NDI
NATIONAL DEMOCRATIC INSTITUTE

HOUSE DEMOCRACY PARTNERSHIP

Manual de Ciberseguridad

para

Parlamentos

Una guía para los parlamentos que buscan iniciar un plan de ciberseguridad

IRI INTERNATIONAL REPUBLICAN INSTITUTE
Advancing Democracy Worldwide

USAID FROM THE AMERICAN PEOPLE

Manual de Ciberseguridad

para

Parlamentos

Una guía para los parlamentos que buscan iniciar un plan de ciberseguridad

Tabla de contenido

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 casos que destacan el impacto en la vida real de un determinado tema en los parlamentos a nivel mundial o en un país específico.

Consejos Adicionales

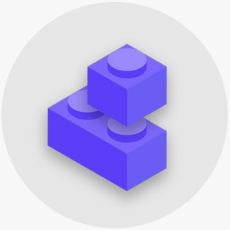
Destaca algunos consejos e información adicionales a los que debe prestar atención mientras lee el Manual.

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 podría 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.

Los 10 Principales

Estos 10 elementos son fundamentales para el plan de seguridad de su parlamento. Si busca un punto de partida, mire primero aquí.

1. **Realice capacitaciones periódicas en seguridad dentro de su parlamento**
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. **Exige 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 parlamento**
10. **Desarrolle un plan de respuesta a incidentes de la organización.**

1

Construcción de una Cultura de Seguridad

2

Cimientos Sólidos: Protección de Cuentas y Dispositivos

3

Comunicación y Almacenamiento Seguro de Datos

4

Mantenerse a Salvo en Internet

5

Protección Física Seguridad

6

Qué Hacer y Cuándo Las Cosas Van Mal

Autores y Agradecimientos

El Instituto Nacional Demócrata (NDI) y House Democracy Partnership (HDP) produjeron esta guía.

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, Fondo de Tecnología Abierta; Bill Budington y Shirin Mori, Fundación Frontera Electrónica; Jocelyn Woolbright, Cloudflare; Martin Shelton, Fundación para la Libertad de Prensa; Dave Leichtman, Microsoft; Stephen Boyce, Fundación Internacional para Sistemas Electorales; Amy Studdart, Instituto Republicano Internacional; Emma Hollingsworth, Alianza Cibernética Global; Caroline Sinders, Diseño de Convocatorias + Investigación; Dhyta Caturani; Sandra Pepera, NDI; Aarón Azelton, NDI; Frieda Arenos, NDI; Anthony De Angelo, NDI; Whitney Pfeifer, NDI; y Derek Luyten, House Democracy Partnership. También nos gustaría agradecer a Paul Kollie en Servicios de Información Legislativa de Liberia, Nihad Bahram y Fuad Ahmed en el parlamento de Kurdistán en Irak, Diana Plata en el Senado de Colombia; Ayad Abbas y Majid Khudhur en el Consejo de Representantes de Irak, y Tanja Danailovska en la Asamblea de Macedonia del Norte por sus valiosos ideas y aportes.

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 se diseñó para complementar esos materiales más detallados, ya que combina lecciones clave en un recurso único y fácil de leer para los parlamentos que buscan iniciar un plan de ciberseguridad.

Además de tomar inspiración indirecta de muchos recursos maravillosos recopilados por la comunidad, hemos copiado directamente 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 Fundación Frontera Electrónica, el Manual de Seguridad Holística de Tactical Tech y una serie de explicaciones del Centro para la Democracia y la Tecnología y la Fundación para la Libertad de Prensa. 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.

¿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 saber más sobre nuestro trabajo puede visitar nuestro sitio web, seguirnos en Twitter o comunicarse directamente con cyberhandbook@ndi.org. Siempre nos encanta saber de usted y responder sus preguntas sobre nuestro equipo y nuestro trabajo en materia de ciberseguridad, tecnología y democracia.

House Democracy Partnership (HDP) trabaja con las legislaturas de todo el mundo para promover un gobierno receptivo y eficaz y fortalecer las instituciones democráticas. Un elemento central de nuestro trabajo es la cooperación entre pares para generar conocimientos técnicos en las legislaturas asociadas que mejorarán la rendición de cuentas, la transparencia, la independencia legislativa, el acceso a la información y la supervisión del Gobierno. En la actualidad, HDP tiene asociaciones con más de 20 legislaturas nacionales en todo el mundo. Las áreas de cooperación con los parlamentos socios del HDP incluyen abordar cuestiones presupuestarias, garantizar operaciones de comités más eficaces, mejorar los servicios de los electores, proporcionar herramientas para una supervisión más sólida, fortalecer la ética legislativa y mejorar procesos y procedimientos de tecnología de la información (TI), legislativos, y de bibliotecas e investigación. El Instituto Nacional Demócrata (NDI) y el Instituto Republicano Internacional (IRI) implementan los programas de HDP mediante un acuerdo de financiación cooperativa con la Agencia de EE. UU. para el Desarrollo Internacional (USAID).

¿Quién Maneja la Ciberseguridad Parlamentaria?

Para tener un parlamento eficaz y seguro se requiere personal con la habilidad y la autoridad adecuada para implementar las recomendaciones incluidas en este Manual. Dicho esto, los responsables de la seguridad cibernética en los parlamentos pueden variar en gran medida, y no existe un modelo "correcto" de quién debería manejar la seguridad cibernética. En algunos casos, puede ser un equipo de ciberseguridad dedicado dentro de su unidad de TI y, en otros, un grupo de diferentes miembros de personal administrativo por igual. De todos modos, tenga en cuenta que si bien es importante contar con un buen equipo a cargo de la ciberseguridad de su parlamento, también es responsabilidad de todos dentro y cerca del parlamento seguir las políticas y los procedimientos necesarios para mantenerlo a salvo. A continuación se presentan algunos ejemplos de diferentes modelos de dotación de personal para manejar la ciberseguridad parlamentaria:

Cámara de Representantes de Estados Unidos
En la **Cámara de Representantes de Estados Unidos**, en algunas oficinas de miembros individuales contratan a un **administrador de sistemas** que es responsable de administrar todos los sistemas de hardware y software de computadora que utilizan, y eso incluye la administración de consideraciones de ciberseguridad. Además, se capacita a los miembros del personal en las mejores prácticas. A nivel institucional, el Director Administrativo de la Cámara de Representantes cuenta con un equipo de Recursos de Información que incluye un **departamento dedicado a la seguridad de la información.**

Asamblea Nacional de Zambia
La **Asamblea Nacional de Zambia** cuenta con su Departamento de Tecnología de Información y Comunicaciones (TIC) para una variedad de funciones, incluido el manejo de software, hardware e infraestructura de información del parlamento, capacitación de miembros del parlamento y personal sobre sistemas tecnológicos y protección de la infraestructura de información del parlamento contra amenazas de ciberseguridad internas y externas.

Parlamento de Malasia
El **parlamento de Malasia** alberga su división de Tecnología de la Información a cargo del administrador principal del parlamento, lo que le permite brindar servicio a ambas cámaras. Esta división incluye un puesto específico para seguridad de la red, lo que le permite garantizar que los sistemas de red, centros de datos e infraestructura de TIC estén al día y sean lo más seguros posible.

¿A quién va dirigido este Manual?

Este manual se escribió con un objetivo simple en mente: ayudar a su parlamento a desarrollar un plan de seguridad cibernética comprensible e implementable.

Mientras el mundo se mueve cada vez más en línea, la ciberseguridad no es solo una palabra de moda, sino un concepto fundamental para el éxito de los parlamentos, y la seguridad de la información (tanto en línea como fuera de ella) es un desafío que requiere enfoque, inversión y vigilancia.

Es probable que, si no lo ha hecho ya, su parlamento descubra que es objetivo de un ataque de ciberseguridad. Esto no pretende ser alarmista; es una realidad incluso para parlamentos que no se consideran objetivos en particular.

En un año promedio, el Centro de Estudios Estratégicos e Internacionales, que lleva 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 esos ataques informados, es probable que haya cientos más pequeños cada año que no se detectan o no se informan, muchos dirigidos a instituciones gubernamentales, cuerpos legislativos y organizaciones políticas.

Los ciberataques de este tipo tienen consecuencias importantes. Ya sea su objetivo interrumpir las operaciones parlamentarias, dañar su reputación o incluso robar información que pueda provocar daños psicológicos o físicos a sus miembros o al personal, tales amenazas deben tomarse en serio.

Lo bueno es que no es necesario convertirse en codificador o técnico para defenderse y defender a su parlamento contra amenazas comunes. Sin embargo, debe estar preparado para invertir esfuerzo, energía y tiempo en el desarrollo y la implementación de un sólido plan de seguridad parlamentaria.

Si nunca ha pensado en la ciberseguridad para su parlamento, no ha tenido tiempo de concentrarse en ella, o conoce algunos conceptos básicos sobre el tema pero cree que podría mejorarla en su parlamento, este Manual es para usted. **Independientemente de su procedencia, este Manual intenta brindar a su parlamento la información esencial que necesita para implementar un plan de seguridad sólido, que vaya más allá de solo consignar palabras en un papel, y le permita poner en práctica los mejores hábitos.**

¿Qué es un plan de seguridad y por qué mi parlamento debería tener uno?

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

Un plan de seguridad organizativa bien elaborado y actualizado puede tanto mantenerlo a salvo como hacerlo más eficaz al proporcionarle la tranquilidad necesaria para concentrarse en el importante trabajo diario de su parlamento. 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 comienza a desarrollar un plan de seguridad, debe hacerse algunas preguntas importantes que forman un proceso llamado **evaluación de riesgos.** Responder estas preguntas ayuda a su parlamento a entender las amenazas únicas que usted enfrenta y le permite dar un paso atrás y pensar en forma exhaustiva en lo que necesita proteger y de quién debe protegerlo. Hay asesores capacitados que, con la ayuda de sistemas como la plataforma de auditoría **SAFETAG** de Internews, pueden ayudar a guiar a su organización en ese proceso. Si puede acceder a ese nivel de experiencia profesional, vale la pena, pero incluso si no puede someterse a una evaluación completa, debería reunirse con sus partes interesadas en todo el parlamento para considerar con cuidado estas preguntas clave:

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

Para responder estas preguntas puede comenzar por **crear un catálogo de todos los activos de su parlamento**. 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, anote 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 del parlamento son de dominio público o es información que ya publica, no son secretos que deba proteger.

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

"Adversario" es un término comúnmente utilizado en la seguridad de las organizaciones. En términos simples, los adversarios son los actores (individuales o en grupos) que están interesados en atacar a su parlamento, alterar su trabajo y obtener acceso a su información o destruirla. En síntesis, los malos. Algunos ejemplos de adversarios potenciales podrían ser estafadores financieros, gobiernos adversarios o piratas informáticos con motivaciones ideológicas o políticas. Es importante hacer una lista de adversarios y pensar en forma crítica sobre quién podría querer afectar de manera negativa a su parlamento y al 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. Usted puede incluso convertirse en su propio adversario si, por ejemplo, borra por accidente 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. ¿Les interesa desacreditar a su parlamento? ¿Quizás tienen la intención de silenciar su mensaje o alterar el trabajo del parlamento? Es importante entender la motivación de un adversario porque eso puede ayudar a su parlamento a evaluar mejor las amenazas que podría plantear.

3 ¿Qué amenazas enfrenta su parlamento? ¿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 parlamento a dar los siguientes pasos productivos, es útil analizar cada amenaza basados en dos factores: la probabilidad de que se produzca el daño que se amenaza y el impacto en ese caso.

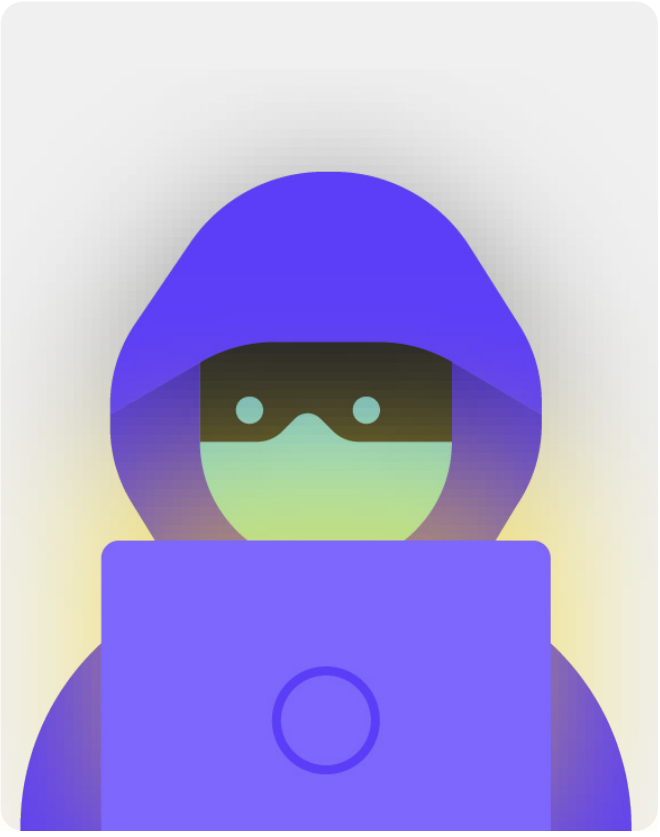
Para medir la probabilidad de una amenaza (tal vez "baja, media o alta" en función de si es probable que se produzca un evento determinado, si podría producirse o si se produce con frecuencia), puede utilizar información que conoce sobre la capacidad y la motivación de sus adversarios, análisis de incidentes de seguridad anteriores, experiencias de otras organizaciones similares y, por supuesto, 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. Haga este tipo de preguntas: "¿Cómo nos ha dañado la amenaza como parlamento y como personas, en forma física y mental?", "¿Cuánto dura el efecto?", "¿Esto crea otras situaciones dañinas?" y "¿Cómo obstaculiza nuestra capacidad para lograr nuestras metas 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 que tienen más probabilidades de ocurrir Y ADEMÁS tendrán impactos negativos significativos, canalizará sus recursos limitados con la mayor eficiencia y eficacia 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 y proteger a sus colegas y a su parlamento al ocuparse de las amenazas más grandes.

Para ayudarlo a manejar este proceso de evaluación de riesgos, considere la posibilidad de utilizar una hoja de trabajo como **esta**, desarrollada por la Fundación Frontera Electrónica (EFF). Tenga en cuenta que la información que desarrolle como parte de este proceso (como una lista de sus adversarios y las amenazas que plantean) puede ser confidencial, por lo que es importante mantenerla segura.



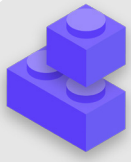
Creación de un Plan de Ciberseguridad para su Parlamento

Si bien el plan de seguridad de cada parlamento 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 parlamento a elaborar un plan de seguridad concreto basado en soluciones prácticas y aplicaciones del mundo real.

En este Manual tratamos de ofrecer opciones y sugerencias gratuitas o de muy bajo costo. Tenga en cuenta que el costo más importante asociado con la implementación de un plan de seguridad eficaz será el tiempo que usted y el personal, los miembros y los equipos del parlamento necesiten para hablar de su nuevo, aprenderlo e implementarlo. Pero dados los riesgos que es probable que enfrente su parlamento, esta inversión valdrá la pena.

En cada sección encontrará una explicación de un tema clave que su parlamento y su personal deberían conocer: qué es y por qué es importante. Cada tema va acompañado de estrategias esenciales, enfoques y herramientas recomendadas para limitar el riesgo, además de consejos y enlaces a recursos adicionales que pueden ayudarlo a aplicar esas recomendaciones en todo su parlamento.



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. Mientras toma notas y comienza a actualizar o elaborar su plan de seguridad, asegúrese de hacer referencia a los "Elementos esenciales 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.
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, y la caja de herramientas de ciberseguridad 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 implementar muchos aspectos básicos.

Crear una cultura de seguridad

La seguridad tiene que ver con las personas y, para proteger a su parlamento, debe asegurarse de que todos los involucrados, incluidos los miembros del parlamento (MP), el personal de apoyo legislativo y personal del servicio de investigación, así como el personal administrativo de finanzas, recursos humanos y TI, entre muchos otros, se toman en serio la ciberseguridad. Cambiar la cultura es difícil, pero unos simples pasos y conversaciones importantes pueden contribuir en gran medida a crear una atmósfera que fomente la resiliencia de su personal y su parlamento frente a amenazas a la seguridad. Uno de los pasos más simples pero más importantes para construir esta cultura de seguridad parlamentaria es comunicarla dentro y por todo el parlamento, y que los líderes siempre modelen un buen comportamiento e inviertan en él.

Construcción de una Cultura de Seguridad en los Parlamentos

En febrero de 2019, Australia sufrió un ciberataque que comprometió las redes del parlamento nacional australiano y de tres importantes partidos políticos. Los atacantes pudieron obtener acceso a documentos de políticas y correspondencia privada por correo electrónico entre parlamentarios, su personal y sus electores. Sucedió solo tres meses antes de la fecha prevista para las elecciones, lo que pone de relieve la vulnerabilidad de las redes inseguras durante esos procesos.

En respuesta a este ataque significativo y exitoso, el parlamento emprendió esfuerzos para mejorar su preparación en ciberseguridad. Dicha inversión incluyó la indagación del Comité Conjunto de Cuentas Públicas y Auditorías de la resiliencia cibernética del Commonwealth. La indagación **se basó en los hallazgos de auditorías** realizadas durante varios años que encontraron que faltaban procesos de mitigación de riesgos de ciberseguridad en el parlamento y otros organismos gubernamentales. Por ejemplo, la Oficina Nacional de Auditoría de Australia destacó que el parlamento no se centró en los objetivos estratégicos a largo plazo y no desarrolló un enfoque basado en el riesgo en lo referente a ciberseguridad. Y aunque la indagación y las auditorías no fueron halagadoras, la voluntad del parlamento de identificar los problemas de ciberseguridad e invertir en abordarlos es un ejemplo de la creación de una cultura conducente a una ciberseguridad parlamentaria eficaz. Es una que comienza con reconocer los problemas e invertir en soluciones técnicas y humanas, en la que la seguridad no se elude sino que se prioriza. Por ejemplo, mediante la contratación de un equipo de "mejora de la seguridad cibernética" y la inversión presupuestaria para un **"fondo de respuesta de ciberseguridad"**, el parlamento (y otras entidades gubernamentales) deberían estar mejor equipados para mitigar futuros ataques si dichos recursos se implementan y mantienen en forma adecuada, y permanece el enfoque en la ciberseguridad como un elemento habitual de las operaciones parlamentarias. Dicho esto, por supuesto es mejor construir este compromiso con la seguridad dentro de su parlamento *antes de* que se produzca una brecha de seguridad significativa.

