivo para entregar datos e información a un adversario potencial.

Si el riesgo de robo o allanamiento de la oficina es alto, mantenga los datos más sensibles de la organización fuera de la oficina, ya sea almacenándolos de forma segura en la nube (como se indicó anteriormente) o trasladándolos físicamente a un lugar menos peligroso. Si los dispositivos antiguos aún tienen información almacenada pero ya no se utiliza, considere la posibilidad de borrarla: esta guía de WireCutter es un buen recurso sobre cómo hacerlo para la mayoría de los dispositivos modernos. Si no es posible borrar sus dispositivos, también puede destruirlos físicamente. La forma más fácil, aunque no la más respetuosa con el medioambiente, es romper los dispositivos y sus discos duros con un martillo. A veces, las soluciones más antiguas siguen siendo las mejores. Incluso antes de estos pasos técnicos, tómese un momento para crear un inventario de todos los equipos de la organización. Si no tiene una lista de todos sus dispositivos, es más difícil hacer un seguimiento de lo que puede faltar si le roban uno.



Cómo instalar su propio sistema de seguridad en la oficina

Si un sistema de seguridad completo para la oficina está fuera del presupuesto de su organización y le preocupa especialmente la privacidad, puede probar una opción creativa como la aplicación Haven de Guardian Project para notificar posibles intrusiones en la oficina. Haven es una aplicación para teléfonos inteligentes que puede convertir cualquier teléfono Android en un detector de movimiento, sonido, vibración y luz. Puede configurar la aplicación en unos pocos dispositivos Android baratos en diferentes puntos de la oficina para notificar y registrar cualquier invitado inesperado e intruso no deseado. La aplicación Haven también puede ser útil para instalarla en una habitación de hotel o en un apartamento si usted corre un mayor riesgo. Lo mejor es un sistema de seguridad completo, pero si eso está fuera de su alcance y quiere saber más sobre cómo utilizar la aplicación Haven, puede visitar el sitio web del proyecto.

¿QUÉ HACEMOS CON TODO ESTE PAPEL?

Es probable que su organización tenga mucha información impresa en papel, escrita en cuadernos o garabateada en notas adhesivas. Parte de dicha información puede ser muy sensible: impresiones de presupuestos, listas de participantes, cartas confidenciales de donantes y notas de reuniones privadas. Es esencial pensar también en la seguridad de esta información. Si es absolutamente necesario conservar copias impresas de la información sensible, asegúrese de que se guardan en un armario cerrado con llave o en otro lugar seguro. No guarde ninguna información privada o sensible (incluidas las contraseñas) en un escritorio o escrita en una pizarra. Si cree que su organización corre un alto riesgo de sufrir un robo o saqueo, guarde la información altamente sensible en un lugar que no sea un blanco fácil. En la medida de lo posible, procure eliminar la información impresa innecesaria. Recuerde: si no la tiene, no se la pueden robar. Establezca una política organizacional en relación con la propiedad de las notas en papel y asegúrese de recoger las notas en papel del personal si éste decide desvincularse o es despedido de la organización (al igual que recogería una computadora o un teléfono de la organización). Para deshacerse de documentos confidenciales, compre una trituradora de calidad. Una actividad divertida de fin de semana puede ser tomarse un descanso de 15 minutos con el personal para destruir los restos de impresiones o notas con información sensible de la semana anterior.

LA POLÍTICA DE LA OFICINA

Aunque para muchos las realidades de "la oficina" han cambiado significativamente desde el comienzo de la pandemia de COVID-19, sigue siendo importante que su organización establezca una política clara respecto del acceso a la oficina. Esta política debe abordar cuestiones clave, como quién puede entrar en la oficina (y cuándo), quién puede acceder a qué recursos de la oficina (como la red wifi) y qué hacer con las visitas.

