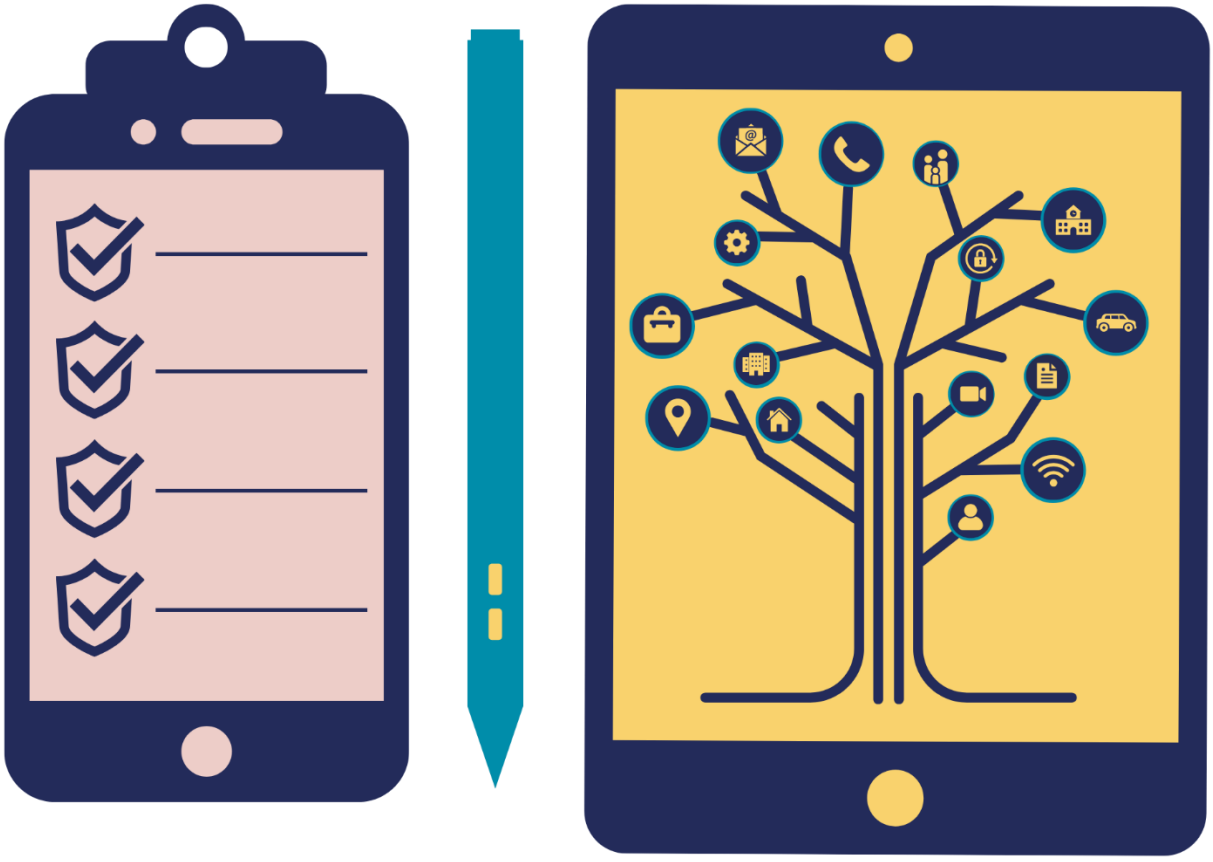
Lista de Verificación para la Planeación de Seguridad Tecnológica



La planeación de la seguridad tecnológica debe realizarse siempre junto con una planeación de seguridad más tradicional. La violencia en línea y la violencia fuera de línea están interconectadas y es importante tener en cuenta los riesgos no relacionados con la tecnología que pueden estar asociados a la planeación de seguridad tecnológica. Esta lista de verificación

para la planeación de seguridad tecnológica está pensada como complemento de un plan de seguridad más amplio y no como una lista de verificación independiente.