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 al personal y los miembros del equipo les preocupa la seguridad, estarán menos ansiosos sobre parecer paranoicos o por hacer perder el tiempo a otras personas. **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 el personal de los equipos 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. Esas conversaciones no solo deberían dejar espacio para temas de seguridad técnica, sino también para cuestiones que afectan la comodidad y seguridad del personal, como acoso en línea (y fuera de ella) o problemas con el uso y la aplicación de herramientas digitales dentro de las oficinas parlamentarias. En las conversaciones puede haber incluso temas como hábitos de intercambio de información fuera de línea y formas en que el personal asegura o no la información fuera del parlamento. Después de todo, es importante recordar que la seguridad de un parlamento 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 coordinar un debate sobre la seguridad entre diferentes miembros del personal, lo que puede ayudar a desarrollar la idea de que la seguridad es responsabilidad de todos y no solo de unos pocos o del "equipo de TI". 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 del parlamento, como durante la incorporación de miembros y personal, y pensar en cortar el acceso a los sistemas durante su desvinculación. La seguridad no debe ser un "elemento extra" del que hay que preocuparse, sino una ***parte integral de su estrategia y sus operaciones.***

Recuerde que todos los planes de seguridad deberían considerarse documentos vivos y reevaluarse y comentarse en forma periódica, en especial cuando cambia su contexto de seguridad.

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 también es garantizar la aceptación de su plan de seguridad en todo el parlamento.

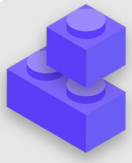
Es fundamental que esto incluya un apoyo explícito fuerte, y una orientación de los directivos de la organización, que en muchos casos serán quienes tomen la decisión final de asignar tiempo, recursos y energía al desarrollo y la implementación de un plan de seguridad eficaz. Si ellos no se lo toman en serio, nadie más lo hará. Para lograr esta aceptación, piense con cuidado cuándo y cómo presentar su plan, hágalo en forma clara, asegúrese de que los directivos refuercen los mensajes y guíe a todos en los elementos y pasos del plan para que no haya ningún misterio ni confusión sobre lo que se intenta lograr. Asegúrese también de presupuestar en forma adecuada para la ciberseguridad en todo el parlamento. Aunque las finanzas podrían ser limitadas, es esencial invertir lo correcto en seguridad cibernética, o de lo contrario, es probable que se pongan en riesgo otras inversiones. Cuando hable de seguridad, evite las tácticas de miedo. A veces, las amenazas que enfrentan su parlamento y su personal pueden asustar, pero intente centrarse en compartir los datos y crear un espacio de calma para 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 cómo capacitará a todos los miembros, el personal y los voluntarios en estas nuevas buenas prácticas.

Requerir capacitación periódica, y hacer obligatoria la asistencia, puede ser una táctica útil. 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, recompensas por una capacitación exitosa y la adopción de políticas puede ayudar a incentivar la mejora en todo el parlamento. Puede encontrar un valioso apoyo adicional en redes locales o internacionales de capacitación en seguridad digital y 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.

Considere cómo puede llegar su plan de capacitación a los MP, al personal parlamentario y también a la administración. Tenga en cuenta que los miembros prominentes muchas veces requieren aún más capacitación y atención cuando se trata de seguridad debido a su alto perfil.Asegúrese de que sus planes de capacitación y de seguridad se apliquen a todos estos diferentes tipos de personas y cualquier activo que puedan tener tanto dentro como fuera del parlamento.



Crear una cultura de seguridad

- **Programe conversaciones y capacitaciones periódicas sobre la seguridad y su plan de seguridad.**
- **Involucre a todos: distribuya la responsabilidad de la implementación de su plan de seguridad en todo el parlamento.**
- **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 cada año o después de cambios importantes en la dotación de personal parlamentario, la estructura o el entorno operativo.**

Cimientos Sólidos: Protección de Cuentas y Dispositivos

¿Por qué centrarse en las cuentas y los dispositivos? Porque forman la base de todo lo que su parlamento hace en forma digital.

Es casi seguro que usted accede a información sensible, se comunica interna y externamente y guarda información privada en ellos. Solo considere la participación de los miembros en las sesiones plenarias, la votación (incluso virtual), los procesos de redacción legislativa y la comunicación con los miembros del personal y el público en general. Sin cuentas y dispositivos seguros, estas operaciones parlamentarias esenciales y otras pueden correr peligro. Por ejemplo, si hay piratas informáticos que observan sus pulsaciones de teclas o escuchan su micrófono, las conversaciones privadas con colegas se capturarán sin importar lo seguras que sean sus aplicaciones de mensajería. O bien, si un adversario obtiene acceso a las cuentas de redes sociales de su parlamento, podría dañar con facilidad su reputación y credibilidad, y socavar la confianza del público. Por eso es esencial como parlamento asegurarse de que todos tomen medidas simples pero eficaces para mantener seguros sus dispositivos y cuentas. 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 con gusto tras el objetivo más fácil y entrarán en una cuenta personal o en una computadora hogareña si sus miembros y el personal las utilizan para comunicarse y acceder a información importante.

Cuentas y Parlamentos Seguros

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 Estados Unidos, proveedores de tecnología como Microsoft y Cisco, y varias 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 piratería informática se producen debido a contraseñas débiles o reutilizadas.

Con la prevalencia cada vez mayor de violaciones como esta de contraseñas y el acceso más fácil para todo tipo de adversarios a herramientas sofisticadas de piratería, las mejores prácticas para las contraseñas y la autenticación de dos factores son elementos imprescindibles de seguridad para todas las organizaciones, incluidos los parlamentos. Ningún incidente ilustra esto con más claridad que el **ataque de 2017** contra el sistema de correo electrónico del parlamento británico. En ese incidente, las malas prácticas de contraseñas de una pequeña pero significativa cantidad de MP llevaron a la exposición de conversaciones y cuentas de correo electrónico, se filtraron miles de credenciales, y hubo una tremenda alteración de las operaciones parlamentarias. **Según** la oficina de prensa del parlamento británico, las cuentas quebrantadas quedaron "comprometidas como resultado de contraseñas débiles que no se ajustaban a la guía emitida por el Servicio Digital Parlamentario".

Cuentas Seguras: Contraseñas y Autenticación de Dos Factores

En el mundo actual, es probable que su parlamento y su personal tengan docenas y hasta cientos de cuentas que, si se quebrantaran, podrían exponer información sensible o incluso hacer que personas en riesgo resultaran heridas.

Piense en las diferentes cuentas que el personal individual y el parlamento en su conjunto pueden tener: correo electrónico, aplicaciones de chat, redes sociales, banca en línea, almacenamiento de datos en la nube, además de tiendas de ropa, restaurantes locales, periódicos y muchos otros sitios web o aplicaciones en los que inician sesión. Una buena seguridad en el mundo actual requiere un enfoque diligente para proteger todas estas cuentas de los ataques. Eso comienza con garantizar una buena higiene de contraseñas y que todos usen autenticación de dos factores.

¿QUÉ HACE BUENA UNA 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. Como resultado, es esencial que tengan como mínimo 16 caracteres, o al menos 5 palabras, y de preferencia, 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 COMO AYUDA

Usted ya sabe que es importante que todos en el parlamento usen una contraseña larga, aleatoria y diferente para cada una de sus cuentas personales y parlamentarias, pero ¿cómo lo hace en realidad? 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 lo ideal sería 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 las demás. Los administradores de contraseñas también pueden compartirse entre varias cuentas para facilitar el intercambio seguro de contraseñas en todo el parlamento.

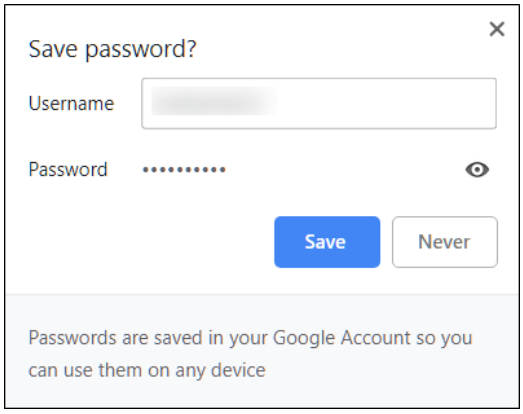
¿Por qué tenemos que usar algo nuevo? ¿No podemos anotarlas en un papel o en una planilla de cálculo en la computadora?

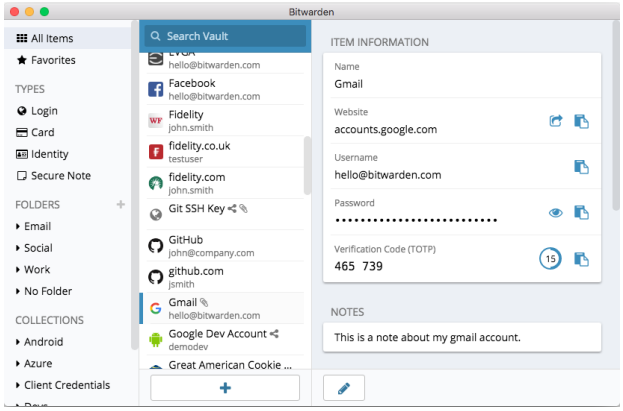
Por desgracia, hay muchos enfoques comunes para la administración de contraseñas que no son seguros. Almacenar las contraseñas en hojas de papel (a menos que las guarde bajo llave en una caja fuerte) puede exponerlas a robos físicos, a miradas indiscretas y a su fácil pérdida y deterioro. Guardar las 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 deberíamos 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, que se ve a la izquierda) para guardar sus contraseñas, utilice un administrador de contraseñas exclusivo (como Bitwarden, a la derecha). Los administradores de contraseñas tienen características que hacen la vida más segura y práctica para su parlamento.





¿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 conveniencia que brinda un buen administrador de contraseñas. Perder esa ventaja hace que sea más probable que las personas en todo el parlamento continúen con prácticas deficientes de creación y uso compartido de 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 compartir contraseñas) que no solo aportan valor a la seguridad individual, sino al parlamento en su conjunto. Si ha estado guardando contraseñas con su navegador (intencionalmente o no), tómese un momento para eliminarlas.

¿Qué administrador de contraseñas deberíamos utilizar?

Existen muchas buenas herramientas de administración de contraseñas que se pueden configurar en menos de 30 minutos. Si busca una opción de confianza en línea para su parlamento a la que se pueda acceder desde múltiples dispositivos en cualquier momento, 1Password (a partir de $2.99 mensuales por usuario) o la gratuita y de código abierto BitWarden tienen buen respaldo y recomendaciones. Una opción en línea como BitWarden puede ser excelente tanto por seguridad como por conveniencia. BitWarden, por ejemplo, lo ayudará a crear contraseñas únicas y sólidas y acceder a ellas desde múltiples dispositivos mediante extensiones del navegador y una aplicación móvil. Con la versión paga ($10 por un año

completo), también proporciona informes sobre contraseñas reutilizadas, débiles y que es posible que hayan quebrantado, a fin de ayudarlo a estar en control. 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 también cuando se utiliza el administrador de contraseñas.** 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 el dispositivo o cree que puede correr un riesgo intensificado de robo físico del aparato. Esto incluye cerrar la sesión de su administrador de contraseñas si deja la computadora o el dispositivo móvil desatendido. Si comparte contraseñas entre equipos o el parlamento en su conjunto, también asegúrese de revocar el acceso a ellas (y cambiarlas) cuando las personas se vayan. Por ejemplo, no debería dejar que un antiguo miembro del personal conserve el acceso a la contraseña de Facebook de su parlamento.

¿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 Parlamento

Puede reforzar las prácticas de contraseñas de todo su parlamento y asegurarse de que todo el personal en forma individual tenga acceso a (y utilice) un administrador de contraseñas al implementar 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 mensuales por usuario. Con él (u otros planes de equipo de administradores de contraseñas, como 1Password), uno tiene la posibilidad de administrar todas las contraseñas compartidas en toda la organización. Las características de un administrador de contraseñas para el parlamento o para todo el equipo no solo brindan mayor seguridad, sino también conveniencia al 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 características brindan a su parlamento 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 todo el parlamento, hay que asegurarse de que alguien se encargue en forma específica 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 MFA o 2FA.

Hay muchas guías y recursos excelentes que explican la autenticación de dos factores, como el artículo Two Factor Authentication for Beginners (Autenticación de dos factores para principiantes) de Martin Shelton y la Election Cybersecurity 101 Field Guide (Guía de campo 101 de ciberseguridad para elecciones) del Centro para la Democracia y la Tecnología. 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 parlamento.

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.

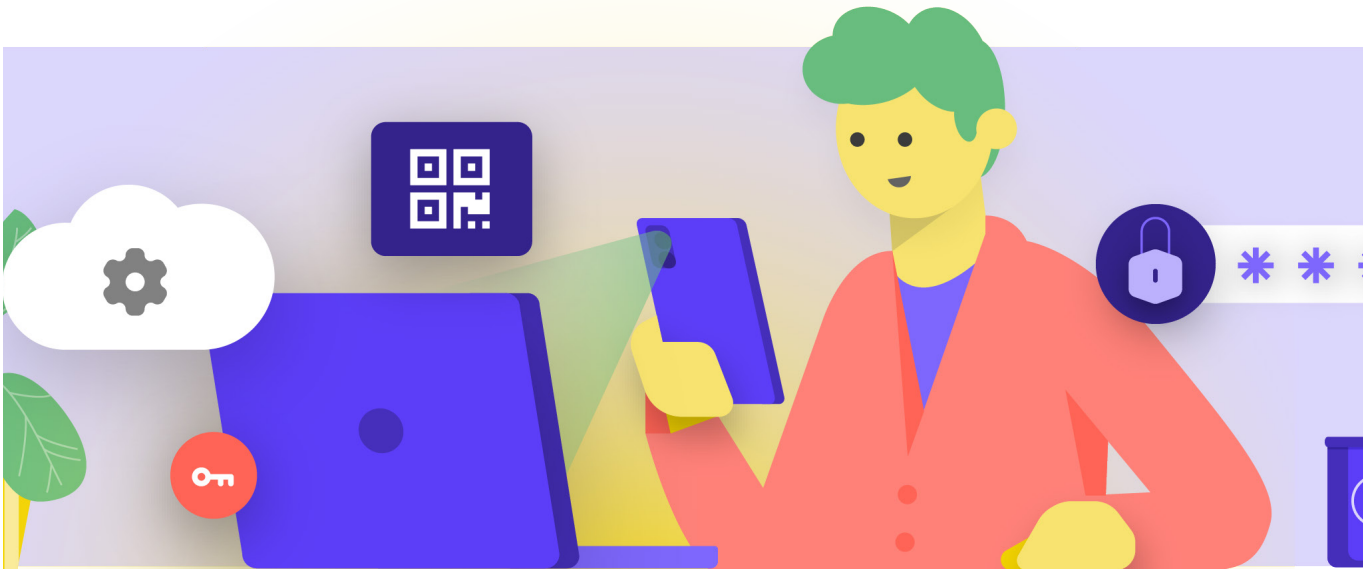
Este segundo dato de información actúa como una segunda capa de defensa. Si un hacker roba su contraseña o accede a ella a través de la descarga de contraseñas de una gran filtración de datos, una 2FA eficaz puede impedirle el acceso a su cuenta (y por tanto, a la información privada y sensible). Asegurarse de que todos en el parlamento implementen 2FA en sus cuentas es de vital importancia.

¿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 por completo a prueba de phishing. Estas "llaves" son tokens de hardware (piense en miniunidades USB) que pueden adjuntarse a su llavero (o permanecer en su computadora) para fácil acceso y 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), incluido YubiKeys, que tiene gran prestigio. 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.



Aplicaciones de Autenticación

La **segunda mejor opción para 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

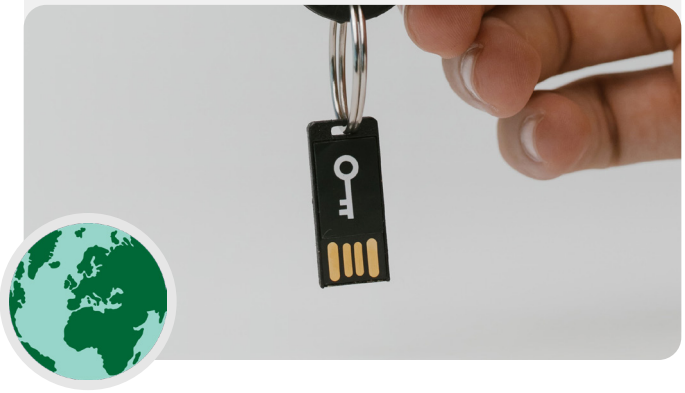
La forma menos segura, pero desgraciadamente aún más común de la 2FA, son los códigos enviados por SMS. Dado que los SMS pueden ser interceptados y los números de teléfono pueden ser suplantados o pirateados a través de su operador de telefonía móvil, los SMS dejan mucho que desear como método para solicitar 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 parlamento, utilice este sitio web (https://2fa.directory/) para buscar con rapidez información de servicios específicos (como Gmail, Office 365, Facebook, Twitter, etc.) e instrucciones para ellos y para ver cuáles de ellos permiten qué tipos de 2FA.

2FA y Parlamentos

Según informes de 2020, los piratas informáticos se infiltraron en el sistema de correo electrónico parlamentario de Noruega, y comprometieron cuentas pertenecientes a varios funcionarios de la institución e incluso descargaron información de los sistemas parlamentarios. Si bien los detalles completos del ataque no se dieron a conocer al público, Noruega atribuyó la intrusión a APT28, un grupo de piratería afiliado a los servicios de seguridad de Rusia. Si bien son altamente sofisticados, APT28 y otros piratas informáticos muchas veces usan tácticas menos complejas, como "ataques de fuerza bruta" (en los que se usan herramientas para intentar muchas contraseñas con la esperanza de al fin adivinar la correcta) para obtener acceso a la cuenta. Esta táctica permite a los piratas informáticos adivinar incluso contraseñas sólidas, como creían que tenían en Noruega. ¿La buena noticia? Es mucho menos probable que estos tipos de ataques tengan éxito con la clave adecuada o la implementación de autenticación de dos factores basada en la aplicación.

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.



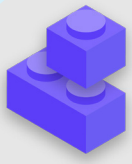
¿QUÉ OCURRE SI ALGUIEN PIERDE UN DISPOSITIVO 2FA?

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. Como alternativa, debería crear códigos de respaldo para las cuentas que lo permitan. 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 conozcan estos pasos cuando comiencen a habilitar 2FA en sus cuentas.

