SEMINARIO WEB

¡La protección de los datos es responsabilidad de todos!

Haga su parte para proteger la información de su proyecto de planificación familiar.

El Centro Nacional de Capacitación sobre Salud Reproductiva (Reproductive Health National Training Center, RHNTC) presentó un seminario web llamado La protección de los datos es responsabilidad de todos el 23 de febrero de 2021. La siguiente información contiene los objetivos, las definiciones clave, los riesgos de la protección de los datos, las medidas que pueden adoptarse para minimizar los riesgos y los recursos desarrollados durante los 60 minutos del seminario web. Puede acceder a los materiales archivados del seminario web en rhntc.org.

A medida que la tecnología, los lugares de trabajo y los servicios de planificación familiar y datos relacionados siguen evolucionando, la protección de la información de los clientes y la organización se vuelve esencial. Los trabajadores de planificación familiar pueden adoptar medidas para protegerse a ellos mismos, sus organizaciones y, los datos sensibles de las amenazas a la ciberseguridad. **La protección de los datos es responsabilidad de todos.**

Objetivos del seminario web

Al finalizar el seminario web, los participantes podrán hacer lo siguiente:

- Describir la importancia de las medidas que deben adoptar los trabajadores de planificación familiar para protegerse de las amenazas a la ciberseguridad.
- Describir una o más medidas que una persona puede adoptar para proteger todos tipos de datos de la organización (ya sean almacenados o compartidos).
- Identificar uno o más recursos que pueden ser útiles para abordar necesidades adicionales de protección de datos.

Definiciones clave:

- **Protección de datos:** Adoptar medidas para proteger la información electrónica almacenada en su computadora, dispositivo, red y otras cuentas. La protección de datos incluye las acciones y los procesos que adopta cada persona a fin de proteger la información privada.
- **Dispositivo:** Una computadora, ya sea portátil, de escritorio, PC o Mac; un teléfono inteligente u otros artefactos que realizan actividades de manera electrónica (p. ej., televisores inteligentes, cafeteras o aspiradoras).
- **Sistema operativo:** Gestiona todo el software y hardware de un dispositivo y se encarga de la coordinación para garantizar que cada programa ejecutado en el dispositivo obtenga lo que necesita (p. ej., Windows).
- **Navegador:** La aplicación de software del dispositivo que se utiliza para acceder a Internet (p. ej., Chrome, Safari, Firefox o Edge).
- **Red:** Todos los dispositivos conectados a través de un nodo central. Esto puede incluir redes de área local en las que múltiples dispositivos pueden acceder unos a otros, generalmente a través de cables wifi o Ethernet.

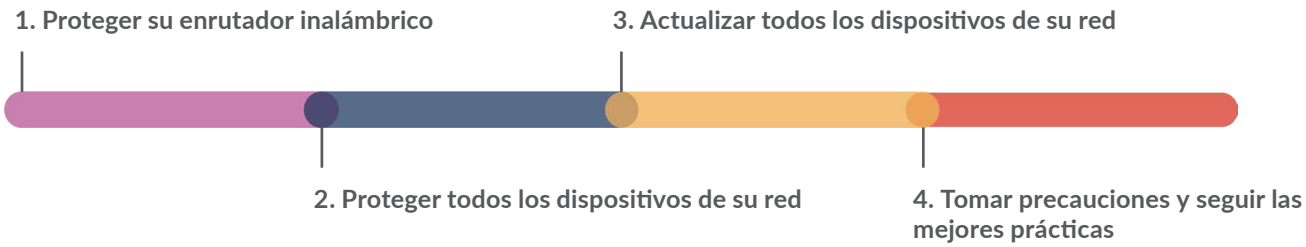
Importancia de la protección de datos

- Las personas trabajan cada vez más desde ubicaciones no tradicionales (como sus hogares o espacios públicos), lo que aumenta la vulnerabilidad y el riesgo de exposición de los datos.
- La recopilación y el uso compartido de datos son cada vez más detallados.
- Independientemente de los mecanismos de recopilación de datos (p. ej., historia clínica electrónica, base de datos, etc.), la necesidad de seguridad para el almacenamiento y el uso compartido prevalece.