Una pregunta sencilla, pero importante, es quién tiene la llave de la oficina. Solo el personal de confianza debe tener llaves, y las cerraduras deben cambiarse cuando el personal se vaya o de forma semirregular. Durante el día, cualquier puerta que se deje sin cerrar debe estar a la vista de alguien de confianza en la organización. Considere también si la organización tiene una relación de confianza con el propietario o el personal de limpieza. Piense en la información o los dispositivos a los que estas personas podrían tener acceso y asegúrese de que estén protegidos, especialmente si no tiene esa relación de confianza. Sea cual fuere el acceso, siempre se debe designar a alguien de confianza para que cierre la oficina y se asegure de que los dispositivos estén bien protegidos antes de partir al final del día.

¿Se permite la entrada de invitados a la oficina? Si es así, asegúrese de que no tengan acceso (o, al menos, acceso desatendido) a los dispositivos ni a los datos sensibles en papel. Si es un requisito o una expectativa que los invitados tengan acceso a internet cuando hagan una visita, debe configurar una red de "invitados" para que dichos invitados no tengan la capacidad de monitorear su tráfico regular. En general, solo el personal de confianza debe poder acceder a la red y a los dispositivos de red, como las impresoras. También suele ser una buena idea exigir el registro de los invitados para tener un registro de quiénes lo han visitado.

A la hora de desarrollar una política de oficina, el objetivo debe ser permitir que solo las personas de confianza accedan a los dispositivos, documentos, espacios y sistemas sensibles.

APOYO AL PERSONAL Y A LOS VOLUNTARIOS

Las amenazas a la seguridad física de su organización también pueden afectar a su personal. Al igual que el acoso en las redes sociales, estas amenazas a la seguridad física suelen afectar de forma desproporcionada a las mujeres y a las comunidades marginadas. No se trata solo de ventanas rotas y computadoras portátiles robadas. La intimidación, las amenazas o los casos de violencia física o sexual, el maltrato doméstico y el miedo a los ataques pueden tener un grave impacto negativo en la vida del personal. Para las organizaciones que trabajan o apoyan a las mujeres políticamente activas en particular, la herramienta de planificación de la seguridad **#Think10** del NDI es un recurso útil para proporcionar a las personas que podrían estar en mayor riesgo personal como resultado de su actividad.

El bienestar del personal es obviamente un activo importante para ellos como individuos, pero también es un elemento crucial para una organización saludable y que funcione bien. Para ello, considere qué recursos adicionales puede proporcionar al personal para mantenerlo protegido y, en caso de ataque físico o digital, ayudarlo a recuperarse. Como se ha mencionado anteriormente en el Manual, esto significa, como mínimo, elaborar una lista de recursos a los que puede poner en contacto con el personal para obtener asistencia jurídica, médica, de salud mental y técnica, si es necesario. Una vez más, el **Manual de Campo contra el Acoso en Línea** de PEN América incluye ideas sobre cómo las organizaciones pueden apoyar al personal durante y después de las crisis, y el **Manual de Seguridad Holística** de Tactical Tech incluye contenido relevante sobre cómo las organizaciones suelen responder en momentos de amenaza intensa.

SEGURIDAD EN LOS VIAJES

Viajar (a otro país o a la ciudad de al lado) suele intensificar los riesgos de seguridad de la información física. En general, es seguro asumir que usted y sus dispositivos no tienen derechos de privacidad cuando cruzan las fronteras. Por ello, es una buena idea incluir una política de viajes de la organización dentro de su plan de seguridad que incluya recordatorios sobre las mejores prácticas de seguridad clave. La política de viajes de su organización debe incluir mucha de la información que se trata en otras secciones del Manual, incluidos el uso seguro de internet y el mantenimiento de los dispositivos y otras fuentes de información físicamente seguros y con usted en todo momento cuando viaja. Si es posible, deje su información sensible y simplemente utilice una computadora nueva y con contenido borrado, acceda a los archivos que necesite desde la nube, y luego bórrelos al regresar a casa.

Además de prepararse para viajar y minimizar los datos compartidos cuando viaja, hay algunos consejos operativos esenciales que se deben considerar e incluir en la política de viajes de la organización.