Imponer la 2FA en Todo el Parlamento

Si su parlamento proporciona cuentas de correo electrónico a todo el personal en Google Workspace (antes conocido como GSuite) o Microsoft 365 con el uso de su propio dominio (por ejemplo, @ndi.org), puede imponer la 2FA y una configuración fuerte de seguridad para todas las cuentas. Esta implementación no solo ayuda a proteger esas cuentas, sino que también actúa como una forma de introducir y normalizar la 2FA en su personal a fin de que se sientan más cómodos de adoptarla también para sus 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 imponer 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 parlamentarias; aliente a hacer lo mismo en las cuentas personales de los miembros, el personal y los voluntarios.**
- **Implemente un administrador de contraseñas de confianza para el parlamento (y fomente su uso también en la vida privada 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 y los miembros dejen el parlamento.**
- **Solo comparta contraseñas en forma segura, como mediante el administrador de contraseñas de su parlamento o aplicaciones cifradas de extremo a extremo.**
- **Exija 2FA en todas las cuentas del parlamento y aliente al personal a configurar 2FA también en todas sus cuentas personales.**
  - Si es posible, proporcione llaves de seguridad físicas a todos los miembros y al 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 asegurarse de que todos conozcan las mejores prácticas en materia de contraseñas y 2FA, incluido qué hace fuerte a una contraseña y la importancia de no reutilizarlas nunca, aceptar únicamente solicitudes legítimas de 2FA y generar códigos de 2FA de respaldo.**

Dispositivos Seguros

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

Esa protección comienza por ser cuidadosos con el tipo de dispositivos que su parlamento y personal compran y usan. 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. Por lo tanto, a pesar de la presencia omnipresente y poco costosa de teléfonos inteligentes como Huawei o ZTE, deberían evitarse. Si bien el bajo costo del hardware puede ser muy atractivo, los riesgos potenciales de seguridad para los parlamentos deberían guiarlo hacia otras opciones de dispositivos y equipos.

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 Dispositivos y Parlamentos

Algunos de los programas maliciosos más avanzados que existen se han desarrollado e implementado en todo el mundo para **atacar** a los MP y otros funcionarios gubernamentales y su personal. En India, por ejemplo, una sociedad de periodistas **reveló** que varios MP y ministros del Gobierno recibieron el ataque del spyware Pegasus, un tipo de software malicioso que llegó a los encabezados en 2020. Pegasus es famoso por su capacidad para infectar dispositivos móviles y dar al perpetrador la posibilidad de grabar audio, interceptar pulsaciones de teclas y mensajes y, de hecho, poner a la víctima bajo vigilancia total sin requerir la interacción de ella. Sin embargo, la gran mayoría del spyware triunfa en poner en peligro a sus víctimas.

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). Deberá instalar cerraduras fuertes, cámaras de seguridad u otros sistemas de monitoreo. 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 consiguen robar un dispositivo (o incluso si solo acceden a él durante un breve período), asegúrese de **imponer el uso de contraseñas fuertes o códigos de acceso en las computadoras y teléfonos de todos.** Los mismos consejos sobre el tema de la sección de contraseñas de este Manual se aplican a 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 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. Asegúrese de que todos los dispositivos que expide el parlamento también estén inscritos en un **dispositivo móvil o sistema de administración de terminales.** Si bien son costosos, estos sistemas permiten que su parlamento imponga políticas de seguridad en todos los dispositivos y ubique uno, y elimine su contenido potencialmente confidencial, si se produjeran un robo, una pérdida o una confiscación. Existen muchas soluciones diferentes para la administración de dispositivos móviles, peo hay unas cuantas opciones confiables que funcionan en todas las plataformas (iPhones, Android, Mac y Windows) como: Hexnode, Meraki Systems Manager de Cisco, MDM de IBM y la función de administración de dispositivos móviles integrada de Google Workspace. Si el costo es un factor limitante, al menos aliente a los miembros y al personal a usar las funciones integradas de "Buscar mi dispositivo" en sus teléfonos inteligentes personales y expedidos por el parlamento, como Find My iPhone, de iPhone, y Find My Device, de Android.

¿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. Debería configurar todos los dispositivos en el parlamento con algo llamado **cifrado de disco completo** si es posible. 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 usan macOS brindan una función llamada FileVault que se puede activar para cifrar todo el disco. Las computadoras con Windows que ejecutan licencias profesionales, empresariales o educativas ofrecen una función llamada BitLocker que se puede activar para cifrar el disco completo. 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 todo el disco si acceden a "Actualización y seguridad > 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 verse una subsección de "cifrado" o "cifrado y credenciales", que le indicará si su teléfono está cifrado y, si no, le permitirá activar esa función.

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 completo, asegúrese de guardar estas llaves o contraseñas en un lugar seguro, como una cuenta segura en la nube o el administrador de contraseñas de su parlamento.

ACCESO REMOTO A DISPOSITIVOS, TAMBIÉN CONOCIDO COMO PIRATERÍA

Además de mantener los dispositivos físicamente seguros, es importante mantenerlos libres de malware. En la publicación Security-in-a-Box de Tactical Tech se ofrece una descripción útil de lo que es el malware y por qué es importante evitarlo, 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.

Sin importar cómo se llamen ni cómo se distribuyan, el malware puede estropear computadoras, robar y destruir datos, alterar operaciones parlamentarias, invadir la privacidad y poner en peligro a los usuarios. En resumen, el malware es realmente peligroso. Sin embargo, existen algunos pasos simples que su parlamento puede seguir 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 punto de partida. El malware cambia con mucha rapidez, y hay nuevos riesgos en el mundo real con gran frecuencia: por eso 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 solo herramientas antimalware o antivirus de buena reputación de fuentes legítimas (como los sitios web en los enlaces mencionados). Por desgracia, existen muchas versiones falsas o comprometidas de herramientas contra malware que hacen mucho más daño que bien.

En la medida en que utilice Bitdefender u otra herramienta antimalware en su parlamento, asegúrese de no ejecutar dos de ellas al mismo tiempo. Muchas identificarán el comportamiento de otro programa contra el malware como sospechoso y detendrán su ejecución, y quedarán 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.

Mantenga los dispositivos actualizados

Las actualizaciones son esenciales. Use la última versión de cualquier sistema operativo que se ejecute en un dispositivo (Windows, Mac, Android, iOS, etc.), y manténgalo al día. Mantenga también actualizado el resto del software, el navegador y los complementos que tenga. Instale las actualizaciones tan pronto como estén disponibles: lo ideal es activar las actualizaciones automáticas. Cuanto más actualizado esté el sistema operativo de un dispositivo, menos vulnerabilidades tendrá. Piense en las actualizaciones como poner un apósito en una herida abierta: sella una vulnerabilidad y reduce en gran medida la posibilidad de que 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.

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? Por sistemas operativos Windows desactualizados y "sin parches", muchos de los cuales se piratearon en un principio. 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, **piense 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 en forma segura en todo el parlamento, 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 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.

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.

¿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 la empresa o el desarrollador adecuados hayan creado una aplicación, que tenga buenas críticas y la cantidad de descargas esperada (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.

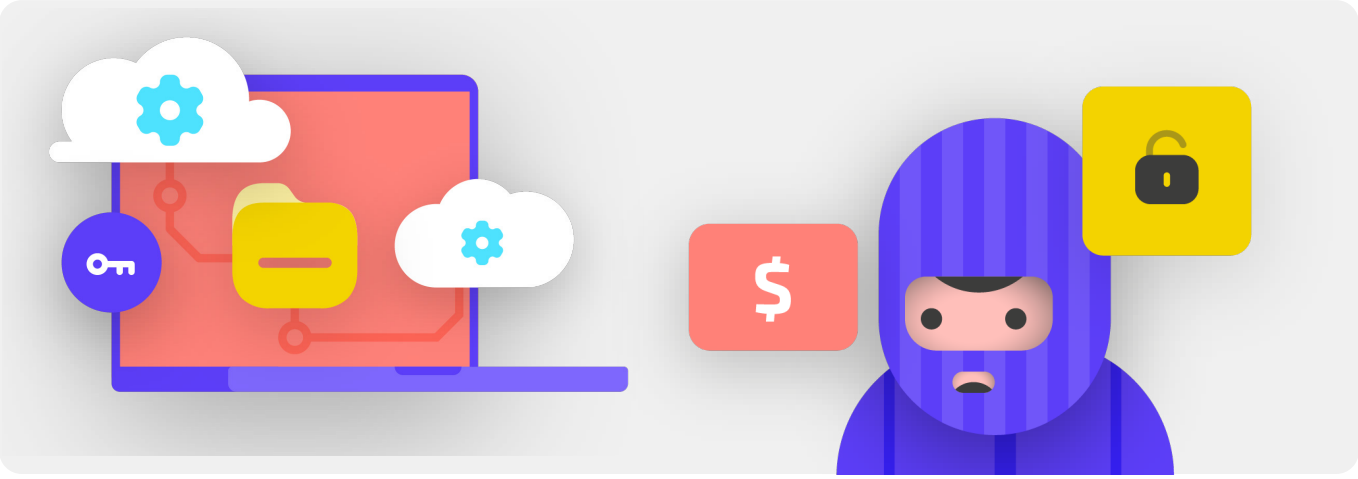
Mantener la Seguridad de los Dispositivos

- **Capacite a los miembros y 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 bien actualizados.**
  - Active las actualizaciones automáticas siempre que sea posible.
- **Inscriba todos los dispositivos parlamentarios en un dispositivo móvil o en un sistema de manejo de terminales.**
- **Asegúrese de que todos los dispositivos utilicen software con licencia.**
- **Exija la protección con contraseña de todos los dispositivos parlamentarios, incluidos los dispositivos móviles personales que se utilizan para comunicaciones relacionadas con el parlamento.**
- **Habilite el cifrado de disco completo en los dispositivos.**
- **Recuerde con frecuencia al personal que mantenga la seguridad física de sus dispositivos, y maneje la seguridad de su oficina con cerraduras adecuadas y formas de proteger las computadoras.**
- **No use dispositivos USB para compartir archivos, ni conecte esos dispositivos a sus computadoras.**
  - Utilice opciones alternativas para compartir archivos de forma segura.

Phishing, o Suplantación de Identidad: Una Amenaza Común para Dispositivos y Cuentas

El phishing es el ataque más común y eficaz contra las organizaciones de todo el mundo, incluidos los parlamentos. 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"). Con los mensajes de phishing pueden intentar hacerlo escribir 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) por mensaje de voz o 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?

El phishing puede parecer siniestro e imposible de atrapar, pero hay algunas simples medidas que todos en el parlamento pueden tomar para protegerse contra la mayoría de los ataques. Los siguientes consejos de defensa contra el phishing se modificaron y ampliaron a partir de la guía detallada desarrollada por la Fundación para la Libertad de Prensa, y deberían compartirse con todos en el parlamento y sus alrededores 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.

Phishing y Parlamentos

Thu 4/8/2021 8:48 AM

[redacted] <[redacted]@aop.gov.af>

Kindlty mention this email Most Urgent.

To [redacted]@nsc.gov.af

Message | NSC Press conference.rar (38 KB)

Yesterday I called your office and no one answered it. We have received your file and modified it. There is an error in the third line of the second page. Please confirm whether the error exists.
File Pass: nsc2021
Press conference by 5:00PM.

Regards | [redacted]

[redacted]

Press office | Spokesman
Presidential Palace (ARG) | Islamic Republic of Afghanistan
Mobile: [redacted] | [redacted] | [redacted] | ocs.gov.af
Mail: [redacted] | [redacted]

En forma habitual los parlamentos y otros actores gubernamentales de todo el mundo sufren sofisticados ataques de phishing personalizados.

Algunos funcionarios parlamentarios federales y locales en Alemania fueron blanco de correos electrónicos de phishing en el período previo a las elecciones en el otoño de 2021. Apenas unos meses antes en Afganistán, un grupo de piratas informáticos **utilizó técnicas de phishing para infiltrarse con éxito** en el antiguo Consejo de Seguridad Nacional, para lo que asumieron la identidad del portavoz de prensa del expresidente afgano Ashraf Ghani. Los malhechores enviaron correos electrónicos de phishing (como el que se ve aquí) que pedían a las víctimas que abrieran un archivo adjunto que, según el "vocero", contenía un error. Cuando lo descargaron y abrieron para "confirmar el error", el archivo adjunto malicioso desplegó malware que otorgó acceso sostenido a las computadoras. Ese acceso permitió a los piratas informáticos cargar y descargar archivos, ejecutar comandos en los dispositivos a voluntad y robar datos gubernamentales altamente confidenciales.

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 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 hacerlo, el archivo adjunto debería abrirse solo en un entorno seguro (vea la sección Avanzado más adelante), donde no pueda desplegarse un potencial malware en su dispositivo.

Si utiliza Gmail y recibe un archivo adjunto en un mensaje de correo electrónico, en lugar de descargarlo y abrirlo en su computadora, solo haga clic en el archivo 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 documentos de texto, archivos 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, el mejor enfoque es simplemente no descargar nunca archivos adjuntos de remitentes que no conozca o en los que no confíe, y sin considerar lo importante que pueda parecer, nunca se debe abrir algo con un tipo de archivo que no reconozca o no tenga intención de usar nunca.

Defensa contra el Phishing para su Parlamento

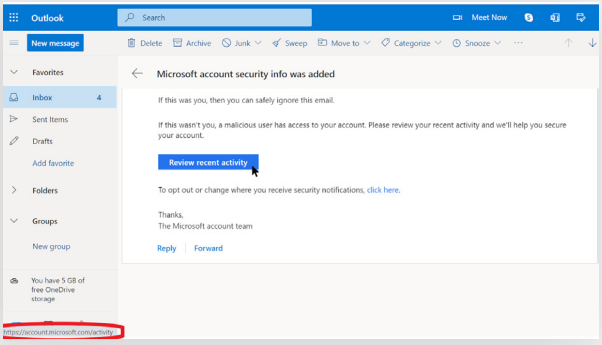
Si en su parlamento utilizan Microsoft 365 empresarial para el correo electrónico y otras aplicaciones, el administrador del dominio debería configurar la política de archivos adjuntos seguros para protegerse contra los envíos adjuntos peligrosos. Si se utiliza el Google Workspace para empresas (antes conocido como GSuite), existe una opción igualmente eficaz que el administrador debe configurar, denominada Google Security Sandbox. Los usuarios individuales más avanzados pueden considerar configurar sofisticados programas de Sandbox, como DangerZone o, quienes tengan la versión Pro o Enterprise de Windows 10, Windows Sandbox. Otra opción avanzada para considerar implementar en todo el parlamento es un servicio de filtrado de sistema de nombres de dominio (DNS) seguro.

En los parlamentos se puede utilizar esta tecnología para bloquear al personal e impedir que accedan o interactúen por accidente con contenidos maliciosos, lo que proporciona una capa adicional de protección contra el phishing. Hay nuevos servicios como Gateway de Cloudflare que brindan tales capacidades a las organizaciones sin requerir grandes sumas de dinero. 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. Cuando está en una computadora, hay un truco simple para asegurarse de que un enlace en un correo electrónico o mensaje lo envíe a donde se supone que debe hacerlo: use su mouse y páselo por encima de cualquier enlace antes de hacer clic en él, y mire en la parte inferior de la ventana de su navegador para ver cuál es la URL real (vea la imagen que figura a continuación).

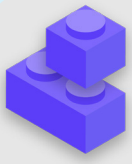
Es más difícil comprobar los enlaces de un correo electrónico en un dispositivo móvil sin hacer clic accidentalmente en ellos, así que tenga cuidado. Para revisar el destino de un enlace en la mayoría de los teléfonos inteligentes puede presionar en forma prolongada (mantener presionado) un enlace hasta 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 breve (por ejemplo, bit.ly o tinyurl.com) 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 abreviada. Además, no haga clic en enlaces a sitios web con los que no esté familiarizado. En caso de duda, realice una búsqueda, 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 con el escáner de URL de VirusTotal. Esto no es absolutamente exacto, pero es una buena precaución a tomar.



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 redirige al sitio apropiado. Muchos ataques de phishing proporcionan enlaces que lo enviarán 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 desea 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 dentro del parlamento recibe un archivo adjunto, enlace, imagen, mensaje o llamada sospechosos no solicitados, es importante que lo informe de inmediato a la persona o equipo encargados de la seguridad de TI. Si no tiene designada esa persona o equipo, debería identificarlos como parte del desarrollo de su plan de seguridad. El personal y los miembros también pueden denunciar el correo electrónico como spam o phishing directamente en Gmail o Outlook.
Es esencial tener un plan implementado sobre lo que el personal, los miembros o los voluntarios deberían hacer al recibir un posible mensaje de phishing. 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 todos, también puede poner en práctica cómo identificar phishing con el Google Phishing Quiz (Examen de Google sobre phishing). 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. Puede formalizarse como parte de reuniones habituales del equipo y parlamentarias, o llevarse a cabo de manera más informal. Lo importante es que todos los involucrados en las operaciones parlamentarias se sientan cómodos al hacer preguntas sobre phishing, informar incidentes de este tipo (incluso si sienten que podrían haber cometido un error al hacer clic en un enlace), y que todos tengan la facultad para ayudar a defender al parlamento contra esta amenaza de alto impacto y gran probabilidad.



Suplantación de Identidad

- **Capacite en forma periódica 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 a los miembros y al personal las mejores prácticas, como las siguientes:**
  - 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.
- **Aliente la denuncia del phishing.**
  - Establezca un mecanismo de denuncia y una persona encargada del phishing dentro del parlamento.
  - Premie los informes y no castigue los fracasos.

Comunicar y Almacenar Datos de Manera Segura

Comunicaciones e Intercambio de Datos

Para tomar las mejores decisiones en su parlamento 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 elementos más importantes de la seguridad de las comunicaciones se relaciona con mantener comunicaciones privadas de esa forma, de lo que en la era moderna se ocupa en gran medida el cifrado. Sin el cifrado adecuado, cualquier cantidad de adversarios podría ver las comunicaciones internas del parlamento. Las comunicaciones inseguras pueden exponer información y mensajes confidenciales o incómodos, revelar contraseñas u otros datos privados y poner en posible riesgo a sus miembros o personal, según la naturaleza de sus comunicaciones y el contenido que comparta. Como parlamento, también es importante asegurarse de que las comunicaciones gubernamentales oficiales de los miembros y el personal cumplan con todas las obligaciones abiertas pertinentes de Gobierno (como solicitudes de libertad de información) y los compromisos de seguridad de datos. Por lo tanto, al diseñar e implementar sistemas y políticas de comunicaciones seguras en todo el parlamento, asegúrese de tener en cuenta estos factores para que puedan protegerse como corresponde los mensajes pertinentes y, cuando sea necesario por ley, conservarlos.