Siempre que planees la seguridad de una persona que ha sufrido violencia facilitada por la tecnología, es importante tener en cuenta que el agresor puede tener acceso a sus dispositivos o cuentas y puede estar vigilando sus comunicaciones y movimientos a través de estos dispositivos y cuentas. Hacer cambios en cualquier dispositivo, cuenta de redes sociales, correo electrónico u otra tecnología puede alertar al agresor de que tu cliente está buscando ayuda y puede desencadenar abusos adicionales. En estas situaciones puede ser necesario tomar precauciones adicionales de planeación de la seguridad.

En algunos casos, es posible que necesites la ayuda de un especialista en informática o de la policía, como cuando se trata de detectar programas de acoso u otros programas espía.

Contraseñas

- ☐ Hacer una lista de todos los dispositivos (por ejemplo, laptop, teléfono móvil, Fitbit, AirTags, sistema de seguridad doméstico, auto inteligente, dispositivos conectados a Internet, Siri/Alexa, sistemas de sonido conectados por Bluetooth, etc.) y cuentas (por ejemplo, redes sociales, correo electrónico, compras en línea, servicios de comida en línea, aplicaciones de transporte, cuentas en la nube, monitores de ejercicio, juegos, etc.). En el Apéndice A se encuentra una lista de posibles cuentas.

- ☐ Tomar nota de cuáles de estos dispositivos el agresor tiene acceso, conoce las contraseñas o puede conocerlas.

- ☐ Repasar qué información se incluye en esas cuentas (por ejemplo, domicilio, número de teléfono, dirección de correo electrónico, información sobre tarjetas de crédito, mensajes personales, historial de búsquedas en Internet, comunicaciones sobre planes de seguridad, etc.).

- ☐ Cambiar todas las contraseñas por frases de contraseña únicas que el agresor no pueda adivinar. Evitar utilizar los nombres de los niños o mascotas, fechas importantes, direcciones o números de teléfono antiguos. Una frase de contraseña es una frase fácil de recordar pero que no sería fácil de adivinar. Añadir símbolos de números en lugar de letras puede hacerla aún más difícil de adivinar (por ejemplo, L1tTl3R3dC0rV3Tt3).

- ☐ No utilizar la misma contraseña para varias cuentas.

- ☐ Utilizar una frase de contraseña única para cada cuenta o utilizar un administrador de contraseñas.

- ☐ Cambiar la contraseña del Wi-Fi de la casa.

- ☐ Para las preguntas de seguridad de las cuentas, inventar respuestas falsas o no utilizar preguntas que el agresor pueda adivinar; de lo contrario, podría acceder a la cuenta (por ejemplo, en lugar de utilizar el apellido de soltera de tu madre, inventa una respuesta cuando te pregunten el apellido de soltera de tu madre y contesta con algo diferente. Asegúrate de recordar la respuesta falsa).

- ☐ Desactivar todas las contraseñas guardadas automáticamente en todos los dispositivos y cuentas.

- ☐ Cerrar sesión en todas las cuentas y dispositivos cuando no se utilicen.

- ☐ Utilizar la autenticación de dos pasos en cualquier aplicación o cuenta que lo permita. La autenticación de dos pasos requiere que se introduzca una contraseña que se envía al teléfono o correo electrónico para confirmar que eres tú quien accede a la cuenta.

    - Para obtener información general sobre la autenticación de dos pasos, consulte HackBlossom.

    - Utiliza este sitio web para ver qué aplicaciones comunes utilizan la autenticación de dos pasos.

- ☐ No utilizar cuentas de redes sociales para iniciar sesión en otras cuentas (por ejemplo, las opciones "Iniciar sesión con Facebook" o "Iniciar sesión con Google").

- ☐ Eliminar las direcciones de correo electrónico o los dispositivos del agresor de las cuentas compartidas y como Dispositivos de Confianza en tus cuentas.