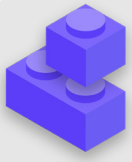
Considere la posibilidad de utilizar computadoras portátiles o teléfonos específicos para viajes, en los que se almacenen pocos o ningún dato sensible. Si la mayor parte del trabajo de su organización se realiza en la nube, una Chromebook relativamente asequible puede ser una buena opción para un dispositivo de este tipo. Restablezca la configuración de fábrica, o haga un borrado de datos, a su regreso antes de conectarse a redes wifi comunes en casa o en la oficina. Prepare al personal para saber qué hacer si es interrogado por las autoridades o detenido en un paso fronterizo. Considere cómo puede limitar la cantidad de información con la que alguien viaja si esto representa una preocupación, y cree protocolos de registro para el personal que viaja a regiones sensibles. Proporcione al personal información de contacto y un plan de acción sobre lo que deben hacer si algo sale mal en su viaje. Esto incluye información sobre hospitales, clínicas o farmacias locales en caso de que necesiten asistencia médica durante el viaje.

El personal también debe mantener todos los dispositivos consigo mientras viaja. Por ejemplo, mantenga la computadora portátil a sus pies (no en el compartimento superior ni en el equipaje despachado) cuando viaje en autobús, tren o avión. No asuma que una habitación de hotel (o la caja fuerte del hotel) es un "lugar seguro" para guardar dispositivos y objetos delicados. Y no confíe en los puertos de carga USB públicos. Los puertos de carga USB de aeropuertos, estaciones y vehículos se están convirtiendo en algo cada vez más habitual, y en una forma muy cómoda de fuente de alimentación para los dispositivos. Pero pueden ser un vector fácil para captar malware. Así que asegúrese de cargar los dispositivos de la manera tradicional a través de un enchufe en la pared, o compre **bloqueadores de datos USB** para que el personal que viaja pueda cargar sus dispositivos de forma segura a través de USB.



Reserva segura de los viajes para su organización

Cuando elabore una política de viajes, también tenga en cuenta la información que puede quedar expuesta cuando organice o reserve un viaje. Esto puede ser especialmente importante si se organizan grandes eventos, capacitaciones o conferencias en las que se maneja información sensible de diversos empleados, socios o asistentes. Piense detenidamente en cómo compartirá y almacenará de forma segura (si es necesario) información personal, como datos del pasaporte, itinerarios de viaje e historiales médicos. El Organizer Activity Book (Libro de actividades del organizador) de Tactical Tech tiene una excelente planilla de trabajo para ayudar a su organización a pensar en las cuestiones clave relacionadas con la seguridad de los viajes, **cuyo enlace está aquí**.



Proteger la seguridad física

- **Recuerde al personal que debe mantener los dispositivos protegidos físicamente en todo momento.**
- **Compruebe y asegure todas las vías de acceso a su espacio: puertas y ventanas.**
- **Desarrolle una política de invitados y acceso a la oficina.**
- **Utilice cerraduras fuertes, y rótelas/cámbielas cuando sea necesario.**
- **Considere la posibilidad de instalar una cámara u otro sistema de seguridad en la oficina.**
- **Tenga y utilice una trituradora de papel.**
  - Establezca un tiempo exclusivo para que el personal elimine los documentos impresos que contienen información sensible.
- **Elabore una lista de profesionales, organizaciones y cuerpos de seguridad locales con los que pueda poner en contacto al personal para obtener asistencia jurídica, médica y de salud mental en respuesta al acoso en línea.**
- **Desarrolle una política de viajes de la organización.**
- **Asegúrese de que el personal sepa qué hacer en caso de una emergencia durante el viaje, incluida la preparación del personal para saber qué hacer si es detenido en una frontera o un puesto de control.**
- **Antes de cualquier viaje local, nacional o internacional, recuerde al personal que debe limitar la información almacenada en los dispositivos.**
- **Tenga en cuenta los datos adicionales que se crean y comparten al organizar viajes o eventos.**



Qué hacer cuando las cosas van mal

Así que, ya sabe lo que hay que hacer. Ha puesto en marcha las políticas y ha capacitado a todos los miembros de la organización en las mejores prácticas. Incluso con todo este trabajo duro, es muy probable que algo salga mal.

