

**COMIENZE
CON**

SEGURIDAD

UNA GUÍA PARA NEGOCIOS

LECCIONES APRENDIDAS DE LOS CASOS DE LA FTC.

LA COMISIÓN FEDERAL DE COMERCIO

COMIENZE CON **SEGURIDAD**

-
1. **Comience con seguridad.**

 2. **Controle prudentemente el acceso a los datos.**

 3. **Exija el uso de contraseñas seguras y un sistema de autenticación.**

 4. **Almacene la información personal delicada de manera segura y protéjala durante la transmisión.**

 5. **Segmente su red y haga un monitoreo para controlar quién está tratando de entrar y salir.**

 6. **Proteja el acceso remoto a su red.**

 7. **Aplique prácticas de seguridad sólidas cuando desarrolle nuevos productos.**

 8. **Asegúrese de que sus proveedores de servicio implementen medidas de seguridad razonables.**

 9. **Implemente procedimientos para mantener actualizada la seguridad y ocúpese de las vulnerabilidades que pudieran surgir.**

 10. **Proteja los archivos impresos en papel, los soportes físicos y los dispositivos.**

Cuando usted maneja su red informática, desarrolla una aplicación o incluso cuando organiza sus archivos impresos en papel, la implementación de una seguridad sólida en su negocio no es algo fortuito. Las compañías que consideran la seguridad desde el comienzo pueden evaluar sus opciones y tomar decisiones basadas en la naturaleza de su negocio y en el nivel de vulnerabilidad de la información que manejan. Las amenazas contra los datos pueden transformarse con el transcurso del tiempo, pero los fundamentos de una seguridad sólida permanecen constantes. Tal como lo señaló la FTC en su publicación ***Cómo proteger la información personal: una guía para negocios***, es crucial que usted sepa cuál es la información que almacena física y electrónicamente, y que conserve únicamente aquella información que sea esencial para su negocio. Proteja la información que mantiene en archivo y elimine correctamente los datos que no necesite. Y por supuesto, debe crear un plan para responder a los incidentes de seguridad.

La FTC también tiene ***recursos sobre ciberseguridad*** especialmente destinados a los pequeños negocios, entre los que se incluyen publicaciones que abordan los desafíos particulares de la seguridad de datos, alertas para negocios y orientación para ayudarlo a identificar, y posiblemente prevenir, inconvenientes.

Además, hay otra fuente de información sobre la protección de los datos delicados: las lecciones aprendidas a partir de las más de 80 acciones de cumplimiento de la ley anunciadas por la FTC hasta la fecha. Por supuesto que se trata de acuerdos resolutorios, la corte no se ha expedido sobre esos casos, y los detalles específicos de las órdenes se aplican únicamente a esas compañías. Pero aprender de los errores alegados que originaron las acciones de cumplimiento de la ley pueden ayudarlo a mejorar las prácticas de su compañía. Y la mayoría de las prácticas alegadas en esos casos involucra errores de seguridad básicos y fundamentales. Mediante un exhaustivo análisis de los hechos de esos casos, le ofrecemos diez lecciones para aprender en detalle cuáles son las vulnerabilidades que podrían afectar a su compañía, junto con orientación práctica sobre cómo reducir los riesgos que plantean.

1

Comience con seguridad.

Los ejecutivos de los negocios suelen preguntar cómo se debe manejar la información confidencial, lo cual incluye desde los datos personales de las solicitudes de empleo hasta los archivos de las redes informáticas que contienen los números de tarjeta de crédito de los clientes. Los expertos concuerdan en el primer paso clave: comenzar con seguridad. Incluya el factor seguridad en la toma de decisiones de cada departamento de su negocio: personal, ventas, contabilidad, tecnología de la información, etc. Recolectar información y guardarla “solo porque sí” ya no es una estrategia comercial sólida. En lugar de eso, piense deliberadamente en las implicancias de sus decisiones sobre los datos. Usted puede reducir el riesgo de que surjan incidentes de seguridad de datos en el futuro tomando decisiones meditadas acerca del tipo de información que recolecta su negocio, cuánto tiempo la conserva y quiénes pueden acceder a ella. Por supuesto que todas esas decisiones dependerán de la naturaleza de su negocio. Las lecciones que surgen de los casos de la FTC ilustran los beneficios de construir la seguridad desde el comienzo preparando y perfeccionando sus políticas de recolección, retención y uso de datos.

No recolecte información personal que no necesite.

Este es un principio fundacional que debe considerar en sus decisiones iniciales: nadie puede robarle lo que no tiene. ¿Cuándo le solicita información delicada a la gente? Quizás cuando se registran en internet o establecen una cuenta nueva con su compañía. ¿Cuándo fue la última vez que revisó ese proceso para asegurarse de que realmente necesita todos los datos que está solicitando su negocio?

Esa es una de las lecciones que se puede aprender a partir de una cantidad de casos de la FTC. Por ejemplo, en la demanda de la FTC contra [RockYou](#), se acusó a la compañía de haber recolectado mucha información durante el proceso de inscripción en el sitio que incluía el domicilio de email de los usuarios y sus contraseñas. La FTC dijo que, al recolectar las contraseñas de email, que no era un dato que el negocio necesitara, y al almacenarlas en un formato de texto sin codificación, la compañía generó un riesgo innecesario para las cuentas de email de la gente. El negocio podría haber evitado ese riesgo si en primer lugar no hubiera recolectado esa información delicada. Incluso

cuando se deba recopilar y almacenar información, considere si se puede almacenar exclusivamente en el dispositivo del usuario.

Retenga la información solo durante el tiempo que la necesite para un fin comercial legítimo.

A veces es necesario recolectar datos personales como parte de una transacción. Pero puede ser imprudente conservar esos datos después de cerrada la transacción. En el caso de la FTC contra **BJ's Wholesale Club**, la compañía recolectó los datos de las tarjetas de crédito y débito de los clientes para procesar las transacciones en sus tiendas minoristas. Pero de acuerdo a los términos de la demanda, la compañía continuó almacenando esos datos durante 30 días, bastante tiempo después de la fecha de venta. La FTC dijo que lo que hizo BJ's Wholesale Club no solo infringió las regulaciones bancarias, sino que la retención de la información sin una necesidad comercial legítima también generó un riesgo injustificado. Aprovechándose de las debilidades de las prácticas de seguridad de la compañía, unos piratas informáticos robaron los datos de las cuentas y los usaron para falsificar tarjetas de crédito y débito. El negocio podría haber limitado su riesgo eliminando la información financiera de manera segura cuando ya no tenía una necesidad legítima de conservarla.

