
CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

El Mercado y la seguridad cibernética

Centros de Servicios de Medicare y Medicaid (CMS)
Centro de Información al Consumidor y Supervisión de Seguros (CCIIO)

Febrero de 2024

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Temas

01 Amenazas frecuentes contra la información de identificación personal (PII)

02 Seguridad de la información y PII

03 Amenazas e incidentes de seguridad cibernética

04 Higiene de seguridad cibernética

05 Recursos de seguridad cibernética

Amenazas frecuentes contra PII

- Proteger la PII de sus clientes es una de sus funciones más importantes como agente o corredor. Una parte crucial de la protección es la prevención: tener consciencia de que las amenazas cibernéticas pueden provenir de un mensaje de texto, un correo electrónico o cualquier otro lugar en línea.
- Tenga presentes las estadísticas siguientes mientras piensa cómo pueden afectarle las amenazas cibernéticas y cómo debe hablar sobre ellas con sus clientes.

Tipos de PII

- PII es información que puede usarse sola o combinada con otros elementos de datos a fin de distinguir o rastrear la identidad de un individuo.
- Para manipular PII de manera efectiva, consulte esta pregunta frecuente (FAQ) a fin de informarse sobre los requisitos para agentes y corredores.
- Hay muchos tipos de PII, que pueden incluir:
  - Dirección del solicitante
  - Pago adelantado máximo del importe del crédito tributario para las primas (APTC) del solicitante
  - Nivel de reducciones de costos compartidos (CSR) del solicitante
  - Ingresos del hogar del solicitante
  - Identificación (ID) del Intercambio Facilitado por el Gobierno Federal (FFE) del solicitante
  - Cuenta corriente y número de ruta
  - Información de salud privada (PHI), como historias clínicas y resultados de laboratorio
  - Información tributaria federal

Cómo proteger la PII de los consumidores

- Los agentes y corredores no pueden difundir, publicar ni divulgar PII de consumidores a personal no autorizado y deben proteger esa información de acuerdo con las regulaciones y las leyes federales referidas a la manipulación de PII.
- Como agente o corredor, usted puede proteger la PII de los consumidores con estas acciones:
  - Aplicar un principio de "necesidad de saber" antes de divulgar PII a otro personal.
  - Evaluar una necesidad de PII solicitada antes de compartir con terceros.
  - Limitar la PII al uso oficial únicamente.
  - Consulte el Acuerdo de privacidad y seguridad con el Mercado Individual para el año del plan 2024, sección II, párrafo E "Obligación de proteger PII" para obtener más información sobre cómo trabajar con PII de consumidores.

Mejores prácticas para proteger PII

- **Personalmente**
  - Proteja los formularios de consentimiento de consumidores impresos en un lugar con llave.
  - Durante las citas con consumidores, use espacios privados para garantizar la privacidad.
- **En línea**
  - No envíe ni reenvíe correos electrónicos con PII a cuentas de correo electrónico personales.
  - No use dispositivos móviles no autorizados para acceder a PII.
- **Al trabajar con terceros**
  - Asegúrese de que todos los originales de registros de consumidores se devuelvan antes de salir de su oficina y solo haga copias para sí u otras personas si es necesario para realizar tareas requeridas.

Escenario de incidentes con PII

Charlie, experto en seguridad cibernética de los CMS, pregunta…

Jackson está revisando un documento que contiene PII, donde aparecen varios números de seguro social (SSN). Copia a su supervisor en un correo electrónico para recibir su opinión sobre un enfoque con respecto a esa información, pero olvida cifrar el correo electrónico con una contraseña. ¿Por qué las acciones de Jackson indican una posible vulneración de PII?

Escenario de incidentes con PII (continuación)

» Las acciones de Jackson indican una posible vulneración de PII porque si copia información sensible en un correo electrónico sin cifrado (como protegerlo con una contraseña), esto deja la información vulnerable a partes externas, como hackers. Los SSN constituyen PII.

Consejo de Charlie, experto en seguridad cibernética de los CMS:

Si se debe enviar PII por correo electrónico, se la debe cifrar y seguir determinados protocolos para proteger los datos.