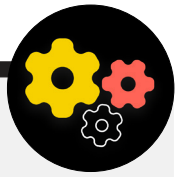
Las cosas pasan. Cuando esto sucede, es esencial contar con un plan de respuesta ante incidentes. La respuesta a los incidentes es una parte fundamental, y a menudo infravalorada, del plan de seguridad de su organización porque puede ser la diferencia entre que un ataque destruya la reputación de su organización o que sea un desagradable bache en el camino. Recuerde que solo puede responder a un incidente si sabe cómo hacerlo. Es muy importante tener una sólida cultura de seguridad en la organización y animar al personal a informar los problemas. Por eso, es mejor premiar el buen comportamiento en materia de seguridad que castigar las fallos o errores de seguridad. También es importante expresar empatía y comprobar el bienestar del personal cuando éste informa un incidente. Quiere que el personal denuncie inmediatamente si hace clic en un enlace de phishing, un teléfono robado o una cuenta de redes sociales pirateada, y no que dude por miedo a las represalias o a la falta de apoyo. Después de todo, la respuesta a incidentes, al igual que las estrategias de mitigación mencionadas en otras secciones del Manual, es un esfuerzo de toda la organización.

- Entonces, ¿qué debe planificar? En resumen, cualquier cosa que tenga cierta probabilidad de ocurrir. Esto será diferente para cada organización, pero las preguntas comunes que un plan de respuesta a incidentes ayudará a responder incluyen:
- ¿Qué hacemos si nuestras cuentas o sitios web son pirateados?
- ¿Qué hacemos si alguien hace clic en un correo electrónico de phishing o si un dispositivo actúa de forma sospechosa?
- ¿Qué hacemos si nos roban y filtran nuestros correos electrónicos o documentos más sensibles?
- ¿Qué hacemos si uno de nuestros empleados corre peligro físico o es detenido? ¿O si están luchando contra el estrés y la ansiedad debido a esas amenazas?
- ¿Qué hacemos si nuestra oficina resulta dañada por un incendio, una inundación o una catástrofe natural?
- ¿Qué hacemos si un empleado pierde o le roban la computadora o el teléfono?

Las respuestas a estas y otras preguntas variarán según la organización, pero es importante que las analicen juntos y que articulen y compartan claramente un plan para que todos los miembros de la organización estén preparados para actuar inmediatamente y limitar los daños.

Según la Guía de Seguridad Holística de Tactical Tech, un buen punto de partida para un plan de respuesta a incidentes es definir un incidente o una emergencia en el contexto de su organización. Decidan qué es una "emergencia", es decir, el momento en que debemos empezar a aplicar las acciones y medidas de contingencia previstas. Esto es importante, ya que a veces no estará claro. Si imagina un escenario como la pérdida de contacto con un colega en una misión de campo, ¿cuánto tiempo esperaría antes de declarar una emergencia? Uno no quiere alarmarse demasiado pronto, pero esperar demasiado puede ser desastroso en algunas circunstancias. También es importante pensar en los pasos de **las operaciones**. Asigne a cada persona una función clara que conozca y haya aceptado de antemano: esto reducirá la desorganización y el pánico en caso de incidente. En el caso de cada amenaza, considere las diferentes funciones que puede tener que asumir y los aspectos prácticos que implica la respuesta a una emergencia. Dentro de esta importante estrategia para las emergencias, se encuentra la activación de una red de apoyo: una amplia red de aliados, que puede incluir amigos y familiares, la comunidad, aliados locales, recursos gubernamentales y aliados nacionales o internacionales, como las ONG y los periodistas. ¿Cómo pueden apoyarlo sus aliados? ¿Debe ponerse en contacto con ellos de antemano para verificar que estarán dispuestos a ayudarlo en caso de emergencia y hacerles saber lo que espera de ellos?