Bloquear, borrar y cancelar la amistad

- ☐ Considerar bloquear o eliminar de tu lista de amigos la dirección de correo electrónico, el número de teléfono o el contacto en redes sociales del agresor. Asegúrate de haber reunido toda la evidencia necesaria de esas cuentas antes de hacerlo. Algunos programas eliminarán o no te permitirán acceder a las conversaciones e

información de la cuenta de la otra persona una vez que haya sido eliminada, bloqueada o borrada de tu cuenta.

- ☐ Cuando se decide bloquear, borrar o eliminar la amistad de alguien, se debe tener en cuenta si esto puede agravar el abuso. Tener acceso a las redes sociales del agresor puede ser beneficioso (por ejemplo, conocer su ubicación) y merece la pena tenerlo en cuenta.

- ☐ Considerar cuáles de tus amigos y familiares pueden tener a tu agresor como "amigo" en sus cuentas. Solicita a tus amigos y familiares que no publiquen información sobre ti o fotos tuyas en Internet y que no compartan información con el agresor.

Acecho, rastreo y vigilancia

- ☐ Cubrir las cámaras de todos los dispositivos cuando no se estén utilizando.

- ☐ Si el agresor está rastreando tu dispositivo o tus cuentas, considera la posibilidad de utilizar un dispositivo diferente (por ejemplo, la computadora de un amigo, un dispositivo del trabajo o una computadora en una biblioteca) para buscar información y empezar a planear cómo hacer cambios en tus dispositivos o cuentas.

- ☐ Considerar qué información personal se publica en Internet (por ejemplo, la dirección de casa en una invitación a un cumpleaños, el número de teléfono en una publicación de Facebook o un nuevo lugar de trabajo en LinkedIn) y decide si quieres borrar esa información o hacerla privada. Recuerda que otras personas podrían compartir esa

información con tu agresor, aunque les hayas bloqueado de tus cuentas.

- ☐ Desactivar o limitar las funciones de localización de los dispositivos cuando no se utilicen.

- ☐ Desactivar funciones de localización como Buscar mi Teléfono o Buscar a mis Amigos.

- ☐ Borrar el historial de ubicaciones almacenado previamente, especialmente antes y después de llegar a refugios para víctimas de violencia doméstica u otros espacios seguros.

- ☐ No "hacer check-in" en lugares en las redes sociales.

- ☐ Cambiar la configuración de privacidad de las aplicaciones y redes sociales a una configuración más privada.

- ☐ No publicar fotos en las redes sociales que contengan metadatos o información de fondo que puedan alertar al usuario sobre tu ubicación. Una forma de eliminar los metadatos basados en la ubicación de una foto es hacer una captura de pantalla de la foto y publicar la captura de pantalla en lugar de la foto original que contiene los metadatos.

- ☐ Eliminar las direcciones de correo electrónico o los dispositivos del agresor de las cuentas compartidas y eliminar su dispositivo de los Dispositivos de Confianza de todas tus cuentas. Consulta el Apéndice A para ver posibles cuentas.

- ☐ Comprobar la Última Actividad de la Cuenta o la Actividad de la Cuenta para ver si alguna dirección IP inusual está accediendo a la cuenta.

- ☐ Si existe alguna preocupación de que el agresor tenga acceso a tus cuentas, considerar la posibilidad de utilizar un apartado de correos como dirección para las cuentas y entregas en línea. Considerar el riesgo de que el agresor acceda a la información de la tarjeta de crédito o haga un uso indebido de la cuenta si tiene acceso.

- ☐ Desvincule el teléfono u otros dispositivos de los del agresor (por ejemplo, el estéreo Bluetooth del coche o casa, las notificaciones de ejercicio del reloj inteligente, etc.).

- ☐ Registrar las pertenencias (por ejemplo, bolsos, coches, chamarras) en busca de dispositivos de localización GPS u otros dispositivos de grabación.