Comprobación de conocimientos n.° 1

Charlie, experto en seguridad cibernética de los CMS, pregunta…

Fatimah está trabajando en el informe de un cliente para su gerente. Le resulta más rápido extraer datos del cliente existentes de otro informe que crear uno nuevo. El informe existente también contiene SSN y fechas de nacimiento, datos que Fatimah no necesita. ¿Está bien que Fatimah use el informe para ahorrar tiempo?

a) Sí. Le ayudará a hacer su trabajo.

b) No. Como agente o corredora, Fatimah solo debe acceder a información según sea necesario para cumplir su función laborar y solo para propósitos autorizados.

Comprobación de conocimientos n.° 1: Respuesta

Charlie, experto en seguridad cibernética de los CMS, pregunta…

Fatimah está trabajando en el informe de un cliente para su gerente. Le resulta más rápido extraer datos del cliente existentes de otro informe que crear uno nuevo. El informe existente también contiene SSN y fechas de nacimiento, datos que Fatimah no necesita. ¿Está bien que Fatimah use el informe para ahorrar tiempo?

a) Sí, porque le ayudará a hacer su trabajo.

b) No: como agente o corredora, Fatimah solo debe acceder a información según sea necesario para cumplir su función laborar y solo para propósitos autorizados.

Comprobación de conocimientos n.° 2

Charlie, experto en seguridad cibernética de los CMS, pregunta…

> ¿Cuáles son las restricciones para que agentes y corredores compartan PII?

a) Los agentes y corredores deben aplicar un principio de necesidad de saber cuando se trata del uso autorizado de PII y si los agentes o corredores venden o transfieren su libro de negocios a otro productor, deben informar a los consumidores impactados por la venta y el cambio del número de productor nacional (NPN).

b) Los agentes y corredores pueden compartir PII con cualquier persona de su organización, siempre y cuando no compartan la PII con nadie fuera de la organización.

c) Los agentes y corredores no pueden compartir PII con nadie de su organización, incluso si eso implica ayudar al cliente con funciones necesarias para la inscripción.

Comprobación de conocimientos n.° 2: Respuesta

Charlie, experto en seguridad cibernética de los CMS, pregunta…

> ¿Cuáles son las restricciones para que agentes y corredores compartan PII?

a) Los agentes y corredores deben aplicar un principio de necesidad de saber cuando se trata del uso autorizado de PII y si los agentes o corredores venden o transfieren su libro de negocios a otro productor, deben informar a los consumidores impactados por la venta y el cambio del NPN.

b) Los agentes y corredores pueden compartir PII con cualquier persona de su organización, siempre y cuando no compartan la PII con nadie fuera de la organización.

c) Los agentes y corredores no pueden compartir PII con nadie de su organización, incluso si eso implica ayudar al cliente con funciones necesarias para la inscripción.

Suspensión por riesgo para operaciones o sistemas del Mercado

- Los CMS pueden suspender de inmediato la posibilidad de un agente o corredor de acceder a sistemas del Mercado si descubren circunstancias que representan un riesgo inaceptable para las operaciones o los sistemas de tecnología de la información del Mercado hasta que el incidente o la vulneración se solucione o se mitigue suficientemente a satisfacción del Departamento de Salud y Servicios Humanos (HHS).
  - La aplicación de esta disposición suspendería el acceso por parte de un agente o corredor al Portal empresarial de los CMS, al Sistema de Gestión de Aprendizaje del Mercado (MLMS) y a los procesos de Inscripción Directa Mejorada (DE/EDE).
  - Cualquier terminación en virtud de 45 C.F.R. § 155.220(g)(5) incluirá un aviso con 30 días de anticipación, tiempo en que los agentes tienen la oportunidad de presentar pruebas para refutar las conclusiones de los CMS antes de la terminación.
- Si su acceso al Mercado alguna vez se suspende y usted tiene preguntas sobre su suspensión, contacte a la Mesa de ayuda para agentes/corredores: FFMProducer-AssisterHelpDesk@cms.hhs.gov