Cuando se responde a un incidente, las **comunicaciones** eficaces son cada vez más importantes. Decida cuál es el medio más seguro y eficaz para comunicarse con cada participante en diferentes escenarios e identifique también un medio de copia de seguridad. Tenga en cuenta que, en caso de emergencia, puede ser útil disponer de pautas claras sobre lo que se debe (y lo que no se debe) comunicar, cuándo se debe comunicar, qué canales utilizar para comunicarse y con quién se debe comunicar. Considere también el impacto de un incidente en la reputación de su organización y prepárese para responder en consecuencia. Asegúrese de que el responsable de comunicaciones de la organización (en algunas organizaciones, puede ser simplemente quien administre la página de Facebook o la cuenta de Twitter) esté al tanto del incidente y pueda vigilar las redes sociales u otros medios de comunicación en busca de posibles repercusiones. El responsable de comunicaciones de la organización también debe estar preparado para responder a posibles preguntas del público o de los medios de comunicación sobre un incidente, si es pertinente. Esto es especialmente importante para adelantarse a cualquier posible noticia negativa o daño a la reputación. Aunque cada incidente y cada contexto son diferentes, una comunicación sincera y transparente suele ayudar a generar confianza tras un incidente.



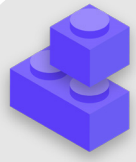
Creación de un Sistema de Alertas Tempranas y Respuestas

Considere la posibilidad de establecer un Sistema de Alertas Tempranas y Respuestas. Un sistema de este tipo suena elegante, pero en esencia no es más que un documento centralizado (electrónico o no) que se abre en caso de emergencia. En el documento, debe registrar todos los detalles sobre los indicadores de seguridad y los incidentes que se han producido en una línea de tiempo, proporcionar una descripción clara de las acciones y la secuencia para la respuesta planificada, e indicar lo que debe lograrse para suponer que el riesgo ha vuelto a disminuir. También debe incluir las medidas que deben tomarse después de un incidente para proteger a los involucrados de nuevos daños y ayudarlos a recuperarse física y emocionalmente. Un Sistema de Alertas Tempranas y Respuestas puede proporcionar documentación útil para compartir con las fuerzas de seguridad (si corresponde), un análisis posterior de lo sucedido y una orientación sobre cómo mejorar sus tácticas de prevención y respuestas ante futuras amenazas.

Además de estos importantes conceptos de respuesta ante incidentes, su organización también debe prepararse para cualquier respuesta técnica específica. En algunos casos, la respuesta técnica puede ser gestionada por el personal de TI interno o los administradores del sistema. Por ejemplo, si una cuenta de correo electrónico parece haber sido pirateada, el administrador de la cuenta debe estar preparado y ser capaz de cerrar o desactivar la cuenta afectada. Sin embargo, algunos incidentes técnicos pueden requerir conocimientos especializados que no tiene dentro de su organización. Para situaciones como esta, es importante identificar una lista de confianza de expertos técnicos externos que puedan ayudarle en su respuesta a los incidentes. En algunos casos, es posible que quiera negociar previamente las condiciones con los proveedores de servicios (como el alojamiento de su sitio web o un consultor informático) para asegurarse de que están disponibles (y no cobrarían un cargo adicional) para este tipo de respuesta a incidentes técnicos.

Por último, pero no por ello menos importante, debe considerar las medidas legales. Es importante entender las protecciones legales que puede tener, así como las obligaciones legales o las consecuencias que su organización podría enfrentar como resultado de una filtración de datos u otro incidente de seguridad. Un primer paso puede ser identificar a un asesor legal de confianza que conozca las leyes y normativas específicas de su país o localidad. Tómese un tiempo para repasar los posibles incidentes con esta persona y elabore un plan sobre lo que haría en respuesta. Es una buena idea llegar a un acuerdo con este asesor de confianza para que lo represente a usted y a sus intereses si es necesario también después de un incidente. Como parte de esta preparación legal, asegúrese de comprender las obligaciones legales de cualquier proveedor o socio. ¿Están obligados a notificarlo en caso de que se produzca su propia filtración de datos? ¿Qué apoyo (si lo hubiera) están obligados a prestarle en caso de incidente? Cuando elabore contratos y acuerdos con proveedores externos, tenga en cuenta la posibilidad de que se produzca una filtración de datos u otro incidente.