No use información personal cuando no sea necesario.

Usted no haría malabares con un jarrón de la Dinastía Ming. Su negocio tampoco debería usar información personal en contextos donde se puedan generar riesgos innecesarios. En el caso **Accretive**, la FTC alegó que la compañía usó información personal verídica en sus sesiones de capacitación de empleados, y que omitió eliminar esa información de las computadoras de los empleados después de finalizadas las sesiones. De manera similar, en el caso **foru International**, la FTC acusó a la compañía de facilitar el acceso a datos delicados de consumidores a unos proveedores de servicio que estaban desarrollando aplicaciones para la compañía. En ambos casos, se podría haber evitado ese riesgo usando información ficticia tanto para propósitos de capacitación de empleados como para el desarrollo de las aplicaciones.

Controle prudentemente el acceso a los datos.

Una vez que haya decidido que tiene una necesidad comercial legítima que justifica la retención de datos delicados, tome las medidas razonables para protegerlos. Por supuesto que deberá mantener la información a salvo de la mirada indiscreta de los extraños, pero ¿qué sucede con sus propios empleados? No todos los miembros de su personal necesitan acceder de manera irrestricta a su red y a la información que ahí se almacena. Implemente controles para asegurarse de que sus empleados puedan acceder a la red únicamente sobre un criterio de una “necesidad de conocer los datos”. Para proteger su red informática, considere adoptar medidas tales como establecer cuentas de usuario separadas para limitar el acceso a los archivos donde se almacenan los datos personales o para controlar quiénes pueden usar bases de datos en particular. Para proteger los archivos impresos en papel, discos externos, otros dispositivos de almacenamiento de archivos, etc., el control del acceso podría ser algo tan simple como instalar un archivero con llave. Al momento de pensar en cómo controlar el acceso a la información delicada que tiene en su poder, considere estas lecciones que surgen de los casos de la FTC.

Restrinja el acceso a los datos delicados.

Si los proveedores y contratistas no tienen que usar información personal delicada de los clientes como parte de su trabajo, entonces no hay motivo para que tengan acceso a esos datos. Por ejemplo, en el caso **BLU**, la FTC alegó que la compañía no le impuso límites a uno de sus contratistas con respecto a la información de consumidores a la que podía acceder. El contratista recolectó y transfirió a sus servidores mucha más información de la que necesitaba para hacer su trabajo y esa información incluía el contenido completo de los mensajes de texto de los consumidores, los datos de localización en tiempo real, registros de llamadas y mensajes de texto con números de teléfono completos y listas de contactos. La compañía podría haber protegido estos datos delicados de los consumidores implementando procedimientos de seguridad adecuados para supervisar las prácticas de seguridad de sus proveedores de servicio, así como tomando las medidas necesarias para garantizar que solo los empleados o contratistas autorizados con una necesidad comercial legítima tuvieran acceso a la información personal de los usuarios.

En su demanda contra **MoviePass**, la FTC alegó que la compañía no protegió la información personal y financiera de sus usuarios, entre otras cosas, por almacenar esta información en texto sin codificar y no imponer restricciones acerca de quiénes podían acceder a esos datos. MoviePass almacenó información de consumidores que incluía nombres, domicilios de email, fechas de nacimiento, números de tarjeta de crédito y datos de geolocalización. Luego, la compañía cargó la información a un servidor en el cual había desactivado el firewall, y, por lo tanto, los datos quedaron accesibles a cualquier persona con una conexión a internet. El incidente de seguridad de datos resultante podría haberse evitado codificando los datos de los consumidores y manteniendo y gestionando controles de seguridad para proteger y restringir el acceso a esos datos.

Limite el acceso a los controles administrativos del sistema.

El acceso a los controles administrativos, que es lo que permite que un usuario efectúe cambios en todo su sistema, debería estar limitado al empleado a cargo de esa tarea. Por ejemplo, en su acción contra **Uber**, la FTC alegó que la compañía no restringió el acceso a los sistemas en base a las funciones laborales de los empleados, y permitió que todos los programas e ingenieros utilizaran una única clave de acceso a Amazon Web Services (AWS) que otorgaba plenos privilegios administrativos sobre todos los datos que la compañía tenía en el servicio de almacenamiento en la nube. Como resultado de esta práctica, cuando un ingeniero publicó la clave en un sitio de desarrollo de software, un sujeto malintencionado pudo utilizarla para acceder a la información personal delicada de miles de conductores de Uber que incluía nombres y números de licencias de conducir, cuentas bancarias y de Seguro Social.

3

Exija el uso de contraseñas seguras y un sistema de autenticación.

Si usted almacena información personal en su red informática, la implementación de sólidos procedimientos de autenticación, incluida una regla clara y firme para el establecimiento de contraseñas, puede ayudarlo a garantizar que solo aquellos individuos autorizados puedan acceder a los datos. Cuando desarrolle las políticas de su

compañía, puede considerar algunas de las recomendaciones que surgen de los casos de la FTC.

Insista en la creación de contraseñas únicas y complejas.

Establecer contraseñas como 121212 o qwerty no ofrece mucha más protección que ninguna contraseña en absoluto. Analice los estándares a implementar para la creación de las contraseñas. Por ejemplo, en el caso contra *Twitter* de 2011, la FTC alegó que la compañía permitió que sus empleados crearan contraseñas de control administrativo con palabras que comúnmente figuran en los diccionarios, y también les permitió usar las mismas contraseñas que estaban usando en otras cuentas. Según la FTC, esas prácticas laxas generaron una vulnerabilidad en el sistema de Twitter que fue aprovechada por unos piratas informáticos que usaron herramientas de predicción de contraseñas, o que trataron de acceder usando contraseñas robadas a otros servicios esperando que los empleados de Twitter hubieran usado la misma contraseña para acceder al sistema de la compañía.