- ☐ Examinar cualquier regalo o artículo inusual en el hogar, incluidos los artículos de los niños, en busca de cámaras ocultas o dispositivos de grabación.

- ☐ Considerar qué información hay en los dispositivos y cuentas de sus hijos (por ejemplo, teléfonos, sistemas de videojuegos, cuentas de redes sociales) y qué puede estar compartido con el agresor.

- ☐ Considerar si el agresor tiene acceso a cualquier información del sistema de seguridad del hogar, como el acceso a las cámaras o la información cuando la gente sale o entra en la casa.

- ☐ Considerar el uso de un dispositivo o programa (por ejemplo, escáneres de red, escáneres de puertos, detectores de señales de radiofrecuencia) que pueda detectar ciertas cámaras ocultas para escanear tu Wi-Fi o tu casa.

- ☐ Revisar las aplicaciones del teléfono y eliminar las que no le resulten familiares.

- ☐ Si existe la preocupación de que el agresor pueda haber instalado software espía en tus dispositivos, puedes pedir a un especialista en informática o a la policía que comprueben si el dispositivo contiene este tipo de programas. Recuerde que, si el software espía está instalado en el dispositivo, el agresor puede ser capaz de ver lo que se hace en el dispositivo, lo que puede intensificar el abuso.

    - La Clínica para Poner Fin al Abuso Tecnológico también dispone de recursos para ayudar a identificar programas espía en un dispositivo.

    - Señales de que un dispositivo puede tener programas espía:

        - El dispositivo funciona lentamente.
        - La batería se descarga rápidamente.
        - Se agotan los datos.
        - El dispositivo se calienta.
        - El dispositivo se ilumina cuando no está en uso.
        - Clics o sonidos extraños durante las llamadas.
        - Tarda mucho en apagarse.

- ☐ Mantener actualizados los sistemas operativos de los dispositivos. Estas actualizaciones suelen corregir cualquier vulnerabilidad de seguridad encontrada en el software que los piratas informáticos podrían utilizar indebidamente y los programas espía. Comprueba dos veces la configuración de privacidad después de una actualización para asegurarte de que ésta no ha cambiado para ninguna aplicación.

- ☐ Considerar reemplazar completamente los dispositivos. Si decides hacerlo, no debes realizar copias de seguridad de los dispositivos anteriores. Esto podría transferir cualquier programa espía instalado en el dispositivo anterior.

- ☐ Buscar hardware inusual conectado a computadoras de escritorio (por ejemplo, los registradores de teclas suelen estar conectados entre el teclado y CPU de la computadora).

- ☐ Es importante tener en cuenta que los hackers e ingenieros informáticos experimentados pueden acceder a la ubicación de un dispositivo, incluso cuando está apagado en la configuración. Si tu agresor tiene experiencia en TI, puede haber retos adicionales para la seguridad tecnológica dependiendo de sus conocimientos. Si este es el caso, es posible que desees hablar con un especialista en TI o con las autoridades.

Cuentas alternas

- ☐ Si el agresor tiene acceso a tus cuentas y no hay forma segura de impedirlo en este momento (por ejemplo, si te exige que compartas tus contraseñas amenazándote con hacerte daño de otra forma), y para comunicaciones sensibles, crea una cuenta de correo electrónico alternativa o una cuenta de redes sociales que el agresor no conozca o a la que no tenga acceso.

- ☐ No inicies sesión en esta cuenta en tus dispositivos personales o compartidos. Utiliza una computadora del trabajo, de la biblioteca o de un amigo para acceder a ella.

Almacenamiento en la nube, cuentas compartidas, acceso no autorizado

- ☐ Eliminar al agresor de cualquier cuenta, dispositivo o plan compartido si es seguro hacerlo.

- ☐ Eliminar las conexiones Bluetooth de los dispositivos del agresor (por ejemplo, los que estén conectados al equipo de música de casa, al coche, etc.).