Acceso a sistemas de los CMS en el extranjero

- Los agentes y corredores no pueden acceder a sistemas de los CMS en ningún punto si se encuentran fuera de los Estados Unidos de América (EE. UU.) o sus territorios. Esto incluye los sitios web de socios de DE y EDE.
- Si un consumidor presentará o actualizará su solicitud en CuidadoDeSalud.gov y contacta al agente o corredor mientras el agente o corredor se encuentra fuera de EE. UU., es posible que el agente o corredor le proporcione asistencia verbal o escrita.
  - Nota: Los agentes y corredores nunca pueden crear una cuenta en CuidadoDeSalud.gov para un consumidor o iniciar sesión en la cuenta de CuidadoDeSalud.gov de un consumidor ni en EE. UU. ni fuera del país.
- Como se indica en los Acuerdos de agentes y corredores, los agentes y corredores no tienen permiso para conectarse o transmitir datos de forma remota a FFE, a intercambios estatales en la plataforma federal (SBE-FP), a sus entornos de pruebas ni conectarse de forma remota desde ubicaciones fuera de los Estados Unidos de América o sus territorios, embajadas o instalaciones militares. Esto incluye cualquier conexión de este tipo a través de VPN.

Acceso a sistemas de los CMS en el extranjero (continuación)

- Algunos ejemplos de sistemas y sitios web a los que los agentes y corredores no pueden acceder desde fuera de EE. UU. incluyen:
  - CuidadoDeSalud.gov y sitios web privados de DE y EDE.
  - El Portal de Empresas de los CMS.
  - La biblioteca REGTAP. Nota: Las grabaciones y las presentaciones con diapositivas de webinarios y eventos organizados por REGTAP se publican en línea y están disponibles para ser revisados en cualquier lugar. Para acceder a presentaciones con diapositivas de los CMS, visite la página de Recursos generales.
- Además, los agentes y corredores no pueden usar servicios profesionales o de TI, operaciones de centrales de llamadas/apoyo a clientes, ni herramientas de software que no estén ubicadas o alojadas en EE. UU. o uno de sus territorios, embajadas o instalaciones militares.
- Si necesita asistencia adicional o quiere denunciar sospechas de violaciones de estos requisitos del Mercado, comuníquese con la Mesa de ayuda por correo electrónico para agentes/corredores escribiendo a FFMProducer-AssisterHelpDesk@cms.hhs.gov.

Incidentes de seguridad cibernética

- Un incidente es un evento o acción adversa no planificada, inusual y no deseada que tuvo lugar como resultado de falta de cumplimiento de las políticas y procedimientos de privacidad de la organización. Debe corresponder al uso o la divulgación no autorizada de PII, incluso una "divulgación accidental" como en correos electrónicos o faxes dirigidos erróneamente.[1]
- Un incidente de seguridad es un evento que debe denunciarse y que cumple con uno o más de los siguientes criterios:
  - El acceso, el uso, la divulgación, la modificación o la destrucción de información o la interferencia no autorizada y exitosa con operaciones en un sistema de información.
  - La pérdida de datos a través de robo, colocación indebida de dispositivos, colocación indebida de documentos impresos y enrutamiento indebido de correo electrónico.
  - Un hecho que real o potencialmente ponga en riesgo la confidencialidad, integridad y disponibilidad de un sistema de información o la información.
  - Una violación o amenaza de violación de políticas de seguridad de computadoras, políticas de uso aceptable o prácticas de seguridad estándar.

[1]Estas definiciones están tomadas del Memorando 17-12 de la Oficina de Administración y Presupuesto (OMB) disponible en https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf.

Incidentes de seguridad cibernética (continuación)

- Amenazas frecuentes incluyen:
  - Ingeniería social
  - Suplantación de identidad
  - Software malicioso (virus, cibersecuestro de datos, etc.)
  - Parches inadecuados o retrasados

Amenazas frecuentes: Ingeniería social

- **Definición:** La ingeniería social intenta manipularle a usted para que involuntariamente divulgue información a un hacker o realice una acción que dé lugar a una vulneración de seguridad o privacidad. Los hackers podrían aparentar ser un colega o un "amigo" para ganarse su confianza y así poder obtener acceso a su información y sistemas de información. Los hackers también pueden acechar en redes Wi-Fi gratuitas, como las de cafeterías, aeropuertos y hoteles.
- **Ejemplos:**
  - Sitios web de apariencia normal que parecen ser legítimos pueden ser comprometidos con vínculos maliciosos o software malicioso que infecte dispositivos que los visitan.
  - "Solicitudes de amistad" en redes sociales pueden suplantar a amigos y colegas para engañarle a fin de que acepte software malicioso o divulgue información sensible.