Twitter podría haber limitado esos riesgos implementando un sistema de contraseñas más seguro, por ejemplo, exigiéndole a sus empleados que escogieran contraseñas complejas y capacitándolos para que no usaran la misma contraseña o una similar para acceder a las cuentas de la compañía y a las cuentas personales.

En el caso *Drizly*, la FTC alegó que la compañía no exigió que se crearan contraseñas complejas y únicas o que se implementara un sistema de autenticación de múltiples factores para acceder a los repositorios GitHub de la compañía. Un ejecutivo de Drizly reutilizó una contraseña que había usado para otras cuentas personales, pero su contraseña reciclada quedó expuesta en un incidente de seguridad de datos no relacionado. Esto creó una oportunidad para que un sujeto malintencionado accediera a los repositorios de GitHub de Drizly, lo que hizo posible que el atacante accediera a otras credenciales de bases de datos y, en última instancia, exfiltrara la información personal de 2.5 millones de consumidores. La compañía podría haber reducido esos riesgos exigiendo a los empleados la creación de contraseñas únicas y complejas (es decir, contraseñas largas que la persona no utilice para ningún otro servicio en línea) o un sistema de autenticación de múltiples factores para proteger el acceso al código fuente o a las bases de datos. Mejor aún, las compañías pueden exigir a los empleados que utilicen llaves de seguridad para acceder a la red.

Guarde las contraseñas de manera segura.

No les facilite el acceso a las contraseñas a los intrusos. En el caso contra *Twitter* de 2011, la FTC dijo que la compañía no estableció políticas para prohibirles a sus empleados el almacenamiento de contraseñas administrativas en formato de texto sin codificación para las cuentas personales de email. Twitter podría haber reducido el riesgo si hubiera implementado políticas y procedimientos para almacenar las credenciales de manera segura. Los negocios deberían considerar otras protecciones para protegerse contra el compromiso de contraseñas, por ejemplo, el uso de un sistema de autenticación de múltiples factores o hashing cifrado fuerte y adaptable que tiene iteraciones significativas del algoritmo hashing para cada contraseña. En el caso *Chegg*, se alegó que la compañía compartía sus credenciales root de acceso a AWS entre sus empleados y contratistas externos, y no cancelaba ni actualizaba dichas credenciales cuando un contratista abandonaba la compañía. Posteriormente, un ex contratista pudo utilizar las credenciales para exfiltrar la información personal de 40 millones de usuarios de Chegg. Chegg podría haber protegido sus credenciales root de acceso a AWS exigiendo que los empleados y contratistas utilizaran claves de acceso distintas, y requiriendo el uso de un sistema de autenticación de múltiples factores para acceder a las bases de datos de AWS de la compañía. Las compañías también pueden rotar periódicamente las claves existentes.

Establezca una protección contra los ataques de fuerza bruta.

¿Recuerda aquel dicho sobre el experimento con una cantidad infinita de monos operando una cantidad infinita de máquinas de escribir? Los piratas informáticos usan programas automatizados que realizan una función similar. Estos ataques de fuerza bruta consisten en el ingreso de interminables combinaciones de caracteres hasta que los piratas informáticos logran dar con la contraseña de alguna persona. O los piratas informáticos pueden tratar de usar credenciales robadas en otros incidentes de seguridad de datos. En el caso *TaxSlayer*, la FTC alegó que la compañía no implementó medidas adecuadas de autenticación basadas en el riesgo. Como resultado, unos piratas informáticos malintencionados pudieron obtener acceso total a las cuentas de casi 9,000 consumidores y luego usaron la información robada para cometer robo de identidad relacionado con impuestos.

Según la FTC, TaxSlayer no puso en práctica una serie de medidas de protección para reducir el riesgo para la información delicada de los consumidores. Por ejemplo, TaxSlayer podría haber tomado medidas para neutralizar los ataques a la lista de validación, podría hacer uso de herramientas fácilmente disponibles para impedir que los dispositivos o las direcciones IP intentaran acceder a un número ilimitado de cuentas en rápida sucesión, y pudo haber realizado una evaluación de riesgos que habría identificado las amenazas razonablemente previsibles relacionadas con una autenticación inadecuada. Las compañías también pueden impedir que los usuarios utilicen contraseñas que se sabe que han sido comprometidas en filtraciones de datos previas.

Establezca una protección para que no se pueda eludir el paso de autenticación.

El hecho de cerrar con llave la puerta principal no ofrece demasiada protección si se deja abierta la puerta trasera. En el caso *Lookout Services*, la FTC alegó que la compañía no probó adecuadamente su aplicación web para verificar si era vulnerable a fallos de seguridad ampliamente conocidos, incluido un fallo llamado “locación predecible de recursos”. Como resultado, un pirata informático pudo predecir fácilmente los patrones y manipular las direcciones URL para eludir la pantalla de autenticación de la aplicación web y acceder a las bases de datos de la compañía sin la debida autorización. La compañía podría haber mejorado la seguridad de su mecanismo de autenticación probando las vulnerabilidades más comunes.

4

Almacene la información personal delicada de manera segura y protéjala durante la transmisión.

Para muchas compañías, el almacenamiento de datos delicados es una necesidad comercial. Y aunque usted tome las medidas apropiadas para proteger su red informática, a veces tiene que enviar los datos a otra parte. Use una codificación sólida para proteger el material confidencial durante el proceso de almacenamiento y

transmisión. El método a aplicar dependerá de los tipos de información que recolecte su negocio, y de cómo la recolecte y la procese. Dependiendo de la naturaleza de su negocio, algunas alternativas incluyen el sistema de codificación Transport Layer Security o TLS, codificación de datos inactivos o un código criptográfico iterativo. Pero cualquiera sea el método que elija, solo funcionará correctamente si el personal que lo implementa lo hace de la manera apropiada. Asegúrese de que el personal asignado a esta tarea comprenda el modo en que su compañía usa los datos delicados y que tenga los conocimientos necesarios para determinar qué es lo que debe hacer en cada situación. Considerando esos conceptos, estas son algunas lecciones que surgen de los casos de la FTC que usted debe tener en cuenta cuando tome medidas para proteger la información delicada durante el proceso de almacenamiento y transmisión.