- ☐ Considerar qué contenido se está cargando o conectando automáticamente (por ejemplo, calendarios, almacenamiento iCloud para fotos y mensajes de texto, Fitbit, relojes inteligentes) y si el agresor pudiera obtener acceso a estas cuentas o información.

- ☐ Eliminar todos los dispositivos, excepto los tuyos, de los Dispositivos de Confianza de todas las cuentas.

- ☐ Comprobar la Última Actividad de la Cuenta en todas las cuentas para ver si una dirección IP o un dispositivo inusual ha estado accediendo a la cuenta.

Historial de búsqueda

- ☐ Si el agresor tiene acceso al dispositivo o a la cuenta, puede comprobar tu historial de búsqueda.

- ☐ Si buscas ayuda o recursos, utiliza una computadora que no esté en casa (por ejemplo, una computadora pública, la de un amigo o del trabajo).

- ☐ Eliminar selectivamente el historial de búsquedas en Internet.
- ☐ Utilizar las opciones "privado" o "incógnito" para que no se registre el historial de búsqueda.
- ☐ Desactivar las cookies en la configuración del navegador.

Imágenes íntimas o “Pornovenganza”

- ☐ Hacer una lista de las imágenes y videos que puedan existir.
- ☐ Considerar utilizar el programa de Facebook que impide que otras personas suban imágenes sexuales que hayan sido registradas y "hasheadas" (número Hash) con la empresa. Sin embargo, tendrías que enviar esas fotos a Facebook para que el programa pueda reconocer y eliminar las imágenes de Facebook e Instagram.
- ☐ Si se puede hacer sin peligro, pide a tus exparejas que borren cualquier imagen íntima una vez finalizada la relación y diles que no hay consentimiento para compartirlas. Documenta esta comunicación.
- ☐ Considerar si el agresor pudo haber capturado imágenes sin consentimiento (por ejemplo, cámara oculta, captura de pantalla de relaciones sexuales a través de Zoom o Skype).
- ☐ Hacer una búsqueda inversa de imágenes en Google.
- ☐ Buscar tu nombre en sitios de pornografía habituales. A menudo se publican datos personales de forma malintencionada *(doxing)* y nombran a personas cuando se comparten sus imágenes.

- ☐ Configurar una alerta de Google para tu nombre, ya que esto puede ayudar a alertarte cuando tu nombre se menciona en línea si se publica junto con tus imágenes.

- ☐ Considerar la posibilidad de alertar a familiares, amigos y compañeros de trabajo que puedan recibir las imágenes para reducir el daño.

- ☐ Si la imagen se ha compartido sin consentimiento, consulta la guía de la Iniciativa de Derechos Civiles en el Ciberespacio para que se retiren contenidos de Internet.

- ☐ Informar a las empresas de redes sociales o de pornografía, ya que la mayoría tienen políticas que prohíben compartir imágenes de desnudos sin consentimiento.

- ☐ Si se comparten imágenes íntimas, considera estrategias de reducción de daños:

    - Evitar imágenes con tu cara o marcas identificativas (por ejemplo, tatuajes, marcas de nacimiento).
    - Evitar imágenes en lugares que sean identificables (por ejemplo, una habitación reconocible).
    - Utilizar programas como Signal que permiten hacer desaparecer los mensajes.

- ☐ Si se han difundido imágenes, considerar la posibilidad de utilizar un servicio de reputación para ayudar a eliminar el contenido.

Alertas de Google

- ☐ Establecer una alerta de Google para tu nombre, de modo que recibas una notificación cuando tu nombre aparezca en Internet. Esto no encontrará todos los lugares donde aparece tu nombre, pero puede alertarte de algunos casos.

- ☐ Crear una alerta de Google para todas las versiones de tu nombre (por ejemplo, Victoria Chan, Vickie Chan, Vicky Chan).

Reportar contenido perjudicial a empresas de redes sociales

- ☐ Reunir evidencia (por ejemplo, capturas de pantalla) del contenido perjudicial antes de denunciarlo, ya que la empresa de redes sociales puede eliminarlo si infringe sus políticas.