Comunicaciones Seguras y Parlamentos

Ha habido muchos incidentes en los últimos años en los que se han visto comprometidos los sistemas de comunicaciones de los parlamentos y las cuentas de los MP y su personal, lo que ha provocado alteraciones en las operaciones parlamentarias y, en algunos casos, el robo de comunicaciones confidenciales. En julio de 2021, por ejemplo, las autoridades polacas anunciaron que **se piratearon las cuentas de correo electrónico de casi una docena de MP** locales, incluida una cuenta personal del principal asistente del primer ministro y cuentas de miembros de casi todos los grupos de oposición parlamentaria. Este informe llegó apenas unos meses después de que saliera a la luz una noticia similar sobre un ciberataque contra los sistemas de información y comunicación del **parlamento finlandés**. Las autoridades de Finlandia **describieron ese ataque** como "espionaje agravado e interceptación de mensajes" dirigido a su parlamento.

¿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 Autodefensa de Vigilancia de la Fundación Frontera Electrónica ofrece una explicación práctica (con gráficos) de lo que significa:

Mensajería No Cifrada

Sin ningún tipo de cifrado, nuestros mensajes quedan abiertos para que los lean adversarios potenciales, incluidos gobiernos extranjeros hostiles o piratas informáticos en la web. Ese cifrado es importante no solo para las comunicaciones parlamentarias internas sino también para las externas en las que es necesario proteger la privacidad y la integridad.

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 camino, una torre de telefonía celular (o en el caso de algo enviado por internet, su proveedor de servicios de internet, conocido como 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 retransmisión del mensaje, y cualquiera que tenga capacidad de echar un vistazo mientras va en camino, pueden 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 datos en movimiento: ***cifrado de la capa de transporte*** y ***cifrado de extremo a extremo***. Es importante conocer el tipo de cifrado que admite un proveedor de servicios cuando su parlamento toma decisiones para adoptar prácticas y sistemas de comunicación más seguros. Estas diferencias se describen bien en la guía de Autodefensa de Vigilancia , que se adapta de nuevo aquí:

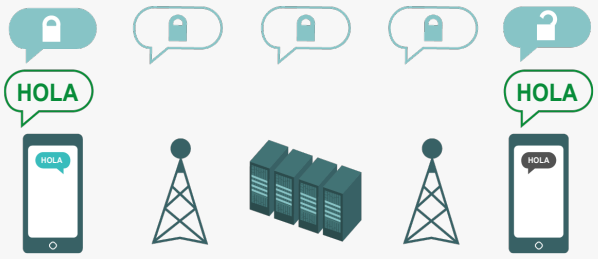
Cifrado en la Capa de Transporte

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 mientras viajan desde su dispositivo a los servidores de la aplicación o del servicio de mensajería y desde allí al dispositivo de su destinatario. Esto los protege de miradas indiscretas de los piratas informáticos que se encuentran en su red o de 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 verlos los servidores de la empresa (y muchas veces se almacenan en ellos), pueden ser vulnerables a solicitudes de la policía o a 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 puede "escuchar" ni espiar su actividad, ni siquiera la aplicación o el servicio que utiliza.



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. En el extremo, 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?

Al decidir si su parlamento necesita cifrado de capa de transporte o de extremo a extremo para sus comunicaciones (o alguna combinación de ambos para diferentes sistemas y actividades), las grandes preguntas que debería hacerse 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 extranjero hostil pudiera obligar a la empresa a entregarles los mensajes suyos y, si así fuera, confía en las políticas de la empresa para protegerse contra pedidos de policías extranjeras?

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.

Otro conjunto de preguntas a considerar es si, como parlamento, usted está obligado por ley a mantener acceso exclusivo a las comunicaciones parlamentarias, si existen requisitos de localización de datos en su país y si deben conservarse ciertas comunicaciones (por ejemplo, que el personal no las borre en forma permanente) para cumplir con leyes y compromisos abiertos del Gobierno. Si es así, podría considerar un sistema de comunicaciones de nivel empresarial con cifrado de extremo a extremo en el que usted, como parlamento, pueda controlar las claves de cifrado por sí mismo. Dichos sistemas (que se analizarán con más detalle en la sección **"Almacenamiento seguro de datos"** del Manual) pueden ser poderosos, pero requieren habilidades técnicas avanzadas para su implementación.

Cuando los envíe 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 con cuidado aplicaciones y sistemas seguros, es importante que todos los miembros del grupo sigan otras buenas prácticas de seguridad en cuentas y 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 DEBERÍAMOS HACER CON EL CORREO ELECTRÓNICO?

En general, el correo electrónico no es la mejor opción cuando se trata de seguridad. Incluso las mejores opciones de correo electrónico cifrado de extremo a extremo suelen dejar algo que desear desde una perspectiva de seguridad; por ejemplo, no cifran la línea de asunto y no protegen los metadatos (un concepto importante que se describirá más adelante). Si necesita comunicar información muy sensible que no es necesario retener para el registro público, tenga en cuenta que es mejor evitar el correo electrónico (ya sea el sistema del parlamento o, más en especial, la cuenta personal de alguien) y es preferible usar opciones de mensajería segura (que se resaltarán en la siguiente sección).

Sin embargo, como parlamento, es posible que aún desee o necesite que los miembros y el personal comuniquen contenido confidencial o privado mediante un sistema que se administre en forma centralizada como parte de sus operaciones diarias. Un sistema de correo electrónico para todo el parlamento, con controles de cuenta apropiados, por supuesto, puede ser útil aquí. Si, según su análisis anterior, el cifrado de la capa de transporte es suficiente, entonces las ofertas comerciales estándar de los proveedores de correo electrónico como Google Workspace (Gmail) y Microsoft 365 (Outlook) podrían ser opciones sólidas para su parlamento. Sin embargo, si le preocupa que su proveedor de correo electrónico pudiera tener la obligación legal de proporcionar información sobre sus comunicaciones a un gobierno extranjero u otro adversario, o si los requisitos de residencia de datos locales pueden ser una preocupación, querrá considerar el uso de una opción de correo electrónico cifrado punto a punto. Algunas de esas opciones incluyen agregar su propia administración de claves de cifrado a Google Workspace o Microsoft 365 (como se describe en la sección **"Almacenamiento seguro de datos"** de este manual), o adoptar servicios de correo electrónico cifrados de extremo a extremo diseñados para grandes organizaciones como **ProtonMail**. Negocios o **Tutanota** Negocios.

¿QUÉ SON LOS METADATOS Y QUÉ DEBERÍA PREOCUPARNOS SOBRE ELLOS?

Con quién hablan usted y su personal, los miembros y equipos, y cuándo y dónde lo hacen muchas veces puede ser tan sensible como el tema del que hablan. 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 Autodefensa de Vigilancia de la EFF ofrece una visión general de los metadatos y de por qué son importantes (incluida una ilustración de cómo se ven 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

Si bien es esencial la transparencia de las operaciones parlamentarias correspondientes, también es importante limitar el acceso no autorizado a los metadatos (además de proteger el contenido de las comunicaciones). Después de todo, los metadatos pueden revelar información confidencial a piratas informáticos, gobiernos extranjeros, empresas u otras personas que usted quizás no desearía que tuvieran acceso. Estos son un par de ejemplos de cómo se pueden revelar los metadatos:

Saben que un MP o un integrante del personal llamó a un periodista y habló con él durante una hora antes de que ese periodista publicara una noticia con una cita anónima. Sin embargo, no saben de lo que hablaron.

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

Herramientas Recomendadas para las Comunicaciones Cifradas de Extremo a Extremo

MENSAJES DE TEXTO (INDIVIDUALES O GRUPALES)	• **Signal** • **WhatsApp (solo con configuraciones específicas detalladas a continuación)**
LLAMADAS DE AUDIO Y VIDEO	• **Signal (hasta 40 personas)** • **WhatsApp (hasta 32 personas en audio, ocho en video)**
ARCHIVOS COMPARTIDOS	• **Signal** • **Keybase/Keybase Teams** • **Tresorit**

¿QUÉ HERRAMIENTAS DE MENSAJERÍA CIFRADA DE EXTREMO A EXTREMO DEBERÍAMOS UTILIZAR (A PARTIR DE 2022)?

Si necesita utilizar el cifrado de extremo a extremo, o solo quiere adoptar la mejor práctica sin importar el contexto de amenazas de su parlamento, estos son algunos ejemplos de servicios de confianza que, **a partir de 2022**, ofrecen mensajería y llamadas cifrados de extremo a extremo. Esta sección del Manual se actualizará en forma periódica en línea, pero tenga en cuenta que todo cambia con rapidez en el mundo de la mensajería segura, por lo que es posible que estas recomendaciones no estén al día en el momento en que usted lee esta sección. Tenga en cuenta también que sus comunicaciones son tan seguras como su mismo 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.

Los metadatos no están protegidos por el cifrado que ofrecen 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, todavía es posible que otros sepan con quién se comunica, con qué frecuencia y, con las llamadas telefónicas, durante cuánto tiempo. Como resultado, debería tener en cuenta qué riesgos existen (si los hay) si ciertos adversarios pueden averiguar con quién habla, cuándo habló con ellos y (en el caso del correo electrónico) las líneas generales de asunto de su comunicaciones parlamentarias.

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.

Esto puede no ser crítico para la mayoría de las comunicaciones parlamentarias, pero es importante estar al tanto de los riesgos que plantean los metadatos y seleccionar en consecuencia las herramientas y políticas de comunicación apropiadas.

¿PODEMOS CONFIAR EN VERDAD EN WHATSAPP?

WhatsApp es una opción popular para la mensajería segura, y puede ser buena, 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 realmente esencial es que se asegure de desactivar las copias de respaldo en la nube o, al menos, que habilite la nueva función de copias de respaldo cifradas de extremo a extremo de WhatsApp con el uso de una clave de 64 dígitos o una contraseña larga, aleatoria y única guardada en lugar seguro (como su administrador de contraseñas). También asegúrese de mostrar notificaciones de seguridad y verificar los códigos de seguridad. Puede buscar guías sencillas para configurar estos ajustes en 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 con eficacia) y deberían evitarse para cualquier cosa que no deba darse a 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 seguros y **evitar los mensajes de texto para todo lo que sea remotamente sensible, privado 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 se lo activa en forma deliberada (y solo en chats entre dos personas), por lo que no son buenas opciones para mensajes sensibles o privados, en especial de equipos. 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 COLEGAS PARLAMENTARIOS Y ELECTORES UTILIZAN OTRAS APLICACIONES Y SISTEMAS DE MENSAJERÍA PARA COMUNICARSE. ¿CÓMO PODEMOS CONVENCERLOS DE QUE DESCARGUEN UNA NUEVA APLICACIÓN PARA COMUNICARSE CON NOSOTROS?

A veces hay que sacrificar la comodidad por la seguridad, pero un pequeño esfuerzo extra merece la pena con comunicaciones sensibles. Sea un buen ejemplo para sus contactos, ya sea en otros organismos e instituciones gubernamentales, en el parlamento o electores externos. Si tiene que utilizar otros sistemas menos seguros, sea muy consciente de lo que dice. Evite hablar de temas delicados. Algunos parlamentos pueden tener diferentes protocolos para conversaciones generales u orientadas al público en comparación con diálogos confidenciales con los directivos, por ejemplo. Clasifique sus comunicaciones parlamentarias (internas y externas) en función de la sensibilidad y asegúrese de que los miembros y el personal usen los mecanismos de comunicación apropiados de manera acorde. Por supuesto, lo más simple es que se haga un cifrado automático de todo en todo momento: no hay que recordar nada 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 todos entiendan la importancia, los pocos minutos necesarios para descargar una nueva aplicación y el par de días que podría llevar acostumbrarse a usarla no parecerán un gran problema.

¿HAY OTRAS CONFIGURACIONES PARA APLICACIONES CIFRADAS DE EXTREMO A EXTREMO QUE DEBERÍAMOS CONOCER?

En la aplicación Signal, también es importante verificar 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 alguien más del personal necesitan ayuda para configurar estos ajustes, en el mismo Signal se **proporcionan instrucciones útiles.** Si utiliza Signal, ampliamente considerada como la opción más fácil de usar para mensajería segura y llamadas personales, asegúrese de establecer también un pin sólido. Utilice al menos seis dígitos, y algo que no sea fácil de adivinar, como su fecha de nacimiento. Para obtener más consejos para configurar **Signal** y **WhatsApp** en forma correcta, puede revisar las **guías de herramientas** para ambos desarrolladas por la EFF en su **Guía de Autodefensa de Vigilancia.**

¿QUÉ OCURRE 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 grupos grandes de su oficina o reuniones masivas virtuales de MP. 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.

Las necesidades específicas de las sesiones plenarias y las reuniones de comités se analizarán más adelante en este Manual, pero para sus otras reuniones más generales que no requieren funciones de colaboración como compartir pantalla o salas privadas, hay un par de opciones. Para grupos de hasta ocho personas, se recomienda enfáticamente el uso de Signal. En Signal, las videollamadas en grupo pueden realizarse desde un teléfono inteligente o desde la aplicación de escritorio de Signal en una computadora. Sin embargo, tenga en cuenta que solo sus contactos que ya utilizan Signal pueden ser añadidos a un grupo de Signal.

Si busca otras opciones, una plataforma que acaba de agregar una opción de cifrado de extremo a extremo es **Jitsi Meet.** Es una solución para conferencias en audio y video en la web que puede funcionar para una gran concurrencia de público (hasta 100 personas) y no requiere la descarga de una aplicación o 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 deteriorarse. 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 cifrado de extremo a extremo, eche un vistazo a estas **instrucciones** que se resumen en 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 sus equipos, 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 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 soporte y seguir **estas instrucciones** para asegurarse de que se configure. 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 códigos de acceso sólidos 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 configurar mal por accidente estas características, no es ideal confiar en Zoom como opción cifrada 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 revisar cualquier llamada antes de que se inicie para asegurarse de que en verdad está cifrada de extremo a extremo, para lo que deberá hacer clic en el candado verde del extremo superior izquierdo de la pantalla de Zoom y ver 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.

Sin embargo, cabe señalar que ciertas características populares de las herramientas mencionadas solo funcionan con cifrado de la capa de transporte. Por ejemplo, al activar el cifrado de extremo a extremo en Zoom se desactivan las salas privadas, las capacidades de encuestas y la grabación en la nube. En Jitsi Meet, al activar salas privadas puede desactivarse la función de cifrado de extremo a extremo, lo que provoca una disminución involuntaria de la seguridad.

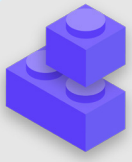
NOTA SOBRE EL INTERCAMBIO DE ARCHIVOS

Además de compartir mensajes en forma segura, es probable que hacer lo mismo con archivos sea una parte importante del plan de seguridad de su parlamento. La mayoría de las opciones para compartir archivos están integradas en las aplicaciones de mensajería o 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 parlamento. Tiene que asegurarse de configurar en forma correcta las funciones de uso compartido de manera que solo las personas adecuadas tengan acceso a un determinado documento o carpeta, y cerciorarse 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 USB dentro de su parlamento aumenta de manera considerable la probabilidad de malware o robo y confiar en el correo electrónico u otras formas de archivos adjuntos debilita las defensas de su parlamento contra los ataques de phishing.

¿Y SI EN VERDAD NO NECESITAMOS CIFRADO DE EXTREMO A EXTREMO EN TODAS NUESTRAS COMUNICACIONES?

Si no es necesaria esa función para todas las comunicaciones de su parlamento según su evaluación de riesgos, puede considerar el uso de aplicaciones protegidas por cifrado de 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 pudieran tener obligación de compartir información) pueden ver y oír 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 (mediante Google Workspace)** • **Outlook (a través de Office 365)** • No aloje su propio servidor de Microsoft Exchange para el correo electrónico de su parlamento. Si lo hace actualmente, debería migrar a Office 365.
MENSAJES DE TEXTO (INDIVIDUALES O GRUPALES)	• **Google Hangouts** • **Slack** • **Microsoft Teams** • **Mattermost** • **Line** • **KaKao Talk** • **Telegram**
CONFERENCIAS GRUPALES, LLAMADAS DE AUDIO Y VIDEO	• **Jitsi Meet** • **Google Meet** • **Microsoft Teams** • **WebEx** • **GotoMeeting** • **Zoom**
ARCHIVOS COMPARTIDOS	• **Google Drive** • **Microsoft Sharepoint** • **Dropbox** • **Slack** • **Microsoft Teams**



Comunicar Datos en Forma Segura

- **Clasifique las comunicaciones en función de su sensibilidad.**
  - Determine los sistemas y herramientas apropiados para la comunicación en consecuencia.
  - Establezca una política sobre cuánto tiempo conservará los mensajes por consiguiente, si se tienen en cuenta tanto la seguridad como los compromisos con la transparencia parlamentaria.
- **Requiera el uso de servicios confiables de mensajería cifrada de extremo a extremo para comunicaciones confidenciales de su parlamento.**
  - 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.
- **Asegúrese de que se han implementado configuraciones apropiadas de las aplicaciones de comunicaciones, 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.
- **No intente alojar su propio servidor de correo electrónico: use servicios de correo electrónico basados en la nube como Office 365 o Google Workspace como alternativas.**
  - No permita que el personal utilice cuentas de correo electrónico personales para trabajar.
- **Recuerde con frecuencia al personal y a los miembros las mejores prácticas de seguridad relacionadas con mensajes grupales y metadatos.**
  - Esté atento a quién se incluye en los mensajes de grupo, chats e hilos de correo electrónico.

Parlamentos Digitales (parlamento electrónico)

Como parlamento, es importante prestar especial atención a las políticas de seguridad operativa y de comunicaciones de sus funciones más esenciales, incluidas las que tienen lugar en línea y en el espacio digital.

Ya sea que su parlamento considere instalar un sistema completo de "parlamento electrónico" en el que se pueda digitalizar todo, desde la redacción de proyectos de ley hasta debates y votación electrónica (como Nextsense, Propylon o Granicus, por nombrar algunos ejemplos), o si utiliza herramientas más simples y menos costosas para facilitar sus operaciones parlamentarias, es esencial tener en cuenta cómo cualquier herramienta y proceso tienen presente la seguridad, la integridad y la disponibilidad de la información.

Seguridad y Parlamentos Digitales

Como lo demuestra una serie de incidentes en Sudáfrica, la transición de las operaciones parlamentarias al mundo digital requiere atención a la seguridad cibernética para evitar no solo la pérdida o el robo de datos confidenciales, sino también la vergüenza, el insulto y el daño potenciales a los miembros y al personal. En mayo de 2020, aparecieron imágenes pornográficas minutos antes del inicio de una reunión virtual de la Asamblea Nacional del país. Tras la exhibición de las imágenes ofensivas, el pirata informático o "bombardero de zoom" profirió insultos sexistas y raciales al orador de la asamblea que era anfitrión de la sesión, lo que obligó a suspender la reunión. Un incidente similar se produjo un mes antes cuando interrumpieron con imágenes pornográficas una reunión presidida por la ministra de las mujeres, la juventud y las personas con discapacidades.