Mantenga la seguridad de la información delicada a lo largo de su vida útil.

Los datos no permanecen quietos en un solo lugar. Por lo cual, si su negocio necesita transmitir información, es importante que considere la seguridad en todas las etapas. Por ejemplo, en el caso *Superior Mortgage Corporation*, la FTC alegó que la compañía usó codificación SSL para proteger la transmisión de la información personal delicada entre el navegador de internet del cliente y el servidor del sitio web del negocio. Pero cuando la información llegó al servidor, el proveedor de servicio de la compañía la decodificó y la envió por email a la oficina central y a las sucursales de la compañía en un formato de texto legible y sin codificación. La compañía podría haber prevenido ese riesgo verificando la protección de los datos a lo largo de su vida útil, y no solo durante la transmisión inicial.

Use métodos probados y aceptados por la industria.

Cuando esté considerando los estándares técnicos a seguir, tenga presente que es posible que los expertos ya hayan desarrollado estándares efectivos que usted puede aplicar en su negocio. No tiene que comenzar desde cero cuando no es necesario. En lugar de eso, aproveche los conocimientos acumulados por los expertos. El caso *Lenovo* ilustra ese principio. Según la FTC, la compañía usó un método inseguro para reemplazar certificados digitales en sitios web codificados por otros certificados firmados por su propio software. Sin embargo, su software no verificaba adecuadamente que los

certificados digitales de los sitios web fueran válidos antes de reemplazarlos. La compañía podría haber evitado esta debilidad utilizando métodos probados y aceptados por la industria para autenticar sitios web.

Controle la correcta configuración del sistema de codificación.

La codificación, incluso la mejor de todas, no les ofrecerá protección a sus usuarios si usted no la configura correctamente. Ese es un mensaje que los negocios pueden extraer de las acciones de la FTC contra *Fandango* y *Credit Karma*. En estos casos, la FTC alegó que las compañías usaron una codificación SSL en sus aplicaciones móviles, pero que desactivaron un proceso crítico conocido como validación del certificado SSL sin implementar ninguna otra medida de seguridad compensatoria. Eso causó la vulnerabilidad de las aplicaciones a los ataques de intermediarios lo cual permitió que los piratas informáticos decodificaran la información delicada transmitida por las aplicaciones.

5

Segmente su red y haga un monitoreo para controlar quién está tratando de entrar y salir.

Cuando diseñe su red informática, considere utilizar algunas herramientas para validar y limitar la fiabilidad implícita entre los sistemas conectados en red. Dé por supuesto que todo tráfico es hostil, independientemente de su origen. Parte de sus herramientas de “confianza cero” deben ser aquellas que sirvan para inspeccionar y registrar el tráfico de red, como las herramientas SIEM y SOAR, para monitorear su red en busca de actividad maliciosa. A continuación, algunas lecciones que surgen de los casos de la FTC para tener en cuenta al momento de diseñar su red.

Valide continuamente el acceso a los datos.

No es necesario que todas las computadoras de su sistema puedan comunicarse entre sí. Usted puede proteger los datos particularmente delicados alojándolos en un lugar seguro y separado de su red. Esa es una lección que surge del caso *Infotrax*. La FTC

alegó que la compañía no limitó suficientemente el acceso de los distribuidores de un cliente a los datos de otro cliente en la red. Como resultado, unos piratas informáticos se introdujeron en el servidor de la compañía a través de la página web de un solo cliente y así lograron acceder a los datos de los consumidores de todos los clientes de la red.

La compañía podría haber reducido ese riesgo validando continuamente el acceso a sus datos.

Monitoree la actividad de su red informática.

“¿Qué está sucediendo en mi red?” Una herramienta de información sobre seguridad y gestión de eventos conocida como SIEM permitirá responder esa pregunta a su personal de seguridad.

En el caso ***i-Dressup***, la FTC alegó que la compañía no utilizó un sistema de detección y prevención de intrusiones. La compañía no tuvo conocimiento de que un pirata informático había logrado acceder a su red comprometiendo la información personal de alrededor de 245,000 niños menores de 13 años hasta que se enteró del incidente de seguridad de datos por un periodista que había estado en contacto con el pirata informático. La compañía podría haber detectado este incidente de seguridad de datos mucho antes si hubiera utilizado medidas de seguridad fácilmente disponibles y de bajo costo para recibir alertas acerca de las instancias de acceso no autorizado a su red.

En términos más generales, en el caso ***DealerBuilt***, la FTC alegó que la compañía no usó medidas de seguridad para monitorear sus sistemas y activos. Como resultado, cuando un empleado conectó un dispositivo de almacenamiento a la red de copias de seguridad de la compañía sin asegurarse de que ese dispositivo estuviera configurado de forma segura, la conexión insegura resultante creó una oportunidad para que un pirata informático accediera a la base de datos de copias de seguridad. La FTC dijo que, entonces, el pirata informático descargó la información personal de decenas de miles de consumidores que incluían números de Seguro Social y licencias de conducir, fechas de nacimiento e información financiera. La compañía podría haber identificado antes este incidente de seguridad de datos utilizando herramientas fácilmente disponibles para monitorear sus sistemas.

Las compañías preocupadas por mantener la seguridad de sus redes pueden considerar el uso de “canarios” como una ayuda para descubrir intentos de acceso no autorizados. ¿Qué es un canario? Es una trampa diseñada para comprobar si hay intrusos que están intentando entrar a su sistema sin poner realmente en peligro su red. Esto podría implicar, por ejemplo, añadir un hardware o software a una red simulada que en realidad no interactúa con su sistema. Si aparece algo que intenta interactuar con ese canario, es señal de que puede haber un intruso moviéndose por su red.

6

Proteja el acceso remoto a su red.

La actividad de un negocio no se desarrolla únicamente en la oficina. Si bien es cierto que tener personal que realiza tareas fuera de la oficina puede aumentar la productividad de su negocio, también es cierto que la movilidad puede plantear nuevos desafíos para la seguridad. Si usted permite que sus empleados, clientes o proveedores de servicio accedan a su red informática desde terminales remotas, ¿ha tomado las medidas necesarias para proteger esos puntos de acceso? Los casos de la FTC indican algunos factores a tener en cuenta cuando desarrolle sus políticas de acceso remoto.