Amenazas frecuentes: Ingeniería social (continuación)

- **Prevención:**
  - Sospeche de llamadas telefónicas, visitas o mensajes de correo electrónico no solicitados de individuos que pregunten sobre empleados u otra información interna. Si un individuo desconocido declara ser de una organización legítima, intente verificar su identidad directamente con la compañía.
  - No proporcione información personal ni sobre su organización, incluida su estructura o sus redes, a menos que tenga certeza sobre la autoridad de una persona para recibir la información.
  - No revele información personal o financiera en correos electrónicos y no responda a solicitudes por correo electrónico de esa información.

Amenazas frecuentes: Suplantación de identidad

- **Definición:** La suplantación de identidad es una forma de ingeniería social con la que intrusos buscan tener acceso a información y sistemas de información haciéndose pasar por una persona, un negocio o una organización real con un motivo legítimo para solicitar la información.

  Los correos electrónicos (o mensajes de texto) de suplantación de identidad suelen alertar al usuario de un problema con su cuenta y pedirle que haga clic en un vínculo para proporcionar información a fin de corregir el problema.

- **Ejemplos:**
  - Esos vínculos pueden descargar programas maliciosos en su computadora o dispositivo móvil y permitir que el atacante acceda al dispositivo, dispositivos conectados e información almacenada en esos dispositivos.
  - Esos correos electrónicos suelen tener una apariencia real y parecer contener logotipos y marcas comerciales organizacionales reales. Pueden estar dirigidos personalmente a usted y parecer ser enviados desde una fuente legítima que usted conoce y en la que confía, como una agencia gubernamental o una organización profesional.
  - La dirección URL provista incluso puede parecerse a la dirección web auténtica, por ejemplo, “Amazons.com” con un error de ortografía muy ínfimo que uno fácilmente podría pasar por alto.

Amenazas frecuentes: Suplantación de identidad (continuación)

- **Prevención:**
  - Mantener el software antivirus actualizado.
  - Actualizar con regularidad el software en su computadora y teléfono celular.
  - Utilizar una autenticación multifactorial (MFA) con todas sus cuentas.
  - Hacer copia de seguridad de los datos de su computadora y teléfono celular.
  - Filtrar los correos electrónicos no deseados.
  - No hacer clic en vínculos ni abrir adjuntos.
- Si toma conocimiento de una vulneración o un incidente que involucre PII como resultado de suplantación de identidad, denuncie la situación de inmediato a la organización apropiada. Además, cambie la contraseña de cualquier cuenta que pueda estar comprometida.
- También puede denunciar el ataque cibernético a la policía, presentar un informe a la Comisión Federal de Comercio o denunciar el ataque cibernético a la Oficina Federal de Investigaciones (FBI), la agencia federal principal para investigar ataques cibernéticos e intrusiones.
- Para más información sobre suplantación de identidad, consulte esta hoja de consejos.

Amenazas frecuentes: Software malicioso

- **Definición:** El software malicioso, o malware, perjudica o roba información de un sistema informático o lo altera. Con frecuencia lo instala un usuario que:
  - Abre adjuntos de correo electrónico infectados.
  - Descarga archivos infectados.
  - Visita un sitio web infectado.
- **Ejemplos:** Ejemplos de software malicioso incluyen:
  - Virus
  - Gusanos
  - Troyanos
  - Cibersecuestro de datos
  - Programas espía
  - Rootkits o encubridores.

Amenazas frecuentes: Software malicioso (continuación)

- **Prevención:**
  - Leer correos electrónicos en texto sin formato.
  - Escanear los adjuntos con software antivirus antes de descargarlos.
  - Nunca abrir un adjunto de alguien desconocido.
  - Usar el botón de Correo no deseado para denunciar correos electrónicos sospechosos sin abrirlos.
- Si cree que la computadora de su negocio que contiene información sensible del Mercado está infectada, contacte a la Mesa de ayuda de TI de los CMS escribiendo a CMS_IT_Service_Desk@cms.hhs.gov.