SESIONES PLENARIAS Y REUNIONES DE COMITÉS REMOTAS

Entre esos procesos, los principales son las sesiones plenarias y las reuniones de comités. Esas sesiones y las conversaciones, decisiones y votaciones que tienen lugar en ellas son el núcleo de gran parte del trabajo de su parlamento y, como tales, pueden ser un blanco particular de sus adversarios. En un mundo moderno e impactado por una pandemia, tales sesiones y reuniones se llevan a cabo de manera cada vez más diversa según el contexto de su país: en persona, completamente en línea o con un modo "híbrido".

Como se describe en la reciente guía de **Parlamentos en respuesta a una pandemia** de House Democracy Partnership, la estructura de debate parlamentario típica es diferente de una charla en conferencia normal o una reunión estándar de una organización. Las necesidades de votación a distancia, la presentación de propuestas y enmiendas oficiales, el debate estructurado e incluso la interpretación simultánea para garantizar la inclusión de todos los electores muchas veces requieren características adicionales que no se encuentran en la mayoría de las soluciones tecnológicas estándar. Como resultado, al organizar una sesión virtual o híbrida, es probable que su parlamento necesite desarrollar (o ya haya desarrollado) software personalizado, o compre soluciones empresariales costosas (como **Webex Legislate de Cisco**) diseñadas de manera específica para administrar sesiones parlamentarias remotas. Cualquiera sea la opción que elija su parlamento, es importante reflexionar, como se describe en la guía **Parlamentos en respuesta a una pandemia**, sobre cómo todos los miembros y el personal podrán acceder a ese sistema. También es esencial asegurarse de que el sistema esté protegido como se debe.

Al crear e implementar soluciones técnicas para las sesiones parlamentarias, es importante cerciorarse de que se implementen las normas básicas de seguridad. Estas incluyen pasos para garantizar que los datos estén protegidos "en reposo" dentro del propio sistema, que se cifren en forma correcta mientras están en tránsito, y que solo usuarios autorizados puedan acceder al sistema. Hay muchos enfoques que se pueden adoptar para garantizar dicha seguridad, incluidos muchas de las normas básicas descritas en el resto de este Manual. El cifrado de extremo a extremo en cualquier sistema de comunicación e intercambio de datos utilizado, una contraseña fuerte y requisitos de autenticación de dos factores o restricción de dirección IP para que los usuarios accedan a dichos sistemas (a menos que estén destinados a estar abiertos al público), el requisito de redes privadas virtuales (que se analizarán más adelante en el manual) y la limitación de acceso solo a dispositivos confiables y limpios son todos pasos útiles.

VOTO A DISTANCIA

La necesidad de una seguridad resistente es quizás más crítica cuando se trata de votación remota. Como se destaca en la mencionada guía de **Parlamentos en respuesta a una pandemia**, se elige a los MP para el parlamento con el propósito específico de que voten en nombre de sus electores. La capacidad de confiar y verificar estos votos es esencial no solo para el funcionamiento de su parlamento sino para el sistema democrático en su conjunto. Dichos votos se verifican con relativa facilidad cuando vota un MP en persona, pero cuando su participación es virtual, la autenticación técnica se convierte en un desafío mayor que requiere cuidado y concentración significativos. Como se describe en el **testimonio** de expertos brindado al Comité Permanente de Procedimiento y Asuntos Internos de la Cámara de los Comunes de Canadá, los parlamentos suelen elegir una de cuatro opciones para la votación remota:

- votación por correo electrónico, en la que los miembros reciben un formulario de votación por la vía electrónica y envían su voto por correo electrónico. Esta opción se considera en general insegura, en parte debido a su falta de cifrado de extremo a extremo, y debería evitarse;
- votación por web, en la que los miembros acceden a un sitio web en una computadora o teléfono celular y allí emiten sus votos. Para este enfoque se requiere inversión en infraestructura segura, incluidos dispositivos seguros con fuertes controles de autenticación, como los ya mencionados;
- votación por aplicaciones, para las que los miembros descargan una aplicación a la cual acceden y donde emiten su voto. Es similar a la votación por la web, pero se utiliza una aplicación específica que se puede descargar a un teléfono o tableta en lugar de acceder desde un navegador;
- votación por video, en la que los miembros votan en pantalla a mano alzada o por voz. Esta votación no anónima puede ser técnicamente menos complicado y técnicamente menos sofisticado de configurar y asegurar. Pero igual se requieren sistemas robustos de cifrado y autenticación para evitar la suplantación o interrupciones durante las sesiones de votación.

Cualquiera sea la opción que su parlamento elija implementar para votaciones remotas, si las realiza, también es importante abordar los aspectos básicos de ciberseguridad a lo largo de todo el proceso de votación. Estas reglas fundamentales incluyen garantizar que los dispositivos que utilizan los MP para emitir votos estén tengan la correcta protección física y estén libres de malware, que el acceso a internet de los miembros esté bien protegido cuando votan (y también cuando realizan otros asuntos parlamentarios), y que tienen conexiones estables a internet y pueden votar cuando se los llama. Como se describe

en la guía de Parlamentos en respuesta a una pandemia, al adoptar el voto remoto, es necesario realizar pruebas exhaustivas del sistema antes de que entre en funcionamiento y brindar soporte y capacitación a los MP para garantizar que puedan usar el sistema con eficacia. Es importante recordar que parte de la seguridad es la *disponibilidad*. También existe la necesidad en particular de garantizar que las mujeres MP y del personal puedan usar los sistemas en línea a salvo, incluida la votación remota, y tengan acceso a la tecnología para hacerlo. Cuando las mujeres, en particular las electas, se conectan a internet, se enfrentan a mayores niveles de intimidación y acoso, y este factor debería tenerse en cuenta al desarrollar y utilizar tecnología como la votación remota para garantizar que todos los parlamentarios puedan cumplir con sus funciones de manera eficaz. Además, es fundamental garantizar un acceso multilingüe remoto adecuado en países donde los miembros y el personal hablan varios idiomas formales.

PROVEEDOR DE PARLAMENTO ELECTRÓNICO Y SEGURIDAD DE SOFTWARE

Cualquier software que adquiera, ya sea que se utilice para votación remota o una gama más amplia de necesidades parlamentarias, **debería provenir de una fuente segura y acreditada, contar con auditoría de seguridad de equipos independientes, y recibir las certificaciones correspondientes.** Es importante recordar que los desarrolladores de software, aquellos a quienes contrata para crear una aplicación o herramienta, no siempre son expertos en seguridad. Por lo tanto, traer expertos en seguridad para probar la aplicación en busca de potenciales brechas de seguridad pro medio de una auditoría es fundamental para reducir el riesgo de que pudieran piratear o poner en peligro su plataforma, herramienta o aplicación. Incluso los mejores desarrolladores de software cometen errores sin un segundo (o tercer) par de ojos expertos que controlen su trabajo.

Voto Remoto en el Mundo Real

Varios parlamentos han implementado sistemas de votación a distancia y, al hacerlo, tomaron medidas considerables para garantizar la seguridad e integridad de los votos de los miembros. Un elemento de este proceso, entre otros ya mencionados, es garantizar una autenticación adecuada. Un ejemplo es el de la Cámara de los Comunes del Reino Unido, donde los miembros usan un proceso de inscripción única para iniciar sesión en sus cuentas parlamentarias antes de votar, lo que requiere que se use una contraseña en un dispositivo asignado específico. En España, a los MP se les asignan códigos personales que deben ingresarse en una aplicación de teléfono inteligente antes de que se pueda registrar una votación en forma remota. En Chile, los senadores que votan mediante la aplicación de votación remota que diseñó la cámara con detalle deben estar visibles en la pantalla para emitir un voto.

Almacenamiento Seguro de Datos

En la mayoría de los parlamentos, una de las decisiones más importantes que deben tomarse 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 en servicios de almacenamiento en la nube de confianza. Quizás los ejemplos más comunes son Microsoft 365 y Google Drive. Sin un plan integral de almacenamiento en la nube, es probable que los datos de su parlamento se almacenen en una variedad de lugares, incluidas las computadoras del personal y de los MP, discos rígidos externos e incluso algunos servidores locales. 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.

Almacenamiento de Datos y Parlamentos

La llegada del almacenamiento de datos basado en la nube asequible (a veces gratuito) ha hecho la vida más fácil (y más segura) para muchos parlamentos y otras organizaciones. Por desgracia, muchos aún intentan alojar sus propios servidores con un presupuesto, personal y soporte de TI relativamente limitados. En marzo de 2021, la amenaza de esa infraestructura organizativa se volvió real para decenas de miles de organizaciones de todo el mundo, incluidos los parlamentos, 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 servidores locales, incluido el del parlamento de Noruega, lo que permitió a los piratas informáticos obtener acceso a las cuentas de correo electrónico del parlamento, instalar malware adicional en los servidores de la víctima y los sistemas conectados y, en última instancia, **extraer datos confidenciales.** Aunque Microsoft publicó una rápida actualización e instrucciones para identificar y eliminar a los potenciales intrusos, muchas organizaciones carecían de la capacidad informática para aplicar velozmente dichas actualizaciones, lo que las dejó expuestas durante largo tiempo. El alcance y el impacto de este ataque global revelan el peligro de que los parlamentos y otras organizaciones decidan autoalojar servidores de correo electrónico y otros tipos de datos confidenciales, en particular sin una inversión significativa en personal especializado en ciberseguridad.

BENEFICIOS DEL ALMACENAMIENTO EN LA NUBE

Aunque tome todas las medidas adecuadas para proteger sus computadoras contra el malware y el robo físico, igual es posible que un adversario decidido piratee su computadora o servidor parlamentario 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 confiable de almacenamiento en la nube será mucho más fácil y menos costosa de implementar y mantener segura en el tiempo. Entonces, en lugar de tratar de identificar (y retener) la cantidad de personal de ciberseguridad especializado y con excelentes habilidades que se requiere para proteger los servidores locales en su parlamento, concentre su energía en un puñado de tareas más simples. Esas tareas incluyen elegir la opción de almacenamiento en la nube adecuada para sus necesidades de localización y privacidad de datos, implementar una buena seguridad de la cuenta, capacitar al personal para compartir en forma correcta (y no compartir) carpetas y documentos (en general, debería configurar carpetas dentro de su unidad de almacenamiento en la nube que limiten el acceso solo al personal que lo necesita para determinados archivos), y auditar en forma rutinaria su sistema para asegurarse de que el personal y los miembros no "comparten de más" ningún archivo (por ejemplo, al activar el uso compartido de enlaces universales para archivos que, en cambio, deberían limitarse a solo algunas personas). Mantener la mayor parte de su información en la nube ayuda con una variedad de 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? ¿Necesita compartimentar datos que pertenecen a un MP en la información que genera para el propio parlamento? ¿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.

¿EN VERDAD PODEMOS CONFIAR EN EL ALMACENAMIENTO EN LA NUBE?

En resumen, no hay nada intrínsecamente poco confiable en el almacenamiento en la nube. Como ya se mencionó, la mayoría de los principales proveedores de almacenamiento en la nube tienen equipos de los mejores ingenieros de seguridad del mundo que trabajan para proteger sus productos todos los días y ofrecen soporte de seguridad a sus clientes más allá de lo que la mayoría de los departamentos de TI pequeños podrían proporcionar por sí mismos. Sin embargo, tenga en cuenta que los servicios tradicionales de almacenamiento en la nube en general requieren otorgar acceso a datos confidenciales a una empresa externa que brinda el servicio. **Dicho esto, cada parlamento individual tendrá sus propias consideraciones políticas y requisitos legales (como mandatos de localización de datos) que hacer al elegir si puede confiar en un proveedor de almacenamiento en la nube determinado, y usarlo.**

¿QUÉ PROVEEDOR DE ALMACENAMIENTO EN LA NUBE DEBERÍAMOS ELEGIR?

Si su parlamento no tiene que considerar ningún requisito de localización de datos y no tiene problemas con que una empresa externa de confianza comparta el acceso a los datos, las dos opciones de almacenamiento en la nube más populares son Google Workspace (antes conocido como GSuite) y Microsoft 365. Si su parlamento ya usa Gmail, tiene mucho sentido registrarse en Google Workspace y almacenar datos en Google Drive con sus aplicaciones integradas de Google Docs, Sheets y Slides para procesamiento de textos, hojas de cálculo y presentaciones de diapositivas. Del mismo modo, si su parlamento depende de Excel y Word, la opción más fácil es registrarse en Microsoft 365, que otorga acceso a Outlook para correo electrónico y versiones con licencia de Microsoft Word, Excel, PowerPoint y Teams.

¿QUÉ SUCEDE SI NECESITAMOS CONTROLAR NUESTROS PROPIOS DATOS O CUMPLIR CON LEYES DE LOCALIZACIÓN DE DATOS?

Para muchos parlamentos, una opción tan simple podría no ser factible dados los requisitos de localización de datos o las expectativas específicas que requieren un control parlamentario exclusivo sobre sus propios datos. La buena noticia es que hace poco los proveedores de almacenamiento seguro en la nube desarrollaron opciones que permiten a los clientes empresariales elegir la ubicación de sus datos (tenga en cuenta que esto se limita principalmente a los clientes europeos por ahora), o controlar sus propias claves de cifrado. **En la práctica, esto significa que su parlamento tiene opciones para controlar sus propios datos mientras se beneficia de la infraestructura y la seguridad del almacenamiento en la nube.**

Si su parlamento utiliza en la actualidad Google Workspace para almacenar y compartir datos en la nube, o le interesa hacerlo, Google introdujo una función que permite el **cifrado del lado del cliente** para organizaciones Enterprise Plus. Si bien en el presente se encuentra en una fase de prueba y solo está disponible para los planes más costosos de Google Workspace, esta función brinda una opción para aprovechar el conjunto completo de funciones de almacenamiento y uso compartido de datos de Google Drive, y las funciones de seguridad integradas, al tiempo que limita la capacidad de Google para acceder a información confidencial o privada de su parlamento. Con el cifrado del lado del cliente, puede elegir integrar un servicio de administración de claves adicional, como Virtru, y permitir que los usuarios administren sus propias claves de cifrado sin permitir el acceso al mismo Google. Dicho servicio requiere que todos tengan mucho cuidado en proteger esas claves para proteger bien el acceso a cualquier sistema de administración de claves que elija integrar en Google Workspace. Los administradores de cuentas pueden obtener más información sobre cómo habilitar el cifrado del lado del cliente en la **página de soporte** de Google Workspace.

Si en su parlamento usan en la actualidad Microsoft 365 para almacenar y compartir datos en la nube, o les interesa hacerlo, ofrece una opción un poco más compleja pero bien establecida para administrar sus propias claves de cifrado conocida como **Microsoft 365 Double Key Encryption.** Para esta opción de seguridad se requiere **Microsoft 365 E5**, pero permite mantener el control de cualquier información parlamentaria confidencial o privada y limitar el acceso incluso al propio Microsoft.

Tresorit es otra opción más simple de implementar si a su parlamento le preocupa permitir que un tercero acceda a su información interna. Proporciona cifrado de extremo a extremo para el almacenamiento en la nube y el uso compartido de archivos, y ofrece una gama de **opciones de residencia de datos.**

¿Y SI NO PODEMOS CONFIAR EN NINGUNA SOLUCIÓN DE ALMACENAMIENTO EN LA NUBE?

Si elige ir por su cuenta y confiar en los servidores locales para almacenar los datos de su parlamento, es esencial que invierta una cantidad considerable de tiempo y recursos en fortalecer las defensas digitales de los dispositivos de su parlamento y asegurarse de que dichos servidores cuenten con la configuración, el cifrado y la protección correctos, y tengan seguridad física. Como ya se indicó, este enfoque requiere identificar, contratar y retener una cantidad de personal de ciberseguridad dedicado y altamente calificado para mantener la seguridad de su infraestructura de servidor local.

Mejora de la Seguridad de las Cuentas Parlamentarias en la Nube

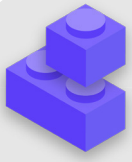
Si su parlamento elige configurar un dominio en Google Workspace o Microsoft 365, tenga en cuenta que ambas compañías ofrecen niveles más altos de seguridad a cuentas en riesgo. El **Programa de Protección Avanzada de Google** y **AccountGuard de Microsoft** proporcionan una seguridad aún más sólida 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 eficaz y pongan en riesgo la cuenta. Si cree que su parlamento califica y está interesado en inscribir a sus miembros y personal en cualquiera de los planes, visite los sitios web en los enlaces antes indicados o comuníquese con **cyberhandbook@ndi.org** para obtener más ayuda.

COPIA DE RESPALDO DE DATOS

Ya sea que su parlamento almacene datos en dispositivos físicos y servidores o en la nube, es importante tener una copia de respaldo. Tenga en cuenta que si confía en el almacenamiento de un dispositivo físico, 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 su robo junto con su maletín. 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 almacenamiento en la nube (como Google Drive), el riesgo de que derriben a Google 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. Explorar una solución de copia de respaldo en la nube como **Backupify** o **SpinOneBackup** puede valer la pena.

Si los datos se almacenan en un servidor local o en dispositivos locales, una copia de seguridad segura es aún más importante. Puede hacer una copia de respaldo de los datos de su parlamento en un disco rígido externo o en una serie de unidades, pero asegúrese de cifrarlas con una contraseña sólida. 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.