Aunque no existe un enfoque único para la respuesta a incidentes, es esencial contar con planes operativos, de comunicación, técnicos y legales claros. Cuando elabore su plan de respuesta a incidentes, le recomendamos encarecidamente que haga uso de algunos excelentes recursos existentes, diseñados para ayudar a las organizaciones de la sociedad civil y otros grupos de alto riesgo a lidiar con la respuesta a incidentes. Estos recursos incluyen el **Kit de Primeros Auxilios Digitales** desarrollado por RaReNet y CiviCERT, el **Manual de Campo contra el Acoso en Línea** de PEN América, el **Manual de Campaña de Ciberseguridad** del Centro Belfer, la **Plantilla del Plan de Comunicaciones de Incidentes Cibernéticos** y la **Línea de Ayuda de Seguridad Digital** de Access Now.



Respuesta a Incidentes

- **Desarrolle un plan de respuesta a incidentes de la organización, y póngalo en práctica.**
  - Haga una lluvia de ideas sobre posibles incidentes y prepare su respuesta antes de que ocurran.
- **Asegúrese de que todos los miembros de la organización sepan cómo se comunicarán y qué medidas técnicas se tomarán en caso de un incidente.**
- **Tómese el tiempo necesario para comprender sus protecciones y obligaciones legales.**
- **Esté preparado para proporcionar al personal de la organización el apoyo emocional y social que necesita después de un incidente.**

Apéndice A: Recursos Recomendados

- "Holistic Security Manual" de Tactical Tech; Creative Commons Attribution-ShareAlike 4.0 International License
  - Chapter 2.4, Understanding and Cataloguing Our Information
  - Chapter 1.5, Communicating about Threats in Teams and Organizations
  - Chapter 3.4, Security in Groups and Organizations
- "Security Education Companion" de The Electronic Frontier Foundation; Creative Commons Attribution 3.0 US License
  - Threat Modeling Activity Handout
- "Phishing Prevention and Email Hygiene Guide" de Freedom of the Press Foundation; Creative Commons Attribution 4.0 International License
- "Locking Down Signal Guide" de Freedom of the Press Foundation; Creative Commons Attribution 4.0 International License
- "Surveillance Self Defense (SSD) Guide" de Electronic Frontier Foundation; Creative Commons Attribution 3.0 US License
  - What Should I Know About Encryption
  - Communicating with Others
  - Choosing the VPN That's Right for You
- "Guide to Secure Group Chat and Conferencing Tools" de Frontline Defenders
- "Data Detox Kit" de Tactical Tech
  - Let the Right One In: Make Your Passwords Stronger
  - Strengthen Your Screen Locks
- "Elections Security Guide on Passwords" de Center for Democracy and Technology; Creative Commons Attribution 4.0 International License
- "Elections Security Guide on Two Factor Authentication" de Center for Democracy and Technology; Creative Commons Attribution 4.0 International License
- "Two Factor Authentication for Beginners" de Martin Shelton; Creative Commons Attribution 4.0 International License
- "Security in a Box" de Tactical Tech y Frontline Defenders; Creative Commons Attribution-ShareAlike 3.0 Unported License
  - Protect your device from malware and phishing attacks
  - Protect your information from physical threats
- SANS' Ouch! Newsletter: Stop That Malware
- "Device and Data Access when Personal Safety is At Risk" de Apple
- Global Cyber Alliance Cyber Hygiene for Mission-Based Organizations

Apéndice B:
Kit de Inicio del Plan de Seguridad

Utilice el siguiente kit de inicio para tomar notas mientras usted y su organización leen el Manual y asimilan el material, y considere las preguntas que acompañan al mismo con sus colegas para ayudar a generar un debate productivo.

Asegúrese también de consultar los "elementos básicos" clave en cada sección del Manual para asegurarse de que está cubriendo los temas importantes a medida que elabora su plan de seguridad. Al final del Manual, los elementos básicos, las respuestas a estas preguntas de debate y sus notas deberían formar la base de un plan de seguridad exitoso.