Controle la seguridad en cada terminal de acceso.

Así como la fortaleza de una cadena se define por su eslabón más débil, el nivel de seguridad de su red estará determinado por la computadora más vulnerable con acceso remoto a su red. Ese es el mensaje de los casos de la FTC contra unas compañías que no se aseguraron de que las computadoras con acceso remoto a sus redes estuvieran protegidas correctamente en cada terminal de acceso. Por ejemplo, en el caso **Premier Capital Lending**, la compañía presuntamente habilitó una sesión de conexión remota a una cuenta para que un cliente del negocio pudiera obtener informes de consumidores sin evaluar previamente la seguridad de ese cliente. Cuando los piratas informáticos accedieron al sistema del cliente, le robaron sus credenciales de conexión remota y las usaron para apropiarse de la información personal de los consumidores. De acuerdo a los términos de la demanda contra **Settlement One**, el negocio permitió que algunos clientes que carecían de las medidas básicas de seguridad, como firewalls y software

antivirus actualizados, accedieran a informes de consumidores a través de su portal en línea.

Y en el caso **LifeLock**, la FTC alegó que la compañía no instaló programas antivirus en las computadoras que los empleados usaban para acceder remotamente a su red informática. Hoy en día, estos negocios podrían haber reducido estos riesgos utilizando herramientas de detección y respuesta en las terminales, así como soluciones de seguridad de detección y respuesta ampliadas, a menudo denominadas herramientas EDR/XDR, para reforzar la seguridad de las terminales de la red y permitir una detección y respuesta más rápidas a los incidentes de seguridad.

Implemente límites prudentes para el acceso.

No todas las personas que ocasionalmente pudieran tener la necesidad de acceder a su red deben tener un pase libre para acceder a toda la información confidencial. En lugar de eso, limite el acceso en función de los parámetros de una tarea concreta. Por ejemplo, en el caso **Dave & Buster's**, la FTC alegó que la compañía no restringió adecuadamente el acceso de terceros a su red. Aprovechando la debilidad del sistema de una tercera compañía, presuntamente, un intruso logró conectarse a la red de Dave & Buster's varias veces e interceptar información personal. ¿Qué podría haber hecho Dave & Buster's para reducir ese riesgo? Podría haber implementado límites para evitar el acceso de terceros a su red, por ejemplo, en las conexiones a datos delicados, o podría haber concedido un acceso temporal cuidadosamente restringido a los datos que el tercero necesitaba para realizar su trabajo.

7

Aplique prácticas de seguridad sólidas cuando desarrolle nuevos productos.

Así que tiene una gran aplicación nueva o un software innovador en su tablero de diseño. Pues en las primeras etapas del proceso de desarrollo piense cómo les gustaría usar el producto a los clientes. Si los clientes van a almacenar o enviar información delicada, pregúntese si su producto está en condiciones de manejar los datos de

manera segura. Antes de lanzar su producto al mercado, considere las lecciones de los casos de la FTC relacionados con el desarrollo, diseño, prueba y puesta en marcha de un producto.

Capacite a sus ingenieros en materia de codificación de seguridad.

¿Les ha explicado a sus desarrolladores la necesidad de mantener la seguridad en primera línea? En los casos como el de **Tapplock** y **Zoom**, la FTC alegó que las compañías no capacitaron a sus empleados en materia de prácticas de codificación seguras. En el caso *Tapplock*, la FTC dijo que la compañía promocionó la seguridad de sus cerraduras, incluida la seguridad digital. Las cerraduras inteligentes de la compañía recopilaban información personal de los consumidores, incluidos nombres de usuario, direcciones de email, fotos de perfil y las ubicaciones precisas de las cerraduras. Sin embargo, según la FTC, las cerraduras presentaban vulnerabilidades que impedían a los consumidores revocar efectivamente el acceso a sus cerraduras. Los investigadores de seguridad descubrieron que podían eludir el proceso de autenticación de cuentas de Tapplock y acceder a los datos de los usuarios. La compañía podría haber evitado estos problemas implementando un programa de seguridad que incluyera pruebas de vulnerabilidad e intrusión de sus cerraduras, asegurándose de que se hubieran implementado salvaguardias eficaces para proteger los datos de los consumidores y formando a sus ingenieros de software en prácticas de codificación seguras.

En el caso *Zoom*, la FTC alegó que la compañía puso en riesgo la seguridad de algunos usuarios al instalar secretamente un software, llamado servidor web ZoomOpener, para una actualización manual de su aplicación de escritorio para Mac. En condiciones normales, antes de que se iniciara la aplicación de Zoom, el navegador Safari de Apple mostraba un cuadro de advertencia que les preguntaba a los usuarios si querían iniciar la aplicación. Pero el servidor web ZoomOpener permitía que Zoom iniciara automáticamente la reunión y la posibilidad de unirse a ella, eludiendo así la protección de Safari que protegía a los usuarios de un tipo común de programa malicioso. De acuerdo a los términos de la demanda, la instalación encubierta de ZoomOpener aumentó el riesgo de videovigilancia remota por parte de extraños, y la compañía no implementó ninguna medida compensatoria para proteger la seguridad de los usuarios. Además, el software permaneció instalado en las computadoras de los usuarios incluso

después de que la eliminaran, y en determinadas circunstancias, la aplicación incluso se reinstalaba automáticamente sin ninguna acción por parte del usuario. La compañía podría haber evitado esta vulnerabilidad implementando un programa de capacitación sobre prácticas seguras de desarrollo de software.

Siga las pautas de las plataformas en materia de seguridad.