Almacenamiento Seguro de Datos

- **Almacene los datos sensibles exclusivamente en un servicio confiable 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 e implemente una política para limitar la configuración de uso compartido dentro de la nube.**
  - Capacite a todos los miembros y al personal sobre cómo compartir documentos en forma correcta (y no compartir demasiado).
- **Si su parlamento elige almacenar datos localmente, invierta en personal de TI capacitado.**
- **Mantenga las copias de respaldo de sus datos a salvo: realice el cifrado de los discos rígidos u otros dispositivos de respaldo.**

Mantenerse seguro en internet

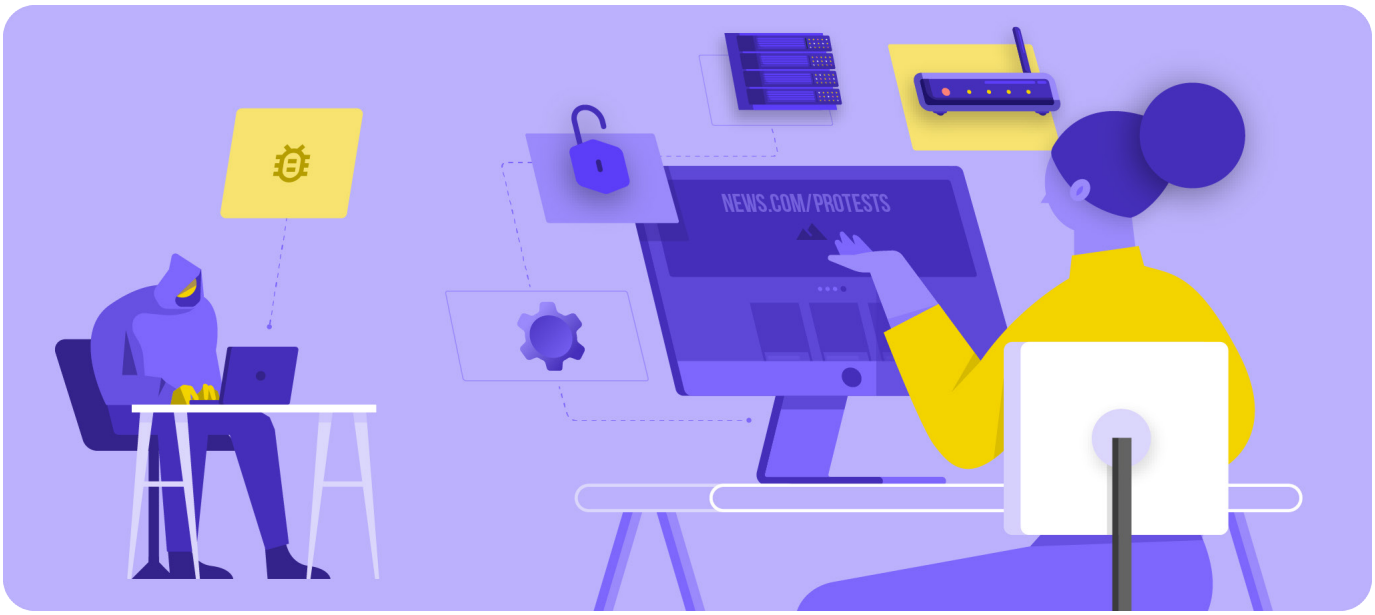
Al utilizar internet en su teléfono o computadora, su actividad puede decir bastante sobre usted y su organización.

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 su parlamento en línea es minimizar la cantidad de información disponible sobre la actividad suya y de sus colegas en internet. 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**, quedan expuestos la información que se teclea en un sitio (como contraseñas, números de cuenta o mensajes), los detalles del sitio y las páginas que visita. 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.



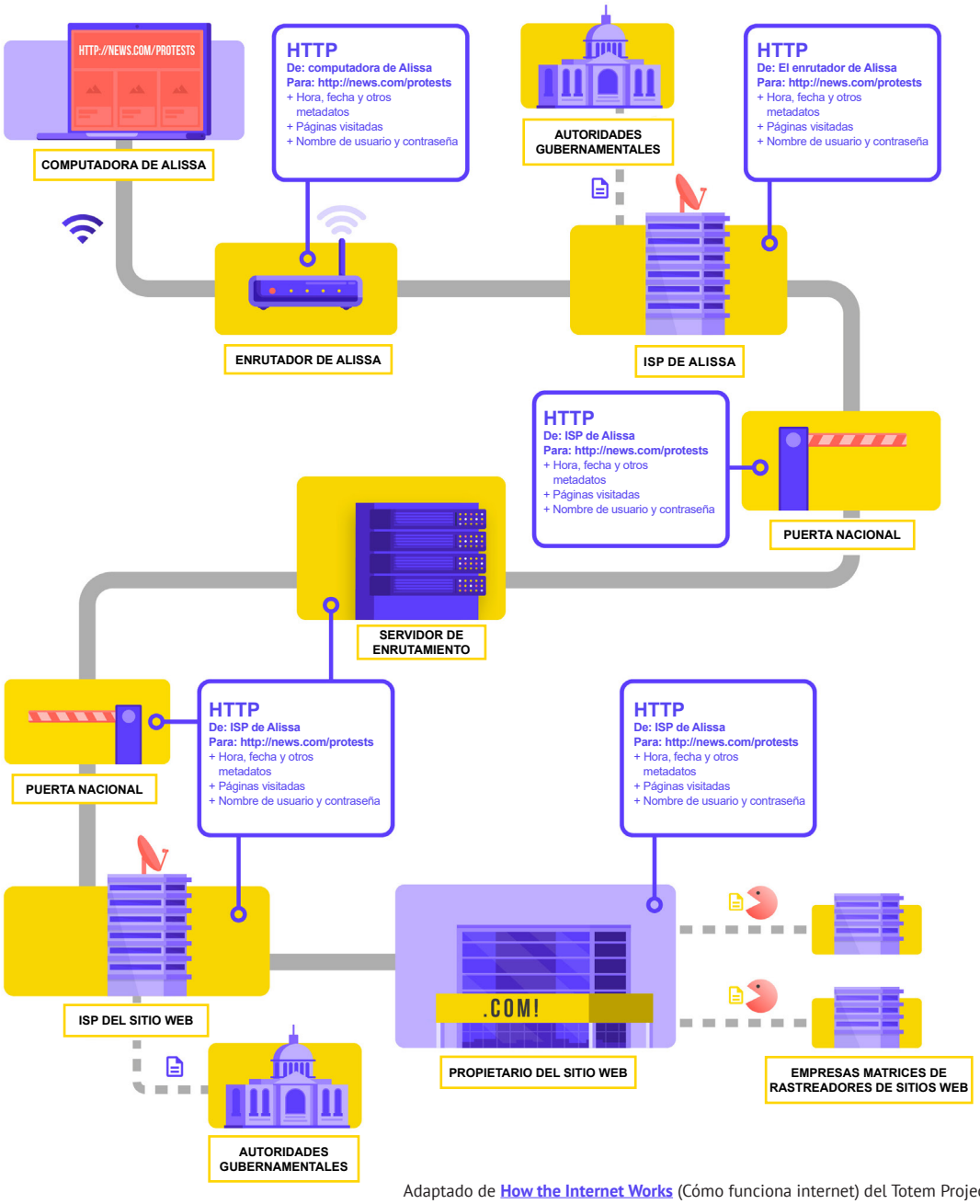
Vigilancia, Censura y Parlamentos

Hay gobiernos hostiles y otros actores de amenazas en todo el mundo que utilizan cada vez más tecnología de vigilancia accesible y, en algunos casos, simple piratería de Wi-Fi, para monitorear la actividad en línea de los MP y otras personas que trabajan en el parlamento. Por ejemplo, piratas informáticos robaron datos del personal del parlamento europeo y de visitantes mediante **suplantación de la red Wi-Fi pública del parlamento** en 2013. Una vista previa de ataques mucho más sofisticados que harían en años siguientes.

Además de secuestrar el tráfico de internet y robar datos, los adversarios también interrumpen las operaciones parlamentarias críticas al bloquear los sistemas y el acceso a la red. En Bruselas, el parlamento de Bélgica quedó desconectado por un **ataque masivo de denegación de servicio** en mayo de 2021. El ataque obligó a posponer algunos debates y reuniones de comités, ya que los usuarios no podían acceder a los servicios virtuales requeridos para participar en la sesión.

La creciente frecuencia de este tipo de ataques al acceso a información en línea y a la libertad de esta resalta lo esencial que es que los parlamentos entiendan los riesgos de operar en internet y la necesidad de desarrollar planes para conectarse cuando la conectividad se ve afectada.

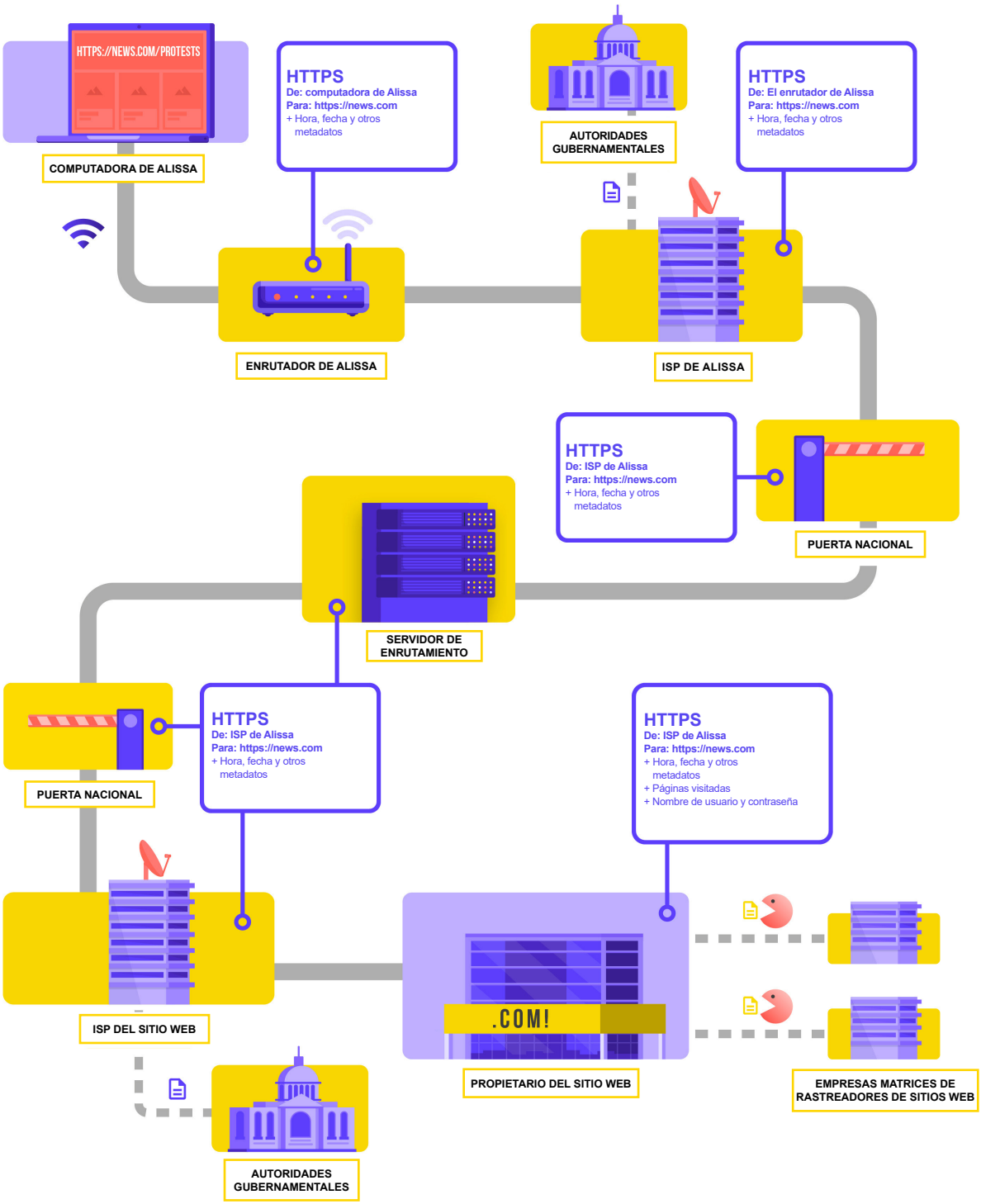
Veamos un ejemplo real de cómo es la navegación sin cifrado:



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

Al navegar sin cifrado, todos sus datos están expuestos. Como se presentó antes, un adversario puede ver dónde se encuentra, que visita news.com y mira la página específica sobre protestas en su país, y quizás lo más importante como MP o integrante del personal parlamentario, ve su contraseña, que usted comparte para iniciar sesión en el sitio. Tal información en las manos equivocadas no solo expone su cuenta, sino que también brinda a adversarios potenciales, en cualquier lugar del mundo en que se encuentren, una buena idea de lo que podría estar haciendo o pensando.

El uso de **HTTPS (la "s" indica "seguro") 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, aún puede ver qué dominios visita (por ejemplo, news.com). 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. Con el HTTPS implementado, un adversario podría saber que visita news.com, pero no podría ver su contraseña, y sería más difícil (pero no imposible) que viera que usted busca información sobre protestas (para usar ese 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 brinda cierta protección adicional contra el fisgoneo y el bloqueo de sitios, pero si a su parlamento le preocupa la vigilancia altamente selectiva con respecto a sus actividades en internet y enfrenta una sofisticada censura en línea (como el bloqueo de sitios web y aplicaciones), podría utilizar una red privada virtual (VPN, por sus siglas en inglés) de confianza.

Uso de un DNS Cifrado

Si desea hacer más difícil (pero no imposible) que un ISP conozca los detalles de los sitios web que visita, puede usar un DNS cifrado.

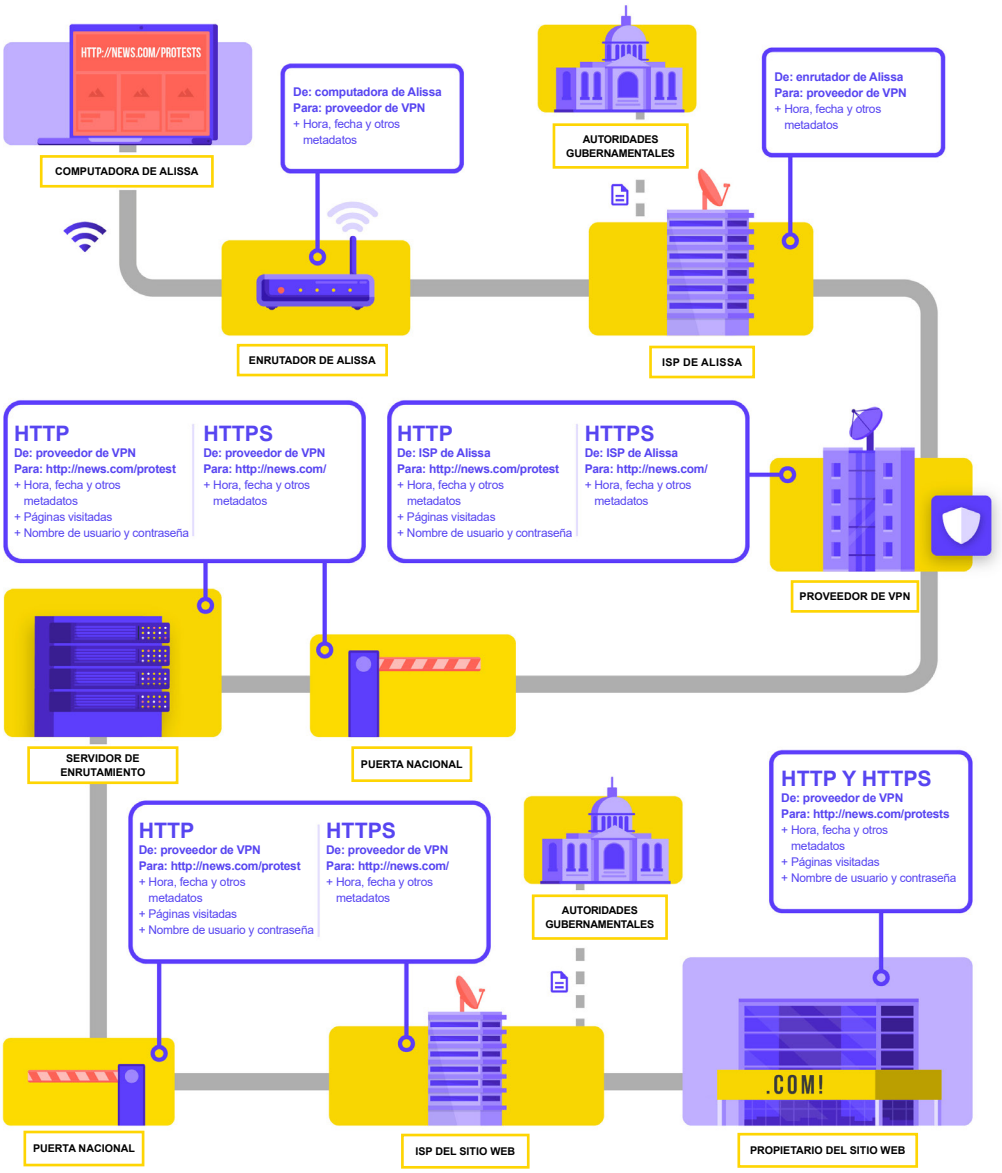
Si se lo **pregunta**, DNS significa "sistema de nombres de dominio". Es en esencia un directorio telefónico de internet, en el que se traducen nombres de dominio fáciles de usar para los seres humanos (como ndi.org) a direcciones de protocolo de internet (IP) fáciles de usar en la web. Esto permite 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 navegadores Chrome o Edge **pueden activar el DNS cifrado** con la configuración de seguridad avanzada del navegador para lo que deben activar "usar DNS seguro" y seleccionar "Con: Cloudflare (1.1.1.1)" o el proveedor de su preferencia.

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 por completo su ubicación de todos los sitios web que visita, es una característica fácil de usar que puede ayudar al personal de su parlamento 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 en esencia un túnel que protege contra la vigilancia y el bloqueo de tráfico de internet por parte de los hackers de su red, su administrador de red, su proveedor de servicios de internet y cualquier persona con la que pudieran compartir datos. En una organización grande, como un parlamento, las VPN "empresariales" o "corporativas" se usan también muchas veces para ayudar a proteger la integridad del acceso a sistemas y aplicaciones internos (como los que se usan para votación remota). Ya sea que use una VPN personal o una diseñada con fines comerciales, el concepto de proteger su tráfico de internet contra el espionaje en general funciona igual, y sigue siendo esencial continuar usando un HTTPS (incluso con la VPN instalada). También es fundamental asegurarse de que confía en la VPN que utiliza su parlamento. 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 (VPN) en mayor profundidad, en esta sección se hace referencia a la Guía de Autodefensa de Vigilancia de la 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 utiliza una VPN, lo que podría elevar su perfil de riesgo.

Esto significa que **es esencial elegir un proveedor confiable de VPN**. 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 parlamento y el personal, puede evaluarlas en función de su modelo de negocio y reputación, qué datos recogen o no y, por supuesto, la seguridad de la propia herramienta.

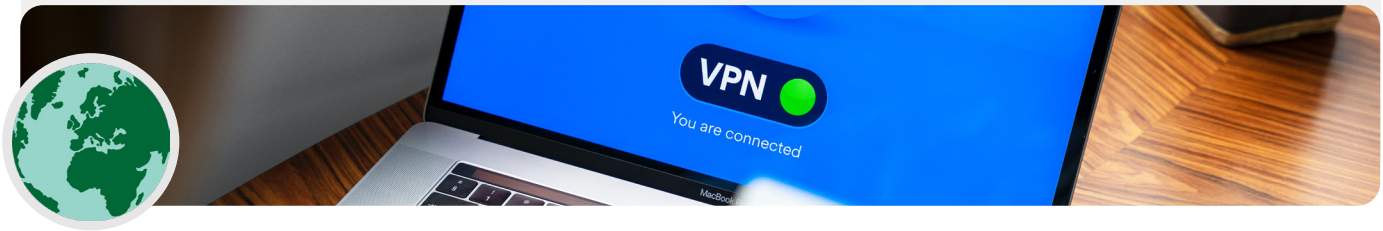
¿Por qué no debería utilizar una VPN gratuita? La respuesta corta es que la mayoría de las VPN gratuitas, incluidas las que vienen preinstaladas en algunos teléfonos inteligentes, vienen con una gran trampa. Al igual que todas las empresas y proveedores de servicios, las VPN tienen que sostenerse de 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 recogen, no pueden venderse ni entregarse a un gobierno extranjero 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.