Amenazas frecuentes: Cibersecuestro de datos

- **Definición:** El cibersecuestro de datos es un tipo de software malicioso que infecta una computadora y restringe el acceso a ella, cifra archivos y los inutiliza, al igual que a los sistemas que dependen de ellos. Después, los hackers exigen que les paguen un rescate para descifrarlos.
- **Ejemplos:**
  - Correos electrónicos de suplantación de identidad
  - Explotación de vulnerabilidades sin parches en el software.
- **Prevención:**
  - Nunca hacer clic en vínculos no verificados.
  - Escanear los correos electrónicos en busca de software malicioso.
  - Descargar solo de sitios de confianza.
  - Mantener copias de seguridad de los datos importantes.
  - Usar una red privada virtual (VPN) cuando se usa Wi-Fi pública.

Comprobación de conocimientos n.° 3

Charlie, experto en seguridad cibernética de los CMS, pregunta…

Dan recibe un correo electrónico dirigido personalmente a él y que parece enviado desde una fuente legítima en la que confía. El correo electrónico le notifica que hay un problema con su cuenta y le pide que lo corrija. Dan duda en hacer clic en el vínculo. También observa que la dirección URL provista se parece a una dirección web auténtica, pero contiene un error de ortografía. ¿Qué debe hacer? **Seleccione todas las opciones que correspondan.**

a) Hacer clic en el vínculo y proporcionar información para corregir el problema con su cuenta.

b) Verificar con su departamento de TI para asegurarse de que el correo electrónico es legítimo.

c) No hacer clic en el correo electrónico y eliminar el mensaje.

d) Reenviarle el correo electrónico a su colega y preguntarle si el correo electrónico es legítimo.

Comprobación de conocimientos n.° 3: Respuesta

Charlie, experto en seguridad cibernética de los CMS, pregunta…

Dan recibe un correo electrónico dirigido personalmente a él y que parece enviado desde una fuente legítima en la que confía. El correo electrónico le notifica que hay un problema con su cuenta y le pide que lo corrija. Dan duda en hacer clic en el vínculo. También observa que la dirección URL provista se parece a una dirección web auténtica, pero contiene un error de ortografía. ¿Qué debe hacer? **Seleccione todas las opciones que correspondan.**

a) Hacer clic en el vínculo y proporcionar información para corregir el problema con su cuenta.

b) Verificar con su departamento de TI para asegurarse de que el correo electrónico es legítimo.

c) No hacer clic en el correo electrónico y eliminar el mensaje.

d) Reenviarle el correo electrónico a su colega y preguntarle si el correo electrónico es legítimo.

Comprobación de conocimientos n.° 4

Charlie, experto en seguridad cibernética de los CMS, pregunta…

Taylor está viajando y el hotel donde se aloja ofrece Wi-Fi gratuita. ¿Está bien que use esa Wi-Fi para acceder al correo electrónico y a los archivos protegidos de su negocio?

a) No, conectarse a redes Wi-Fi gratuitas no seguras pueden exponer a su computadora a riesgos de seguridad innecesarios.

b) Sí, el hotel no ofrecería Wi-Fi gratuita si su uso no fuera seguro.

c) Sí, solo se conectará a la Wi-Fi durante un tiempo breve.

Comprobación de conocimientos n.° 4: Respuesta

Charlie, experto en seguridad cibernética de los CMS, pregunta…

Taylor está viajando y el hotel donde se aloja ofrece Wi-Fi gratuita. ¿Está bien que use esa Wi-Fi para acceder al correo electrónico y a los archivos protegidos de su negocio?

a) **No, conectarse a redes Wi-Fi gratuitas no seguras pueden exponer a su computadora a riesgos de seguridad innecesarios.**

b) Sí, el hotel no ofrecería Wi-Fi gratuita si su uso no fuera seguro.

c) Sí, solo se conectará a la Wi-Fi durante un tiempo breve.

Vulneraciones de seguridad cibernética

- Una vulneración es la pérdida de control, la puesta en riesgo, la divulgación no autorizada, la adquisición no autorizada o cualquier término similar referido a situaciones en que una persona que no sea un usuario autorizado acceda o tenga potencial acceso a PII, ya sea físico o electrónico, por cualquier motivo ajeno a un propósito autorizado.
- Las vulneraciones de seguridad cibernética son una amenaza creciente para los pequeños negocios.
- Los pequeños negocios son un blanco porque tienen información que los hackers desean y suelen carecer de la infraestructura de seguridad de los negocios más grandes.