Riesgos

- **Ransomware:** un tipo de programa maligno que toma el control de una computadora o un sistema informático al cifrar todos los datos del disco. Luego, se pide un rescate por los datos hasta que se pague un costo predeterminado.
- **Los ransomware pueden transmitirse de las siguientes formas:**
  - Mensajes de correo electrónico que fingen ser negocios legítimos o enlaces atractivos;
  - Troyanos que actúan como solicitudes de actualización;
  - Revisiones o actualizaciones de programas antivirus;
  - Actualizaciones falsas del sistema;
  - Notificaciones falsas sobre la presencia de virus;
  - Aprovechamiento de las vulnerabilidades conocidas de la red o el software de seguridad.
- **Los programas malignos** también pueden provocar el robo de datos e información sensible sin dejar señales de lo ocurrido. Luego, la información sensible puede develarse o venderse.

Medidas que pueden adoptarse para proteger los datos



1. **Proteger su enrutador inalámbrico.** Asegúrese de que el software del enrutador esté actualizado y se haya cambiado la contraseña. Asegúrese de que el tipo de seguridad establecido sea el cifrado de datos WPA2.
2. **Proteger todos los dispositivos de su red.** Incluya los dispositivos de trabajo y cualquier dispositivo personal de su red. Cambie las contraseñas por lo menos cada 90 días y utilice contraseñas más largas. Si su organización posee una red privada virtual (virtual private network, VPN), utilícela en su dispositivo de trabajo para obtener una protección mas fuerte. De lo contrario, considere utilizar su propia VPN. Conozca el proceso de respaldo de datos de su organización.
3. **Actualizar todos los dispositivos de su red.** Asegúrese de incluir lo siguiente: navegadores de Internet, sistemas operativos de las computadoras (p. ej., Windows, Mac), sistemas operativos de los teléfonos inteligentes y otros dispositivos inteligentes.
4. **Tomar precauciones y seguir las mejores prácticas.** Los ataques de phishing consisten en enviar comunicaciones fraudulentas que aparentan proceder de una fuente confiable.
   - Intente no hacer clic en los enlaces incluidos dentro de los mensajes. En su lugar, diríjase al sitio o a la cuenta e inicie sesión. Confirme la información allí.
   - Llame o confirme con el remitente antes de hacer clic en los enlaces de los mensajes.
   - Observe si el mensaje concuerda con las comunicaciones recibidas del remitente con anterioridad.

   Tome buenas decisiones informáticas:
   - Utilice una conexión segura y cifrada como una VPN al comunicar datos clínicos o de clientes, o al acceder a estos.
   - Asegúrese de que los dispositivos de trabajo estén protegidos todo el tiempo.
   - No utilice una cuenta de correo electrónico personal para enviar o recibir mensajes de la compañía, no reenvíe mensajes de trabajo a cuentas personales, no envíe o comparta datos a través de herramientas personales para uso compartido de archivos, ni trate asuntos organizacionales a través de redes sociales.

   Actualice la contraseña de su red y luego confirme con las personas a su alrededor que sus dispositivos y sistemas estén actualizados antes de compartir la nueva contraseña de la red.

¡Hay mucho más que hacer!

- **Elabore políticas y procedimientos sólidos de seguridad y privacidad de la organización.**
- **Asegúrese de cumplir con los requisitos reglamentarios como la Ley de Portabilidad y Responsabilidad de Seguros Médicos (Health Insurance Portability and Accountability Act, HIPAA).**
- **Cuente con un plan de respuesta ante incidentes.**
- **Formación y apoyo continuos.**

Recursos

- Ransomware Guide: Best Practices and Response Checklist
- Ransomware: What It Is and What to Do About It
- Confronting Heightened Cybersecurity Threats Amid COVID-19
- How to Secure Your Home Wireless Network
- Cybersecurity Checklist for Staff Working Remotely
- Avoiding Social Engineering and Phishing Attacks
- Don't Wake Up to a Ransomware Attack

Esta publicación fue apoyada por la Oficina de Asuntos de Población (OPA, por sus siglas en inglés) (subvencion FPTPA006030). Las opiniones expresadas no reflejan necesariamente las políticas oficiales del Departamento de Salud y Servicios Humanos, y el hecho de mencionar nombres comerciales, prácticas comerciales, u organizaciones no implica el respaldo por parte del Gobierno de los Estados Unidos.