Vale 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. Conviene ser escéptico con una VPN que ofrece un servicio en el que nadie quiere apostar su reputación, o que está a cargo de una empresa que nadie conoce.

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, además de garantizar la seguridad del tráfico de internet parlamentario, también necesita una solución para limitar en forma segura el acceso a sistemas y aplicaciones parlamentarios internos solo a quienes se encuentran en su red parlamentaria (incluso mientras trabajan en forma remota), es posible que desee implementar una VPN "comercial" o "corporativa". Existe una variedad de opciones en las que se utilizan diversas tecnologías que puede considerar, incluidas **AnyConnect** de Cisco, **Global Protect** de PaloAlto o **Access** de Cloudflare (técnicamente, un sistema de acceso Zero Trust, no una VPN), solo por nombrar algunas. De cualquier manera, dichos sistemas requieren personal de TI calificado para implementarlos y administrarlos con eficacia.

Si un sistema VPN "corporativo" avanzado está fuera del presupuesto o es innecesariamente complicado para su parlamento, también puede considerar usar opciones de VPN personal como **ProtonVPN** o **TunnelBear** (que también ofrece un plan de Teams para simplificar la administración de cuentas) para todos los miembros del parlamento y personal. Otra opción confiable es usar **Outline** de Jigsaw, en el que no hay una empresa que administre su cuenta, sino que usted tiene que configurar su propio servidor.

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

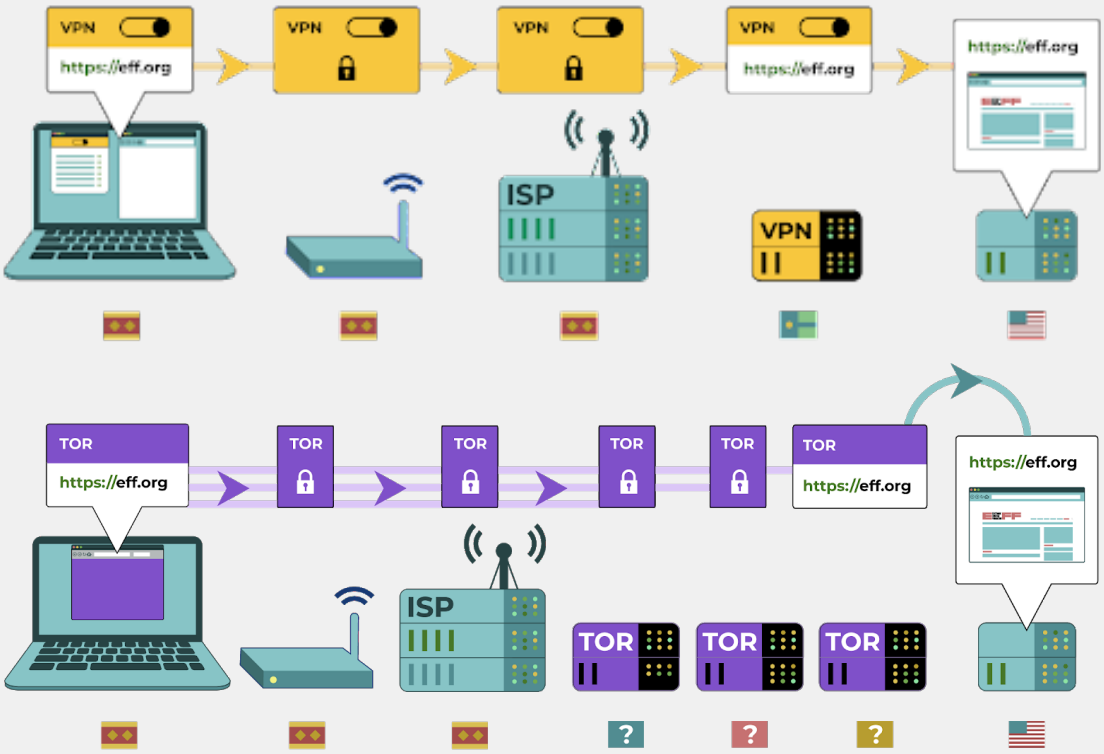
Además de las VPN, es posible que haya oído hablar de Tor como otra herramienta para utilizar internet de forma más segura. Es importante entender qué son ambos y por qué podría usar uno u otro.

Tor es un protocolo para transmitir datos en forma anónima por internet mediante el enrutamiento de mensajes o datos por 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. La diferencia fundamental es que 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 protege 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 su perfil de riesgo de manera considerable, porque Tor no es una herramienta muy común y por lo tanto sobresale para los adversarios que pueden estar monitoreando su tráfico de internet.

Por lo tanto, si bien es probable que haya muy pocos casos en los que sea necesario usar Tor dentro de un contexto parlamentario, si no puede permitirse una VPN confiable o encuentra que su parlamento opera en un entorno en que las VPN se bloquean en forma rutinaria, Tor puede ser una buena opción, si es legal, 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 podría atraer atención no deseada o, en el orden local, ir contra 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. Si eso es ilegal donde operan su parlamento o su personal o podría causar más atención o riesgo que solo navegar por la web con un HTTPS estándar y DNS cifrado, tal vez una VPN o en especial Tor (que se usa con mucha menos frecuencia y, por lo tanto, es una "bandera roja" más grande) no son la elección correcta.

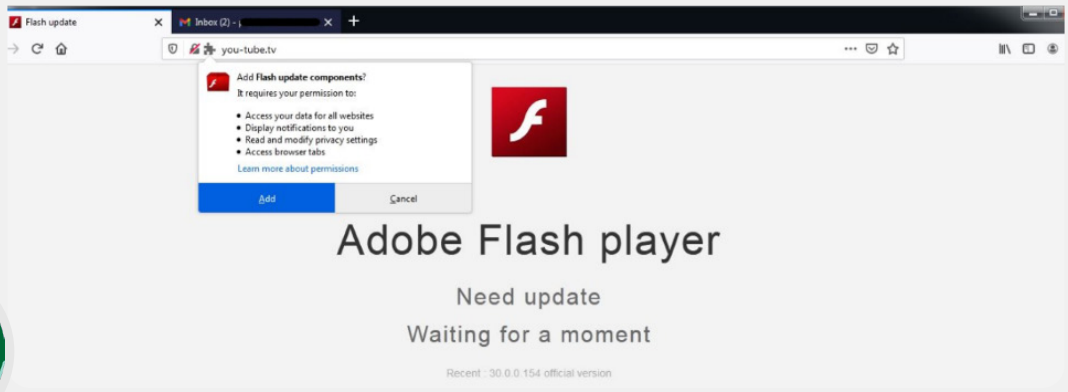
¿QUÉ NAVEGADOR DEBERÍAMOS UTILIZAR?

Utilice un navegador de confianza, como Chrome, Firefox, Brave, Safari, Edge o el navegador de 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 características de los navegadores, consulte este recurso de la Fundación para la Libertad de Prensa. 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 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

Estos ataques a extensiones o complementos del navegador pueden ser tan dañinos como el malware compartido directamente en descargas de phishing u otro software. Por ejemplo, un complemento malicioso diseñado con inteligencia titulado "componentes de actualización de Flash" se dirigió a organizaciones políticas tibetanas a principios de 2021. Se presentó a los usuarios que visitaron sitios web vinculados a correos electrónicos de phishing y, cuando se instalaba, permitía a los piratas informáticos robar correos electrónicos y datos de navegación.

Los complementos del navegador también pueden ser un vector para infectar recursos parlamentarios, como sitios web, que a su vez pueden propagar malware a una amplia gama de visitantes del sitio (incluido el público en general, el personal parlamentario y los propios miembros). Tomemos, por ejemplo, la explotación por parte de piratas informáticos del popular complemento del navegador Browsealoud (ahora conocido como ReachDeck), un programa que convierte el texto del sitio web en audio para usuarios con discapacidades visuales. En 2018, los piratas informáticos insertaron un código malicioso en el complemento del navegador, que se había utilizado en sitios web de varias entidades gubernamentales, incluido el parlamento del estado de Victoria en Australia. Con el complemento del navegador infectado instalado y configurado en forma incorrecta, se infectaron los dispositivos de los visitantes del sitio web con malware al visitar el sitio. En este caso, el malware se usó para aprovechar los dispositivos para extraer criptomonedas, pero los piratas informáticos también podrían usar esas tácticas para propagar malware con fines de robo de datos o espionaje.



Seguridad en las Redes Sociales

El personal parlamentario y los MP pueden revelar mucho, ya veces más de lo que pretenden, 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 los parlamentos, sino también, en algunos casos, para cuentas propias del personal y las de familiares y amigos.

Seguridad en Redes Sociales y Parlamentos

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 piratas informáticos se toman esos esfuerzos para sacarle unos pocos miles de dólares de un refugio de animales, puede imaginar el daño que adversarios sofisticados podrían infligir si obtuvieran acceso a las cuentas de su parlamento o se hicieran pasar en línea con éxito por un MP prominente o alguien del personal.

Además de piratear cuentas de redes sociales, los sitios web del parlamento también son blancos comunes dada su visibilidad pública y la importancia de su reputación. En un ejemplo de 2017, un grupo de piratas informáticos derribó el sitio web del parlamento de Austria: se suponía que estaban enojados por las relaciones amargas del país con Turquía en ese momento.

DESARROLLE UNA POLÍTICA PARLAMENTARIA DE REDES SOCIALES

Suponga que todo lo que publiquen en las redes sociales podría convertirse en conocimiento público, y elabore una política parlamentaria al respecto. Dada la naturaleza pública de la mayor parte del trabajo parlamentario, es probable que desee compartir la mayoría de las publicaciones y mensajes con el público, pero igual es esencial hacer y responder preguntas como: ¿Quién tiene acceso a sus cuentas de redes sociales? ¿Quién puede publicar y quién debe aprobar las publicaciones? ¿Qué ocurre con los comentarios y las respuestas? ¿Qué información debe/no debe compartirse en las redes sociales? Si publica fotos, datos de ubicación u otra información identificatoria sobre su personal, miembros o socios, ¿ha pedido su permiso y han considerado si hay riesgos posibles? Estas preguntas son importantes en especial si su parlamento se involucra públicamente con los ciudadanos en redes sociales o portales en línea similares para participación pública.
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"). Estas son algunas preguntas clave que debe hacerse mientras decide qué configuraciones de privacidad y seguridad tienen más sentido para las cuentas parlamentarias y personales:

- ¿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?
- ¿Las personas deberían poder usar su dirección de correo electrónico o su número de teléfono (personal o profesional) para buscarlo?
- ¿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. Por lo tanto, tenga cuidado al aceptar solicitudes de "amistad" y "seguimiento". Recuerde que las cuentas de redes sociales de su parlamento son tan seguras como las cuentas que están "vinculadas" a él. Es importante en especial recordar esto para Facebook, donde alguien con una cuenta personal vinculada puede manejar las páginas suyas.

ACOSO EN LÍNEA

Por desgracia, muchos parlamentos y grupos afiliados enfrentan un acoso significativo en línea, en especial en 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 lleve a la autocensura o a retirarse del discurso político o cívico. Como se identificó en el informe **Tweets that Chill** del equipo de Género, Mujeres y Democracia del NDI, cuando los ataques contra mujeres activas en política se canalizan en línea, el alcance expansivo de las redes sociales puede magnificar el efecto de acoso y abuso psicológico, y socavar la sensación de seguridad personal de las mujeres de maneras que no experimentan los hombres.

Mientras su parlamento desarrolla su política de redes sociales, es importante estar al tanto de esta dinámica. Incluya en su plan de seguridad un apoyo estructurado para el personal que enfrenta 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 parlamento que incluya una encuesta a su personal para entender cómo los afecta el acoso en línea y cree un equipo de respuesta rápida para ayudar al personal a hacer frente a situaciones desafiantes. 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 trate con personal que ha sido víctima de acoso en línea (y en el mundo físico también), es importante ser sensible. Como se indica en el programa de derechos de la mujer **Dominemos la tecnología** de la Asociación para el Progreso de las Comunicaciones, se debe entender que una sobreviviente 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 parlamento una lista de profesionales locales, organizaciones y agencias policiales 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 seguro a internet, también es importante hacer lo posible para asegurarse de que otros puedan acceder a los sitios o propiedades web de su parlamento.

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. Algunas opciones para la protección DDoS, que hace mucho más difícil para un adversario derribar su sitio web, son Cloudflare, AWS Shield de Amazon o el servicio Deflect de eQualitie.

Alojar el Sitio Web de su Parlamento en Forma Segura

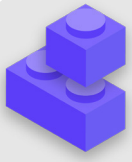
Los sitios web se alojan en computadoras, y éstas son vulnerables a la piratería informática, al igual que sus dispositivos. Si es posible, su parlamento debería aprovechar los servicios de alojamiento existentes como WordPress, Wix u otros que administran toda la seguridad del sitio por usted. Si las necesidades de su sitio web son más complejas o necesita alojar su sitio web usted mismo, entonces asegúrese de concentrarse en mantener actualizado su sistema operativo y el software de alojamiento web, tal como 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 sin importar las herramientas que utilice para alojar su sitio web, asegúrese de que todas las cuentas utilizadas para acceder a la edición de contenidos y ajustes de configuración tengan la protección de contraseñas seguras y una autenticación de dos factores.

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

Proteja su Red Wifi

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

No olvide lo básico, como utilizar una contraseña fuerte (no la predeterminada) en su enrutador wifi, asegurarse de que solo usuarios autorizados tengan acceso a su red mediante el cambio frecuente de la contraseña, y activar el cortafuegos integrado de sus enrutadores inalámbricos. Considere la posibilidad de crear una red de invitados en las instalaciones parlamentarias también si tiene visitantes que entran y salen del edificio que usan internet.



Mantenerse seguro en internet

- **Brinde capacitaciones periódicas a los miembros y 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.**
- **Exíjales reiniciar sus navegadores en forma periódica para instalar actualizaciones.**
- **Fomente el uso de navegadores y extensiones que protejan la privacidad.**
- **Si una VPN es apropiada, elija una de buena reputación, capacite al personal en su uso y asegúrese de que se emplee de manera sistemática.**
- **Desarrolle y distribuya una política parlamentaria clara sobre el uso de redes sociales.**
- **Habilite la configuración de privacidad y seguridad en todas las cuentas de redes sociales.**
- **Entienda los impactos del acoso en línea y esté preparado para apoyar a los miembros y al personal que resulten afectados.**
- **Elabore una lista de profesionales, organizaciones y cuerpos de seguridad locales con los que pueda poner en contacto al personal para obtener asistencia legal, 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.**
- **Use una contraseña segura y una red de invitados para su Wi-Fi local.**

Proteger la seguridad física

Es esencial conservar la seguridad física de sus dispositivos. Tenga en cuenta que eso va más allá de los meros aparatos y debe incluir estrategias para proteger todo lo demás en su mundo. Eso incluye documentos impresos, oficinas del parlamento, cámaras o espacios de trabajo y por supuesto usted, su personal y los miembros.

Seguridad Física y Parlamento

Por desgracia, los ataques físicos a los parlamentos y otros órganos legislativos no son infrecuentes, y muchas veces tienen implicaciones significativas tanto para la seguridad física como para la de la información. El 6 de enero de 2021, un grupo de insurrectos atacaron el edificio del Capitolio de Estados Unidos, sede de ambas cámaras de la legislatura nacional, en un esfuerzo por detener la certificación de los resultados de la elección presidencial. El ataque físico provocó cinco trágicas muertes y causó una gran angustia psicológica a los miembros y al personal del Congreso. Sin embargo, no fue el único impacto negativo. Los atacantes también destruyeron equipos de TI, obtuvieron acceso a materiales confidenciales en las oficinas de los miembros y, quizás lo más dañino, robaron computadoras y otros dispositivos con información potencialmente confidencial del Capitolio estadounidense.

Instalaciones de Información Compartimentada Confidencial (SC

Para mantener conversaciones altamente confidenciales, algunos parlamentos han instalado salas físicas protegidas llamadas SCIF. Estos espacios se establecen de manera que los MP y su personal puedan ver y comentar cuestiones de información confidencial tales como las relacionadas con seguridad nacional o inteligencia, sin preocuparse por vigilancia o espionaje externos. Además de la construcción física correcta, un SCIF adecuado requiere que las personas dejen los dispositivos (como sus teléfonos celulares) fuera de la sala antes de ingresar para el debate.

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 funciones de borrado remoto, también debería considerar cómo evitar que roben esos dispositivos en primer lugar. Para dificultar el robo, asegúrese de instalar cerraduras fuertes (y cambiarlas cada vez que cambie el personal) en las instalaciones parlamentarias y en el hogar. Además, considere comprar una caja de seguridad para la computadora portátil o un gabinete con cerradura para mantener los dispositivos protegidos durante la noche. Los sistemas de cámaras o sensores de movimiento por todas las instalaciones pueden detectar y, con suerte, disuadir robos físicos y entradas forzadas. Busque una opción **que respete la privacidad** disponible en su país, y asegúrese de seleccionar cámaras y sistemas de seguridad proporcionados por empresas de confianza que no tengan un incentivo para entregar datos e información a un adversario potencial.

Si hay dispositivos antiguos que aún tienen información almacenada pero ya no se utilizan, considere borrar su contenido: **esta guía** de WireCutter es un buen recurso para saber cómo hacerlo en 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 todo el equipamiento en el parlamento en su totalidad. Si no tiene una lista de todos sus dispositivos, es más difícil hacer un seguimiento de lo que puede faltar si le roban uno.

¿QUÉ HACEMOS CON TODO ESTE PAPEL?

Es probable que su parlamento tenga mucha información impresa en papel, escrita en cuadernos o garabateada en notas adhesivas. Algo de esto puede ser muy sensible, como notas de testimonios confidenciales o reuniones privadas, por ejemplo. 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) sobre un escritorio ni anotada en una pizarra. Mantenga la información altamente confidencial en una ubicación que sea menos un blanco de ataques y esté bien protegida.