Crear una cultura de seguridad



Cimientos Sólidos: Protección de Cuentas y Dispositivos



Comunicar y almacenar los datos de manera segura



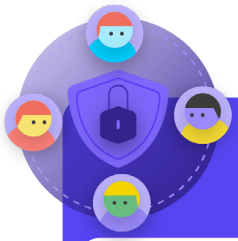
Mantenerse seguro en internet



Proteger la seguridad física



Qué hacer cuando las cosas van mal



Crear una cultura de seguridad

PREGUNTAS A TENER EN CUENTA:

- ¿Cuándo puede programar una conversación para revisar su plan de seguridad con toda la organización?
- ¿Qué días u horarios son los mejores para que la organización programe conversaciones y capacitación periódicas sobre seguridad?
- ¿Qué medidas puede tomar la dirección para mostrar un buen comportamiento de seguridad y compromiso con un plan de seguridad? ¿Cómo pueden los demás miembros de la organización desempeñar un papel en la seguridad?

SUS NOTAS E IDEAS:



Cimientos Sólidos: Protección de Cuentas y Dispositivos

PREGUNTAS A TENER EN CUENTA:

- ¿Cómo implementará las medidas de seguridad de las cuentas (como un administrador de contraseñas y 2FA) en toda la organización? ¿Qué obstáculos podría encontrar durante la implementación?
- ¿Cómo garantizará su organización que los dispositivos se mantengan seguros y actualizados? Como parte de esto, ¿necesitará la organización un plan para abordar el software o las computadoras sin licencia?
- ¿Cuándo es un buen momento para brindar una capacitación para todo el personal sobre los peligros del phishing, el malware y las mejores prácticas de seguridad de los dispositivos?

SUS NOTAS E IDEAS:

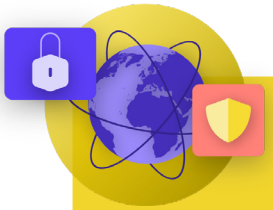


Comunicar y almacenar los datos de manera segura

PREGUNTAS A TENER EN CUENTA:

- ¿Cómo implementará su organización la mensajería cifrada de extremo a extremo para una comunicación segura? ¿Qué obstáculos podría encontrar durante la implementación?
- ¿Cómo aplicará su organización una solución segura para compartir archivos tanto a nivel interno como externo? ¿Qué obstáculos podría encontrar durante la implementación?
- ¿Cómo implementará su organización una solución segura de almacenamiento de datos y copias de seguridad? ¿Qué obstáculos podría encontrar durante la implementación?

SUS NOTAS E IDEAS:



Mantenerse seguro en internet

PREGUNTAS A TENER EN CUENTA:

- ¿Cómo implementará su organización los requisitos de navegación segura, como HTTPS, un navegador de confianza y, si corresponde, una VPN para el personal?
- ¿Cuáles serán los elementos clave de la política de redes sociales de su organización? ¿Cómo se aplicará?
- ¿Cómo protegerá su organización sus sitios y propiedades web?

SUS NOTAS E IDEAS:



Proteger la seguridad física

PREGUNTAS A TENER EN CUENTA:

- ¿Cómo distribuirá y hará cumplir la organización su política de visitas y acceso a la oficina?
- ¿Quién es el responsable de preparar al personal para los desafíos de seguridad física y digital a los que puede enfrentarse durante sus viajes de trabajo?
- ¿Qué medidas puede tomar el personal para mantener sus dispositivos seguros tanto en la oficina como en los viajes?

SUS NOTAS E IDEAS:



Qué Hacer Cuando las Cosas Van Mal

PREGUNTAS A TENER EN CUENTA:

- ¿Cómo distribuirá y pondrá en práctica la organización su política de respuesta a incidentes?
- ¿Hay recursos disponibles para el personal que pueda necesitar apoyo emocional y social tras un incidente? Si no es así, ¿cómo podría la organización proporcionar esos recursos en caso de algún incidente?