En lo que se refiere a la seguridad, tal vez no sea necesario reinventar la rueda. A veces, lo más sensato es escuchar a los expertos. En las acciones contra **HTC America**, **Fandango** y **Credit Karma**, la FTC alegó que las compañías no siguieron las pautas explícitas de la plataforma sobre las prácticas de desarrollo seguro. Por ejemplo, la FTC alegó que Fandango y Credit Karma desactivaron en sus aplicaciones móviles un proceso crucial conocido como validación de certificado, dejando la información delicada que los consumidores transmitían a través de esas aplicaciones en riesgo de ser interceptada mediante ataques de intermediarios. Las compañías podrían haber prevenido esta vulnerabilidad siguiendo las pautas de iOS y Android para los desarrolladores que advierten explícitamente contra la desactivación del certificado de validación. El consejo para otras compañías: cuando escojan entre herramientas y plataformas de terceros, elijan aquellas que estén diseñadas para el mantenimiento de la seguridad y que tengan valores predeterminados seguros que mitiguen los riesgos desde el primer momento.

Verifique el correcto funcionamiento de las funciones de privacidad y seguridad.

Si su software le ofrece una función de privacidad o seguridad, verifique que esa función opere tal como se anuncia. Por ejemplo, en el caso **TRENDnet**, la FTC acusó a la compañía de no probar la efectividad de una opción para mantener la privacidad de las filmaciones de las cámaras de los consumidores para restringir el acceso a esas filmaciones. Como resultado, cientos de filmaciones “privadas” quedaron a la vista del público.

De manera similar, en el caso **Snapchat**, la compañía anunció que los mensajes “desaparecerían para siempre”, pero la FTC dice que la compañía no tomó las medidas necesarias para garantizar la veracidad de esa declaración. Entre otras cosas, la aplicación almacenó archivos de video fuera del entorno restringido de verificación o

sandbox de la aplicación, lo cual facilitó la recuperación de los archivos de video con herramientas comunes de visualización de archivos. Lecciones que surgen de los casos de otras compañías: cuando ofrezca funciones de privacidad y seguridad, asegúrese de que su producto funcione conforme a sus declaraciones publicitarias.

Pruebe las funciones para detectar las vulnerabilidades comunes.

No hay manera de prever cada amenaza, pero hay algunas vulnerabilidades que son comúnmente conocidas y razonablemente evitables. En más de una docena de casos de la FTC, los negocios no evaluaron adecuadamente sus aplicaciones para verificar la existencia de vulnerabilidades bien conocidas. Por ejemplo, en el caso *D-Link*, la FTC alegó que la compañía no llevó a cabo los procedimientos básicos esenciales para un desarrollo de software seguro, incluidas las pruebas y la corrección de fallos de seguridad conocidos y evitables. Como resultado, los enrutadores y las cámaras conectadas a internet de D-Link quedaron expuestos a terceros y vulnerables a ataques de piratas informáticos.

De manera similar, en el caso *CafePress*, la FTC alegó que la compañía no protegió su sitio web contra los ataques comunes por inyección SQL (Structured Query Language), lo cual causó la exposición de información delicada de consumidores como los números de Seguro Social. Ese es un riesgo que podría haberse evitado si CafePress hubiera hecho pruebas para detectar vulnerabilidades conocidas comúnmente, como aquellas identificadas por el Open Web Application Security Project (OWASP).

8

Asegúrese de que sus proveedores de servicio implementen medidas de seguridad razonables.

En materia de seguridad, abra bien los ojos para mantener vigilados a sus proveedores de servicio, por ejemplo, las compañías que contrata su negocio para procesar la información personal de sus clientes o para desarrollar aplicaciones. Antes de contratar un proveedor, sea franco respecto a sus expectativas de seguridad. Siga los pasos

lógicos y necesarios para seleccionar proveedores capaces de implementar medidas de seguridad adecuadas y para controlar que cumplan sus requerimientos. Los casos de la FTC ofrecen orientación sobre lo que se debe tener en cuenta al momento de contratar y supervisar a los proveedores de servicio.

Póngalo por escrito.

Insista para que los estándares de seguridad apropiados formen parte de sus contratos. Por ejemplo, en el caso ***GMR Transcription***, la FTC alegó que la compañía contrató proveedores de servicio para transcribir archivos de audio con información delicada, pero omitió exigirle al proveedor del servicio que tomara medidas de seguridad razonables. Como resultado, los archivos, muchos de ellos con datos de salud altamente confidenciales, quedaron ampliamente expuestos en internet. Por empezar, el negocio podría haber incluido disposiciones contractuales que les exigieran a los proveedores de servicio que adoptaran precauciones razonables de seguridad, por ejemplo, un sistema de codificación.

Verifique el cumplimiento.

La seguridad no puede ser algo que se base en un “le doy mi palabra”. Un primer paso importante es incluir sus expectativas de seguridad en los contratos con sus proveedores de servicio, pero también es importante desarrollar tareas de supervisión a lo largo del proceso. El caso ***Upromise*** ilustra este punto. En este caso, la compañía contrató un proveedor de servicio para desarrollar una barra de herramientas para un navegador. Upromise dijo que la barra de herramientas, que recolectaba información de navegación de consumidores para proporcionarles ofrecimientos personalizados, usaría un filtro para “eliminar cualquier información personal identificable” antes de la transmisión.

Pero según la FTC, Upromise omitió verificar que el proveedor de servicio hubiera implementado el programa de recolección de información de conformidad con las políticas de privacidad y seguridad de Upromise y con los términos del contrato diseñados para proteger la información de los consumidores. Como resultado, la barra de herramientas recolectó información personal delicada que incluía números de cuentas financieras y códigos de seguridad de páginas web seguras, y transmitió

esos datos en formato de texto sin codificación. ¿Qué podría haber hecho la compañía para reducir ese riesgo? Hacerle preguntas al proveedor del servicio e implementar un seguimiento durante el proceso de desarrollo.

9

Implemente procedimientos para mantener actualizada la seguridad y ocúpese de las vulnerabilidades que pudieran surgir.

La protección de su software y de sus redes no es algo que se haga de una vez y para siempre. Es un proceso continuo que exige mantener la guardia alta. Si sus redes usan un software de terceros, o si sus aplicaciones incluyen bibliotecas de software de terceros, aplique actualizaciones a medida que estén disponibles. Si usted desarrolla su propio software, ¿qué medidas va a implementar para que la gente le informe si detectó una vulnerabilidad y qué hará usted para resolver el problema? Los casos de la FTC ofrecen algunos puntos a considerar al momento de analizar el manejo de las vulnerabilidades.