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 parlamentaria con respecto a la propiedad de notas impresas y asegúrese de recoger notas en papel del personal si deciden irse o se los despide de la organización, tal como retiraría una computadora o un teléfono expedidos por el parlamento. 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 sus equipos para triturar los restos de impresiones o notas con información sensible de la semana anterior.

LA POLÍTICA PARLAMENTARIA

Aunque para muchos las realidades de "la oficina" han cambiado de manera significativa desde el comienzo de la pandemia de COVID-19, sigue siendo importante que su parlamento establezca una política clara con respecto al acceso a las instalaciones. Esa política debería abordar cuestiones clave, como quién tiene permiso para 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 simple pero importante que hay que responder es quién obtiene una llave de la oficina o una credencial de acceso. Solo personal de confianza debería tener llaves o credenciales, y las cerraduras deberían cambiarse cuando el personal se vaya o en forma semiperiódica. Durante el día, cualquier puerta que se deje sin llave debería estar a la vista constante de alguien de confianza o un guardia de seguridad. Además, asegúrese de que su parlamento tenga una relación de confianza con los proveedores de servicios, como personal de limpieza y técnicos externos que tienen acceso a las instalaciones. Piense en la información o los dispositivos a los que estas personas podrían tener acceso y asegúrese de que estén protegidos, en particular si no tiene esa relación de confianza. Quienquiera que tenga el acceso, siempre debería designarse a alguien de confianza para que cierre con llave las oficinas y los edificios y se asegure de que los dispositivos tengan la protección apropiada antes de salir al final del día.

¿Se permite a los electores ingresar a su parlamento? ¿Quizás el público tiene derecho a acceder a partes de las instalaciones parlamentarias? 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 el público visitante o los invitados tengan acceso a internet cuando hacen una visita, debería configurarse una red de "invitados" para que no tengan la capacidad de monitorear su tráfico habitual. 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 VOLUNTARIOS

Las amenazas a la seguridad física de su parlamento 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, maltrato doméstico y temor a los ataques pueden tener un grave impacto negativo en la vida de los miembros y el personal. La herramienta de planificación de seguridad **#Think10** del NDI es un recurso útil para mujeres activas en política que podrían estar en mayor riesgo personal como resultado de su participación en el parlamento y en la política en general.

Es obvio que el bienestar del personal es un activo importante para ellos como individuos, pero también es un elemento vital para un parlamento 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. Como ya se mencionó, el **Manual de campo contra el acoso en línea**, de PEN America, incluye ideas sobre cómo las organizaciones pueden apoyar al personal durante y después de las crisis.

SEGURIDAD EN VIAJES

Viajar, ya sea a otro país o a una ciudad vecina, 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 eso es una buena idea incluir una política parlamentaria de viajes dentro de su plan de seguridad que incluya recordatorios sobre las mejores prácticas de seguridad clave. La política de viajes de su parlamento debería incluir mucha de la información que se trata en otras secciones del Manual, como el uso seguro de internet y el mantenimiento de la seguridad física de los dispositivos y otras fuentes de información, que deberían estar 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.

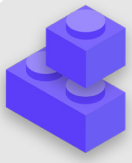
Además de prepararse para viajar y minimizar los datos compartidos cuando viaja, hay algunos consejos operativos esenciales que debería analizar e incluir en la política de viajes.

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 de relativo bajo costo 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. 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 necesitaran 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. No confíe en 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 Viajes para su Parlamento

Cuando elabore una política de viajes, también tenga en cuenta la información que podría quedar expuesta cuando organice o reserve un viaje. Esto puede ser importante en particular si se organizan grandes eventos o conferencias en las que se maneja información sensible de una variedad de integrantes del personal, miembros 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.



Proteger la seguridad física

- **Recuerde a los miembros y al personal que mantengan los dispositivos físicamente protegidos en todo momento.**
- **Revise y proteja todas las formas en que las personas pueden ingresar a sus instalaciones.**
- **Desarrolle una política de acceso e invitados.**
- **Use cerraduras fuertes, sistemas de identificación y credenciales, y cámbielos cuando sea necesario.**
- **Considere instalar cámaras u otros sistemas de seguridad en las instalaciones**
- **Tenga y use trituradoras 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 agencias policiales locales con los que pueda poner en contacto a los miembros y al personal para obtener asistencia legal, médica y de salud mental en respuesta a ataques físicos o amenazas.**
- **Desarrolle una política parlamentaria de viajes.**
- **Asegúrese de que el personal sepa qué hacer en caso de emergencia durante el viaje.**
- **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 implementado las políticas y capacitado a todos en el parlamento sobre 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 incidentes es una parte crucial, y muchas veces subestimada, del plan de seguridad de su parlamento porque puede ser la diferencia entre un ataque que destruya su reputación o una desagradable protuberancia en el camino. Recuerde que solo puede responder a un incidente si sabe cómo hacerlo. Es muy importante tener una sólida cultura de seguridad y alentar a los miembros y 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 todo el parlamento.

Entonces, ¿para qué debería prepararse? En resumen, cualquier cosa que tenga cierta probabilidad de ocurrir. Esto será diferente para cada parlamento, 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 se encuentra en peligro físico? ¿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 se pierde o roban la computadora o el teléfono de un miembro?

Las respuestas a estas y otras preguntas diferirán según el parlamento, pero es importante pensar en ellas juntos y articular con claridad un plan y compartirlo para que todos estén preparados para actuar de inmediato y limitar el daño.

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 emergencia** en el contexto de su parlamento. Decidan qué es una "emergencia": es decir, el momento en que debemos empezar a implementar las acciones y medidas de contingencia planeadas. 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 emergencias está la activación de una red de apoyo: una amplia red de aliados, que puede incluir diferentes ramas de su propio Gobierno, otros gobiernos amigos, empresas de tecnología, proveedores de seguridad e instituciones multilaterales, por nombrar solo algunos ejemplos. ¿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 se vuelven 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 para hacer copias de respaldo. 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. Además, considere el impacto de un incidente en la reputación de su parlamento y esté preparado para responder en consecuencia. Asegúrese de que el líder de comunicaciones del parlamento esté al tanto del incidente y pueda observar las redes sociales u otros medios para detectar un impacto potencial. 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.

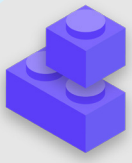
Creación de un Sistema de Alertas Tempranas y Respuestas

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 a incidentes, su parlamento también debería 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, para algunos incidentes técnicos podría requerirse pericia que no tiene dentro de su parlamento. 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 por anticipado las condiciones con los proveedores de servicios (como el alojamiento de su sitio web o una empresa de seguridad informática) 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 medidas **legales**. Es importante entender las protecciones legales que podría tener, así como las obligaciones legales o las consecuencias que su parlamento podría enfrentar como resultado de una filtración de datos u otro incidente de seguridad. Como parlamento, se encuentra en una posición de especial poder y prominencia cuando se trata de entender y respetar las normas locales de seguridad de datos y privacidad. Tómese el tiempo para revisar posibles incidentes con el asesor legal pertinente si es necesario y haga un plan para 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 frente a las repercusiones 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. Mientras elabora su plan de respuesta a incidentes, recomendamos con énfasis que haga uso de algunos excelentes recursos existentes, diseñados para ayudar a las organizaciones a hacerse camino en esta cuestión. Aunque no todos estos recursos están diseñados en forma específica para parlamentos, su contenido es igual muy pertinente. Estos recursos son: 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 y la Plantilla del Plan de Comunicaciones de Incidentes Cibernéticos del Centro Belfer, y la Línea de Ayuda de Seguridad Digital de Access Now.



Respuesta a Incidentes

- **Desarrolle un plan parlamentario de respuesta a incidentes y póngalo en práctica.**
  - Haga una lluvia de ideas sobre posibles incidentes y prepare su respuesta antes de que ocurran.
- **Asegúrese de que todos en el parlamento sepan cómo se comunicará y qué medidas técnicas se tomarán en caso de un incidente.**
- **Tómese el tiempo necesario para entender sus protecciones y obligaciones legales.**
- **Deberá estar preparado para brindar a los miembros y al personal el apoyo emocional y social que necesitan con las repercusiones de un incidente.**

Apéndice A: Recursos Recomendados

- Holistic Security Manual (Manual de Seguridad Holística), de Tactical Tech; Creative Commons Attribution-ShareAlike 4.0 International License
  - Chapter 2.4. Understanding and Cataloguing Our Information (Entender y catalogar nuestra información)
  - Chapter 1.5. Communicating About Threats in Teams and Organizations (Comunicación sobre amenazas en equipos y organizaciones)
  - Chapter 3.4. Security in Groups and Organizations (Seguridad en grupos y organizaciones)
- Security Education Companion (El acompañante de educación en seguridad) de la Electronic Frontier Foundation; Creative Commons Attribution 3.0 US License
  - Threat Modeling Activity Handout (Folleto sobre actividad de modelado de amenazas)
- Phishing Prevention and Email Hygiene Guide (Guía sobre prevención de phishing e higiene en el correo electrónico) de Freedom of the Press Foundation; Creative Commons Attribution 4.0 International License
- Locking Down Signal Guide (Guía de bloqueo de Signal) de Freedom of the Press Foundation; Creative Commons Attribution 4.0 International License
- Surveillance Self-Defense (SSD) Guide (Guía de autodefensa de vigilancia) de Electronic Frontier Foundation; Creative Commons Attribution 3.0 US License
  - What Should I Know About Encryption (Qué debería saber sobre cifrado)
  - Communicating with Others (Comunicarse con los demás)
  - Choosing the VPN That's Right for You (Elegir la VPN adecuada para usted)
- Guide to Secure Group Chat and Conferencing Tools (Guía para chat grupal seguro y herramientas de conferencias) de Front Line Defenders
- Data Detox Kit (Kit de desintoxicación de datos) de Tactical Tech
  - Let the Right One In: Make Your Passwords Stronger (Que ingrese el correcto: Haga más fuertes sus contraseñas)
  - Strengthen Your Screen Locks (Fortalezca sus bloqueos de pantalla)
- Elections Security Guide on Passwords (Guía de contraseñas para seguridad en las elecciones) de Center for Democracy & Technology; Creative Commons Attribution 4.0 International License
- Elections Security Guide on Two Factor Authentication (Guía de autenticación de dos factores para seguridad en las elecciones) de Center for Democracy and Technology; Creative Commons Attribution 4.0 International License
- Two Factor Authentication for Beginners (Autenticación de dos factores para principiantes) de Martin Shelton; Creative Commons Attribution 4.0 International License
- Security in a Box (Seguridad en una caja) de Tactical Tech y Frontline Defender; Creative Commons Attribution-ShareAlike 3.0 Unported License
  - Protect your device from malware and phishing attacks (Proteja su dispositivo contra el malware y los ataques de phishing)
  - Protect against physical threats (Protéjase contra amenazas físicas)
- Boletín de SANS' OUCH!: Stop That Malware (Detenga el malware)
- Apple's Device and Data Access When Personal Safety is at Risk (Dispositivo de Apple y acceso a los datos: Cuando la seguridad personal está en riesgo)
- Cybersecurity Toolkit for Mission-Based Organizations (Kit de herramientas de ciberseguridad para organizaciones basadas en misiones) de Global Cyber Alliance
- Cybersecurity Assessment Tool (Herramienta de evaluación de ciberseguridad) de Ford Foundation

Apéndice B:
Kit de Inicio del Plan de Seguridad

Utilice el siguiente kit de inicio para tomar notas mientras usted y su parlamento revisan el Manual y asimilan el material, y considere las preguntas que lo acompañan 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 cubre los temas importantes mientras elabora su plan de seguridad. Al llegar 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

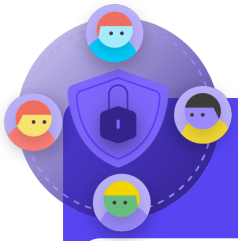
Cimientos Sólidos: Protección de Cuentas y Dispositivos

Comunicar Datos en Forma 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 todo el parlamento?
- ¿Qué días u horarios funcionan bien para que el parlamento programe conversaciones habituales y capacitación sobre seguridad?
- ¿Qué medidas puede tomar la dirección para mostrar un buen comportamiento de seguridad y compromiso con un plan de seguridad? ¿Cómo pueden otras personas del parlamento desempeñar una función en seguridad?

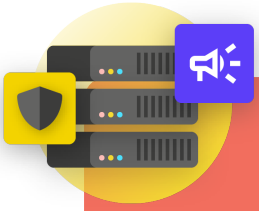
SUS NOTAS E IDEAS:

Cimientos Sólidos: Protección de Cuentas y Dispositivos

PREGUNTAS A TENER EN CUENTA:

- ¿Cómo implementará en todo el parlamento medidas de seguridad de cuenta, como un administrador de contraseñas y 2FA? ¿Qué obstáculos podría encontrar durante la implementación?
- ¿Cómo garantizará su parlamento que los dispositivos se mantengan seguros y actualizados? Como parte de esto, ¿el parlamento necesitará un plan para encargarse de software o 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:

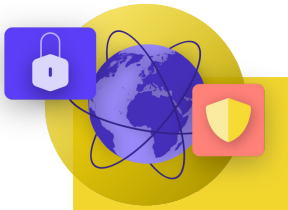


Comunicar y almacenar los datos de manera segura

PREGUNTAS A TENER EN CUENTA:

- ¿Cómo implementará su parlamento la mensajería cifrada de extremo a extremo para una comunicación segura? ¿Qué obstáculos podría encontrar durante la implementación?
- ¿Cómo implementará su parlamento una solución segura para compartir archivos en el ámbito tanto interno como externo? ¿Qué obstáculos podría encontrar durante la implementación?
- ¿Cómo implementará su parlamento una solución segura de almacenamiento de datos y copia de respaldo? ¿Qué obstáculos podría encontrar durante la implementación?

SUS NOTAS E IDEAS:



Mantenerse seguro en internet

PREGUNTAS A TENER EN CUENTA:

- ¿Cómo implementará su parlamento 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 parlamento? ¿Cómo se aplicará?
- ¿Cómo protegerá su parlamento sus sitios web y propiedades web?

SUS NOTAS E IDEAS:

Proteger la seguridad física

PREGUNTAS A TENER EN CUENTA:

- ¿Cómo distribuirá y hará cumplir el parlamento su política de invitados 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 el parlamento su política de respuesta a incidentes?
- ¿Hay recursos disponibles para el personal que pudiera necesitar apoyo emocional y social tras un incidente? De no ser así, ¿cómo podría el parlamento proporcionar esos recursos en caso de un incidente?

SUS NOTAS E IDEAS:

Apéndice C: Citas de imágenes

Página 14: New York Times, "Australian Parliament Reports Cyberattack on Its Computer Network", 2019, imagen digital, Getty Images, https://www.nytimes.com/2019/02/07/world/australia/cyberattack-parliament-hack.html.
Página 18: CNP Collection, "Security Protection Anti-Virus Software cms", 2014, imagen digital, 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: Bleeping Computers, "Norway parliament data stolen in Microsoft Exchange attack", 2021, imagen digital, https://www.bleepstatic.com/content/hl-images/2021/03/10/storting.jpg.
Página 25: Cottonbro, "Person Holding Black and Silver Key", 2020, imagen digital, Pexels, https://www.pexels.com/photo/person-holding-black-and-silver-key-5474292/?utm_content=attributionCopyText&utm_medium=referral&utm_source=pexels.
Página 27: Blogtrepreneur, "Malware Infection", 2016, imagen digital, Flickr, https://www.flickr.com/photos/143601516@N03/.
Página 30: "Microsoft Loading Screen", imagen digital, Kompass, 23 de septiembre de 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, imagen digital, Pexels, https://www.pexels.com/photo/turned-on-iphone-and-displaying-icons-365194/.
Página 33: ZDNet, "Chinese hacking group impersonates Afghan president to infiltrate government agencies", 2021, imagen digital, https://www.zdnet.com/article/chinese-hacking-group-impersonates-afghan-president-to-infiltrate-government-agencies/
Página 38: Andrew Keymaster, "People Gathering on Street During Daytime Photo", 2020, imagen digital, Unsplash, https://unsplash.com/photos/JXQ2bizu7kc.
Página 39: Surveillance Self-Defense, "No Encryption in Transit", imagen digital, Electronic Frontier Foundation, 17 de enero de 2019. https://ssd.eff.org/en/module/what-should-i-know-about-encryption.
Página 40: Surveillance Self-Defense, "4.Transport-layer-alternate", imagen digital, Electronic Frontier Foundation, 17 de enero de 2019, https://ssd.Surveillance Self-Defense.org/files/2018/11/26/4.transport-layer-alternate.png.;Surveillance Self-Defense, "6. End-to-end Alternate", imagen digital, Electronic Frontier Foundation, 17 de enero de 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, imagen digital, Electronic Frontier Foundation, https://ssd.eff.org/en/module/what-should-i-know-about-encryption.
Página 49: African News Agency, "Parliament meeting falls victim to hacking as MPs greeted by pornographic images", 2020, imagen digital, Reuters, https://www.iol.co.za/news/politics/parliament-meeting-falls-victim-to-hacking-as-mps-greeted-by-pornographic-images-47657120
Página 51: UK Parliament, imagen digital, Jessica Taylor, https://e3.365dm.com/20/04/768x432/skynews-parliament-house-of-commons_4974709.jpg?20200422191547
Página 52: Brett Sayles, "Server Racks on Data Center", 2020, imagen digital, Pexels, https://www.pexels.com/photo/server-racks-on-data-center-4508751/.
Página 58: PhotoMIX Company, 2016, "White 2 Cctv Cameras Mounted on Black Post Under Clear Blue Sky", imagen digital, Pexels, https://www.pexels.com/photo/white-2-cctv-camera-mounted-on-black-post-under-clear-blue-sky-96612/.
Página 63: Stefan Coders, "laptop-screen-vpn-cyber-security", 2020, imagen digital, Unsplash, https://pixabay.com/photos/laptop-screen-vpn-cyber-security-5534556/.
Página 65: Surveillance Self-Defense, "Using the Tor Browser", imagen digital, Electronic Frontier Foundation, 25 de abril de 2020. https://ssd.eff.org/files/2020/04/25/circumvention-tor_0.png
Página 67: Nathan Dumlao, "White Samsung Android Smartphone on Brown Wooden Table", 2020, imagen digital, Unsplash, https://unsplash.com/photos/kLmt1mpGJVg.
Página 72: Matt Artz, "Two Broken 6-Pane On White Painted Wall Photo", imagen digital, Unsplash, 1 de octubre de 2017, https://unsplash.com/photos/vT684iB7Ejg.


NDI
NATIONAL
DEMOCRATIC
INSTITUTE


HOUSE
DEMOCRACY
PARTNERSHIP


IRI
INTERNATIONAL
REPUBLICAN
INSTITUTE
Advancing Democracy Worldwide


USAID
FROM THE AMERICAN PEOPLE