SUS NOTAS E IDEAS:

Apéndice C:
Citas de imágenes

Página 17: CNP Collection, “Security Protection Anti-Virus Software cms”, 2014, digital image, Alamy Stock Photo, https://www.alamy.com/security-protection-anti-virus-software-cms-image67114038.html?irclickid=2oWTxrXnOxyIRKXzgq3HowdNUkDzCPSFpyViRI0&utm_source=77643&utm_campaign=Shop%20Royalty%20Free%20at%20Alamy&utm_medium=impact&irgwc=1.
Página 24: Cottonbro, "Person Holding Black and Silver Key", 2020, digital image, Pexels, https://www.pexels.com/photo/person-holding-black-and-silver-key-5474292/?utm_content=attributionCopyText&utm_medium=referral&utm_source=pexels.
Página 26: Blogtrepreneur, "Malware Infection", 2016, digital image, Flickr, https://www.flickr.com/photos/143601516@N03/.
Página 29: "Microsoft Loading Screen," digital image, Kompass, September 23, 2019, https://asset.kompas.com/crops/kYVdzylbrYB5lIpuKDDwJLNFMV4=/164x49:679x393/750x500/data/photo/2018/07/02/4208974652.png.
Página 30: Mateuz Dach, "Turned-on iPhone and Displaying Icons," 2017, digital image, Pexels, https://www.pexels.com/photo/turned-on-iphone-and-displaying-icons-365194/.
Página 33: Crete-Nishihata, "Process For a Phishing Email Sent in 2016," digital image, University of Toronto, January 30, 2017, https://citizenlab.ca/2018/01/spying-on-a-budget-inside-a-phishing-operation-with-targets-in-the-tibetan-community/.
Página 38: Andrew Keymaster, "People Gathering on Street During Daytime Photo," 2020, digital image, Unsplash, https://unsplash.com/photos/JXQ2bizu7kc.
Página 39: Surveillance Self-Defense, "No Encryption in Transit," digital image, Electronic Frontier Foundation, January 17, 2019. https://ssd.eff.org/en/module/what-should-i-know-about-encryption.
Página 40: Surveillance Self-Defense, "4.Transport-layer-alternate," digital image, Electronic Frontier Foundation, January 17, 2019, https://ssd.Surveillance Self-Defense.org/files/2018/11/26/4.transport-layer-alternate.png. ; Surveillance Self-Defense, "6. End-to-end Alternate", digital image, Electronic Frontier Foundation, January 17, 2019, https://ssd.Surveillance Self-Defense.org/files/2018/11/26/6.end-to-end-alternate.png.
Página 42: Surveillance Self-Defense, "9._endtoendencryptionmetadata," 2019, digital image, Electronic Frontier Foundation, https://ssd.eff.org/en/module/what-should-i-know-about-encryption.
Página 50: Brett Sayles, "Server Racks on Data Center," 2020, digital image, Pexels, https://www.pexels.com/photo/server-racks-on-data-center-4508751/.
Página 55: PhotoMIX Company, 2016, "White 2 Cctv Cameras Mounted on Black Post Under Clear Blue Sky," digital image, Pexels, https://www.pexels.com/photo/white-2-cctv-camera-mounted-on-black-post-under-clear-blue-sky-96612/.
Página 60: Stefan Coders, "laptop-screen-vpn-cyber-security," 2020, digital image, Unsplash, https://pixabay.com/photos/laptop-screen-vpn-cyber-security-5534556/.
Página 62: Surveillance Self-Defense, "Using the Tor Browser," digital image, Electronic Frontier Foundation, April 25, 2020. https://ssd.eff.org/files/2020/04/25/circumvention-tor_0.png
Página 64: Nathan Dumlao, "White Samsung Android Smartphone on Brown Wooden Table," 2020, digital image, Unsplash, https://unsplash.com/photos/kLmt1mpGJVg.
Página 69: Matt Artz, "Two Broken 6-Pane On White Painted Wall Photo," digital image, Unsplash, October 1, 2017, https://unsplash.com/photos/vT684iB7Ejg.

NDI
NATIONAL
DEMOCRATIC
INSTITUTE