Actualice y repare el software de terceros.

Un software desactualizado atenta contra la seguridad. La solución es actualizarlo regularmente e implementar los parches de terceros. Por ejemplo, en el caso de **TJX Companies**, la FTC alegó que la compañía no actualizó su software antivirus, lo cual aumentó el riesgo de que los piratas informáticos pudieran explotar las vulnerabilidades conocidas o vencer las defensas del negocio. De manera similar, en el caso **Equifax**, la FTC alegó que la compañía no reparó una vulnerabilidad crucial, en parte debido a que sus políticas y procedimientos de manejo de parches eran inadecuados. Dependiendo de la complejidad de su red informática o de su software, es posible que tenga que priorizar los parches de acuerdo al nivel de gravedad de la amenaza que pretenden impedir. No obstante, disponer de un proceso razonable para actualizar y reparar el software de terceros es un paso importante para reducir el riesgo de un ataque. Considere la posibilidad de utilizar herramientas automatizadas para saber qué versiones de software ejecuta su sistema y si hay actualizaciones disponibles.

Preste atención a las advertencias de seguridad creíbles y actúe con rapidez para solucionarlas.

Cuando se presenten vulnerabilidades, escuche atentamente y actúe. En el caso *HTC America*, la FTC alegó que la compañía no tenía implementado un proceso para recibir los reportes de vulnerabilidades de seguridad y ocuparse de ellas. La presunta demora de HTC en responder a las advertencias implicó que las vulnerabilidades afectaran más aparatos a través de múltiples versiones del sistema operativo.

A veces las compañías reciben alertas de seguridad, pero se pierden en la confusión. Por ejemplo, en el caso *Fandango*, la compañía confió en su sistema general de servicio al cliente para responder a las advertencias sobre los riesgos de seguridad. Según se indicó en la demanda, cuando un investigador se comunicó con el negocio para reportar una vulnerabilidad, el sistema categorizó el reporte incorrectamente como una solicitud de restablecimiento de contraseña, envió una respuesta automática, y marcó el mensaje como “resuelto” sin señalarla para su posterior revisión. Como resultado, Fandango no se enteró de la vulnerabilidad hasta que el personal de la FTC se comunicó con la compañía. ¿Lecciones que surgen de otros negocios? Implemente un proceso efectivo para recibir y resolver los reportes de vulnerabilidad. Considere implementar un canal efectivo y claramente anunciado (por ejemplo, un domicilio de email exclusivo para ese fin como security@yourcompany.com) para recibir los reportes y señalarlos para que su personal de seguridad los revise.

10

Proteja los archivos impresos en papel, los soportes físicos y los dispositivos.

La seguridad de la red es una consideración crucial, pero muchas de las mismas lecciones se aplican a la información impresa en papel y a otros medios físicos de almacenamiento de datos como discos duros, computadoras portátiles, unidades de memoria flash y discos de almacenamiento. Los casos de la FTC ofrecen algunos puntos a considerar al momento de evaluar la seguridad física en su negocio.

Guarde de manera segura los archivos con información delicada.

Si necesita retener documentación impresa importante, tome medidas para protegerla. En el caso **Gregory Navone**, la FTC alegó que el demandado guardó información de consumidores delicada que había recolectado en su ex negocio dentro de unas cajas que mantuvo en su garaje. En la demanda del caso **LifeLock**, se alegó que la compañía dejó documentos enviados por fax que contenían información personal de consumidores en un lugar abierto y de fácil acceso. En ambos casos, los negocios podrían haber reducido el riesgo para sus clientes implementado políticas para almacenar los documentos de manera segura.

Proteja los dispositivos que procesan información personal.

Las medidas de seguridad que implemente para proteger la información almacenada en su red no serán efectivos para proteger a sus clientes si los datos ya han sido robados a través del aparato o dispositivo que los recolecta. En la investigación del caso **Dollar Tree**, el personal de la FTC dijo que los dispositivos que utilizó el negocio para ingresar los números de identificación personal o PIN de los clientes eran vulnerables a la manipulación y al robo. Como resultado, a través de un ataque conocido como “PED skimming” unas personas no autorizadas pudieron capturar los datos de las tarjetas de pago de los consumidores, incluidos los datos de la banda magnética y el PIN. En ese momento, debido a lo novedoso de ese tipo de tentativa y a otros varios factores, el personal de la FTC cerró la investigación. Sin embargo, actualmente los ataques contra los dispositivos utilizados en los puntos de venta son bien conocidos y los negocios deben tomar las medidas lógicas y necesarias para proteger ese tipo de dispositivos.

Implemente estándares de seguridad para proteger los datos itinerantes.

Es necesario comprender la importancia de proteger la información delicada cuando se encuentra fuera de la oficina. Por ejemplo, en el caso **Accretive**, la FTC alegó que un empleado dejó su computadora portátil con más de 600 archivos que incluían 20 millones de datos relacionados con 23,000 pacientes dentro del compartimiento cerrado del asiento del acompañante de un carro que fue robado. El caso **CBR Systems** involucró cintas de copias de seguridad supuestamente codificadas, una computadora

portátil y un disco externo que contenían información delicada, todo lo cual fue sustraído del carro de un empleado. En ambos casos, los negocios podrían haber reducido el riesgo para la información personal de los consumidores implementando políticas de seguridad razonables para proteger los datos itinerantes. Por ejemplo, cuando envíe archivos, discos, unidades de memoria, etc., use un método de envío que le permita hacer un seguimiento del trayecto del paquete. Limite las situaciones que impliquen que sus empleados salgan de la oficina con datos delicados en su poder. Pero cuando se presente una necesidad comercial legítima de viajar con información confidencial, los empleados la tienen que mantener fuera de la vista de terceros, y en la medida de lo posible, deben guardarla bajo llave.

Elimine los datos delicados de manera segura.

La documentación o los aparatos que ya no necesita le pueden parecer basura, pero si contienen información personal sobre consumidores o empleados, son un tesoro para los ladrones de identidad. Por ejemplo, según se indica en las demandas de los casos de la FTC contra *Rite Aid* y *CVS Caremark*, las compañías desecharon información personal delicada como recetas de prescripción médica en contenedores de basura.