Algunos ejemplos frecuentes de vulneraciones incluyen:

Cómo prevenir vulneraciones de seguridad cibernética

» Los agentes y corredores deben seguir estos pasos para prevenir vulneraciones de seguridad cibernética:

1

Identificar los tipos de información que su negocio accederá, procesará, almacenará o transmitirá.

2

Identifique el acceso de usuarios, la solidez de las contraseñas y los procedimientos de seguridad para todos los sistemas.

3

Después de evaluar riesgos potenciales, establezca límites que protejan PII y otra información sensible.

4

Implemente límites apropiados para su negocio.

Cómo responder a vulneraciones e incidentes

» Los agentes y corredores deben respetar fases de respuesta a vulneraciones e incidentes de seguridad y documentar cada paso hacia la resolución:

» Saber cómo responder durante un incidente

- Ayuda a resolver el problema con eficiencia.
- Minimice la pérdida de información.
- Minimizar la alteración de servicios o la vulneración de la seguridad.

Cómo denunciar vulneraciones de seguridad cibernética

- **Cuando esté en duda, denuncie. Todas vulneraciones y los incidentes potenciales y confirmados deben denunciarse a los CMS. Si no tiene certeza de si la situación es una vulneración, un incidente o nada en absoluto, lo mejor es denunciarla.**
- No espere a haber finalizado las investigaciones internas para denunciar una vulneración o un incidente.
- Tenemos en cuenta los esfuerzos de "buena fe" por denunciar un incidente en tiempo y forma, pero los plazos para denunciar están vigentes para garantizar la seguridad de los consumidores.

El Acuerdo de privacidad y seguridad de agentes/corredores con el Mercado Individual y el Programa de opciones de salud para pequeñas empresas (SHOP) de agentes/corredores exige lo siguiente:

- Denuncia de cualquier Vulneración de PII a la Mesa de servicios de TI de los CMS por teléfono al (410) 786-2580 o al 1-800-562-1963, o con una notificación por correo electrónico a CMS_IT_Service_Desk@cms.hhs.gov dentro de las 24 horas de tomar conocimiento de la Vulneración. Los Incidentes deben denunciarse a la Mesa de servicios de TI de los CMS por los mismos medios que las Vulneraciones dentro de las 72 horas de tomar conocimiento del Incidente. **Denunciar una vulneración o un incidente no es admitir un accionar indebido.**
- Si es un agente o corredor que usa sitios de socios de DE o EDE para sus inscripciones y cree que alguna otra persona ha usado o accedido a su cuenta, debe denunciar de inmediato el incidente a la Mesa de servicios de TI de los CMS y a la Mesa de ayuda para agentes/corredores del sitio web del socio de DE/EDE. Asegúrese además de cambiar sus contraseñas para iniciar sesión en su cuenta del Portal de Empresas de los CMS y de DE/EDE lo antes posible.

Reparación de incidentes de seguridad cibernética

- Al contactar a la Mesa de servicios de TI de los CMS por correo electrónico con respecto a una vulneración o un incidente de seguridad, la mejor práctica es presentar una Denuncia de incidente de seguridad (SIR). La plantillas para SIR se puede encontrar en:
  - https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-08-Incident-Response-Appendix-K-Incident-Report-Template
- Después de su denuncia:
  - El Equipo de gestión de incidentes (IMT) emitirá un número de incidente para el seguimiento.
  - El IMT elevará a los equipos apropiados que son responsables del seguimiento y la investigación.
  - Si tiene información adicional para proporcionar sobre su denuncia de incidente, puede hacer actualizaciones llamando o enviando un correo electrónico a la Mesa de servicios de TI de los CMS. Indique que está proporcionando una actualización y use el número de incidente que se emitió cuando hizo la denuncia original.

Cómo practicar higiene de seguridad cibernética

- Los agentes y corredores deben respetar medidas precautorias de “higiene de seguridad cibernética” para mantener seguros los datos sensibles de los clientes y protegerlos de robos y ataques.
- La higiene de seguridad cibernética es un conjunto de prácticas que deben realizarse periódicamente para mantener la seguridad de dispositivos y redes.
- ¿Qué puede hacer?
  - Obtenga más información sobre amenazas cibernéticas frecuentes.
  - Entienda dónde su negocio es vulnerable.
  - Tome medidas para mejorar su seguridad cibernética.
- Las prácticas de seguridad cibernética incluyen:

Cómo practicar higiene de seguridad cibernética (continuación)