En el caso *Goal Financial*, la FTC alegó que un empleado vendió un excedente de discos duros que contenían información personal delicada de aproximadamente 34,000 clientes en un formato sin codificar. Las compañías podrían haber prevenido el riesgo para la información personal de los consumidores triturando, quemando o pulverizando los documentos para que quedaran ilegibles y usando tecnología disponible para borrar la información de dispositivos en desuso.

¿Está buscando más información?

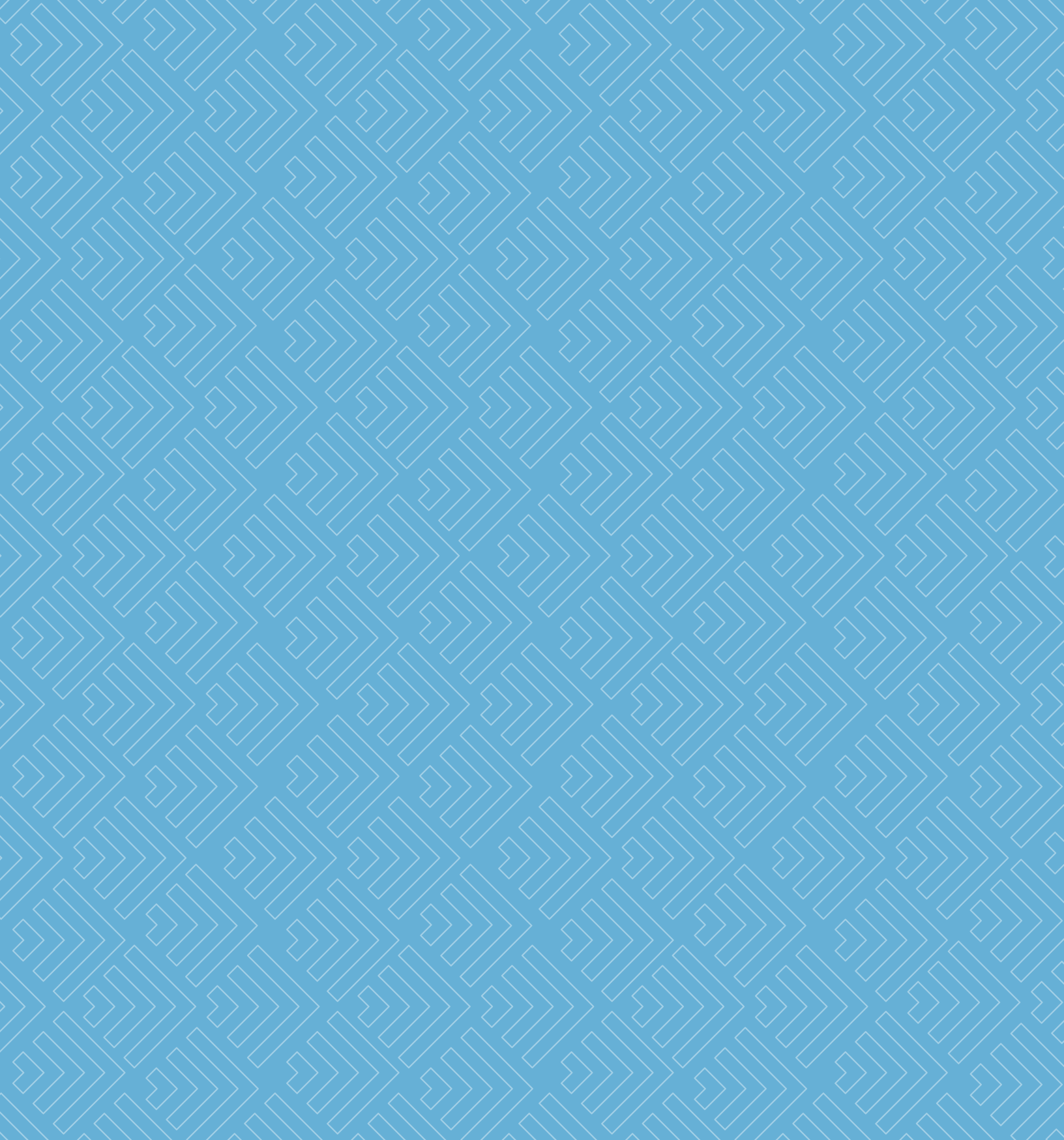
Visite la sección de Seguridad de datos de ftc.gov/es/guia-para-negocios donde podrá encontrar una lista de casos relevantes y otros recursos gratuitos.

Acerca de la FTC

La FTC trabaja para prevenir las prácticas fraudulentas, engañosas y desleales dirigidas contra los negocios y los consumidores. Reporte las estafas y las malas prácticas comerciales en [ReporteFraude.ftc.gov](https://www.ftc.gov/whistleblower). También ofrecemos orientación en [ftc.gov/es/guia-para-negocios](https://www.ftc.gov/es/guia-para-negocios) para ayudar a las compañías a cumplir la ley. Independientemente del tamaño de su organización o del sector al que se dedique, conocer y cumplir sus responsabilidades en materia de cumplimiento es un negocio inteligente y sólido. ¿Quiere acceder a una rápida reseña sobre los casos recientes y otras iniciativas? Suscríbese al [Blog para negocios de la FTC](#).

Su oportunidad de presentar comentarios

La agencia National Small Business Ombudsman y 10 juntas regionales llamadas Regional Fairness Boards recogen comentarios de parte de los pequeños negocios sobre las acciones federales de cumplimiento y ejecución. Todos los años, el Ombudsman evalúa la conducta de dichas actividades y califica la capacidad de respuesta de cada agencia ante los pequeños negocios. Los pequeños negocios pueden presentar comentarios al Ombudsman sin temor a represalias. Para presentar comentarios, llame a la línea gratuita 1-888-REGFAIR (1-888-734-3247) o visite [sba.gov/ombudsman](https://www.sba.gov/ombudsman).



La Comisión Federal de Comercio
ftc.gov/es/guia-para-negocios

Agosto 2023