- Las mejores prácticas de higiene seguridad cibernética también incluyen:
  - **Higiene de contraseñas:** Mantenga una buena higiene de contraseñas: al exigir contraseñas exclusivas, emplear gerentes de contraseñas, revisar la frecuencia de los ciclos de cambio de contraseñas y usar MFA cuando sea posible, para que a los hackers les resulte más difícil obtener acceso no autorizado.
  - **Administración de parches:** Siempre mantenga el software actualizado e instale parches de seguridad tanto en los dispositivos de la compañía como en los dispositivos personales usados para trabajar.
  - **Software de seguridad:** Instale software de seguridad para defender los sistemas contra software malicioso como cibersecuestro de datos, programas espía, gusanos, rootkits y troyanos. Además, haga escaneos periódicos para detectar actividad inusual.
  - Para más información sobre higiene de seguridad cibernética, consulte esta hoja de consejos.

Cómo practicar higiene de seguridad cibernética: Cifrado

- El cifrado es esencial porque suma una capa adicional de seguridad a la PII. Puede asegurar a sus clientes que está protegiendo su información y que sus archivos y datos estarán almacenados de forma segura en su dispositivo. Eso puede hacerse con las siguientes acciones:
  - Tener conocimiento de qué información está almacenada en sus dispositivos y de quiénes tienen acceso a ella.
  - Eliminar toda PII innecesaria de sus dispositivos.
  - Cifrar la PII que se conserva en sus dispositivos o se envía por correo electrónico, por una red inalámbrica o a través de Internet.
  - Usar cifrado cuando se usa acceso remoto en su dispositivo (p. ej. si una compañía soluciona problemas de su software de forma remota).
  - Sobrescribir los datos para que individuos no autorizados no puedan acceder a la información.

Cómo practicar higiene de seguridad cibernética: Cifrado (continuación)

- Mejores prácticas de cifrado:
  - Si es propietario de una agencia, capacite a sus empleados en el modo de cifrar correctamente datos sensibles en sus dispositivos.
  - Asegúrese de saber cómo cifrar los datos en sus dispositivos.
  - Asegúrese de que el cifrado esté correctamente configurado. De lo contrario, la información no estará protegida.
  - Tenga un plan en mente si el cifrado falla o hay fugas de PII.
- Para más información sobre cifrado, consulte esta hoja de consejos.

Software antivirus

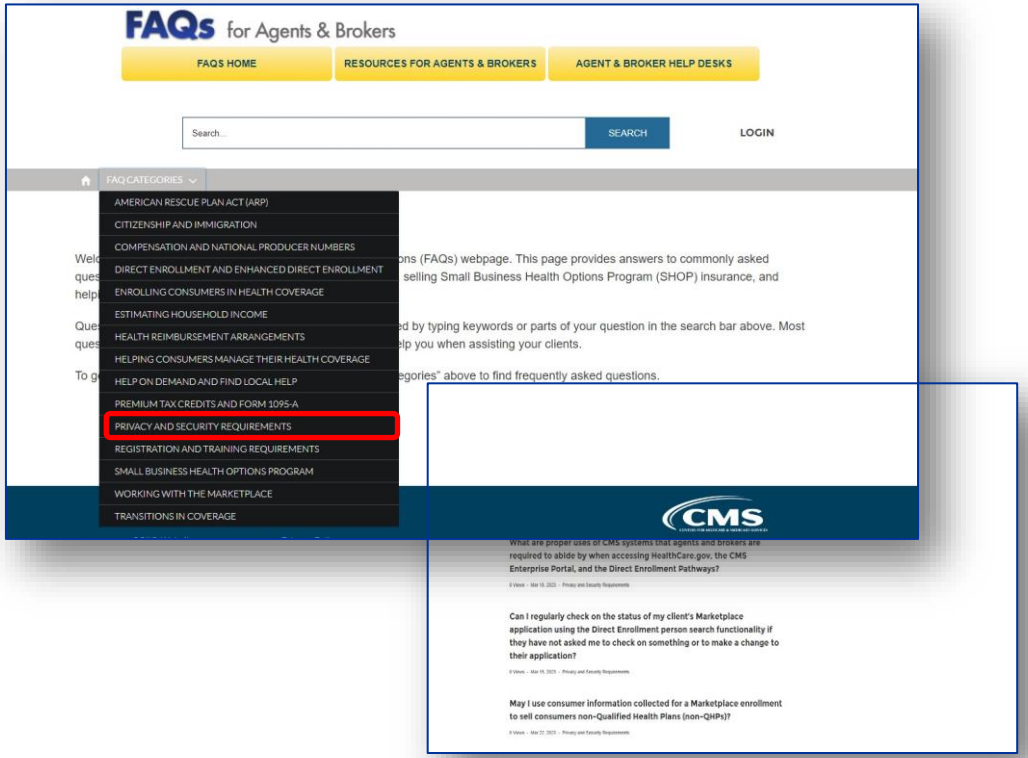
- El **software antivirus** escanea archivos o la memoria de su computadora en busca de ciertos patrones que pueden indicar la presencia de software malicioso (es decir, malware). El software antivirus (a veces mencionado más ampliamente como software antimalware) busca patrones con base en las firmas o definiciones de malware conocido.
  - Se considera una mejor práctica instalar un programa antivirus en su computadora que hará actualizaciones automáticas. Los programas con actualizaciones automáticas suelen tener un juego de herramientas que incluye un servicio de VPN. Sin embargo, incluso la implementación de una herramienta que generalmente está disponible a través de la compañía de su computadora sería mejor que no tener ninguna clase de programa antivirus. Consulte esta guía de la Cybersecurity & Infrastructure Security Agency (CISA) sobre comprender los software antivirus.
  - Si necesita asistencia adicional sobre este tema, comuníquese con la Mesa de ayuda por correo electrónico para agentes/corredores escribiendo a FFMProducer-AssisterHelpDesk@cms.hhs.gov.

Software antivirus (continuación)

- **¿Cómo responderá el software cuando encuentre malware?**
  - A veces, el software producirá un cuadro de diálogo que le alerte que ha encontrado malware y le pregunte si quiere que “limpie” el archivo (para eliminar el malware). En otros casos. el software puede intentar eliminar el malware sin preguntarle primero. Cuando seleccione un paquete antivirus, familiarícese con sus características para saber qué esperar.
- **¿Qué software debe usar?**
  - Hay muchos vendedores que producen software antivirus y decidir cuál elegir puede resultar confuso. El software antivirus habitualmente cumple los mismos tipos de funciones, de modo que su decisión puede impulsarse por recomendaciones, características particulares, disponibilidad o precio. Independientemente del paquete que elija, la instalación de cualquier software antivirus aumentará su nivel de protección.

Preguntas frecuentes sobre requisitos de privacidad y seguridad

- El sitio web de preguntas frecuentes de agentes y corredores incluye una categoría dedicada a Preguntas frecuentes sobre privacidad y seguridad.
  - Nota: Esta página de preguntas frecuentes se ha actualizado para incluir Preguntas frecuentes sobre requisitos de consentimiento del consumidor y revisión de solicitudes.
- Este recurso de autoservicio está disponible en línea y está vinculado en la página web de Recursos para agentes y corredores.



Recursos sobre seguridad cibernética

- El sitio web del Grupo de Seguridad y Privacidad de la Información (ISPG) de los CMS proporciona información adicional sobre el modo en que los CMS llevan a cabo la seguridad cibernética.
- CISA's Cyber Essentials sirve de guía para que las pequeñas empresas desarrollen una comprensión de dónde comenzar a implementar prácticas de seguridad cibernética.
- La Administración de Pequeñas Empresas ofrece sesiones gratuitas de capacitación en seguridad cibernética. Inscríbase para sus capacitaciones aquí.
- La Comisión Federal de Comercio tiene una lista de videos sobre temas como fundamentos de seguridad cibernética, cibersecuestro de datos y mucho más. Haga clic aquí para acceder a esos videos y ver contenido adicional sobre seguridad cibernética para pequeñas empresas.
- La National Cybersecurity Alliance también ofrece eventos virtuales y presenciales sobre seguridad cibernética para ayudar a propietarios de pequeñas empresas a informarse sobre seguridad cibernética y cómo mantenerse seguros.
- Para más información sobre mantener la conformidad en el Mercado, vea las diapositivas del webinario Marketplace Compliance y las diapositivas del webinario Agent/Broker Summit: Marketplace Compliance and Agent/Broker Regulations.