- ☐ Consultar las Guías de Seguridad de Medios de HeartMob para obtener consejos sobre las políticas y los mecanismos de denuncia de las empresas de redes sociales.

Actualizaciones de software, cortafuegos *(firewalls)* y antivirus

- ☐ Actualizar regularmente el software. Esto incluye los teléfonos móviles. Estas actualizaciones suelen corregir cualquier vulnerabilidad de seguridad encontrada en el software que los hackers podrían utilizar indebidamente.

- ☐ Habilitar el firewall y antivirus en todos los dispositivos.

Recopilación de evidencia

- ☐ Crear un registro de todas las experiencias de violencia facilitada por la tecnología e incluir información como hora, fecha, agresor, evidencia recopilada y otra información útil. Consulta el Registro de Violencia Facilitada por la Tecnología de muestra de WSC aquí.

- ☐ Hacer capturas de pantalla o grabar el abuso.

- ☐ Considerar si la aplicación alerta a la otra persona si alguien hace una captura de pantalla. Si lo hace, puede que no sea seguro hacer una captura de pantalla y que sea mejor hacer una foto o un video con un segundo dispositivo.

- ☐ Asegurarse de incluir en la evidencia el perfil y otros datos identificativos del agresor.

- ☐ Asegurarse de que se muestre la fecha del abuso.

- ☐ Si el abuso se produce por correo electrónico, conservar el correo original, ya que contiene metadatos como la dirección IP del remitente.

- ☐ Si el abuso fue publicado por otra persona, hacer una captura de pantalla antes de que tengan la oportunidad de borrarlo.

- ☐ Guardar copias de la evidencia en un lugar seguro. Haz copias de seguridad de la información en un dispositivo adicional por lo menos.

- ☐ Si el agresor tiene acceso al dispositivo o al almacenamiento en la nube donde se guarda la evidencia, podría borrarlas.

- ☐ Conservar copias impresas y electrónicas de la evidencia.

La Violencia de Género Facilitada por la Tecnología (VGFT) es parte de un continuo de violencia que puede ocurrir tanto en línea como en persona. Si tú o alguien que conoces está experimentando VGFT, no están solos. Pueden utilizar sheltersafe.ca para encontrar un refugio o casa de transición cerca de ti o llamar / enviar mensaje de texto al Teléfono de Ayuda para Niños para hablar sobre las opciones y crear un plan de seguridad. No es necesario permanecer en un refugio para acceder a servicios y apoyo gratuitos y confidenciales.

Agradecemos sinceramente a Suzie Dunn, estudiante de doctorado en la Universidad de Ottawa, por la creación de esta hoja informativa.

Adaptado del proyecto Technology Safety de BCSTH, basado en su recurso Lista de Verificación para la Planeación de Seguridad Tecnológica.

APÉNDICE A:

Dispositivos y Cuentas para Considerar

Cuentas de Redes Sociales

- ☐ Facebook
- ☐ Twitter
- ☐ Instagram
- ☐ Snapchat
- ☐ TikTok
- ☐ Pinterest
- ☐ WeChat
- ☐ YouTube
- ☐ Tumblr
- ☐ Reddit
- ☐ LinkedIn

Comunicación

- ☐ Teléfono inteligente
- ☐ Computadora
- ☐ Gmail
- ☐ Correo electrónico personal y de trabajo
- ☐ Messenger
- ☐ WhatsApp
- ☐ Signal
- ☐ Slack
- ☐ QQ
- ☐ Viber
- ☐ Telegram
- ☐ Mensajes Instantáneos, Directos (MD), o Privados en plataformas en línea

Video Conferencias

- ☐ Zoom
- ☐ MS Teams
- ☐ Skype
- ☐ FaceTime
- ☐ Video llamadas en plataformas en línea

Almacenamiento en la nube

- ☐ iCloud
- ☐ Dropbox
- ☐ Google Drive
- ☐ Amazon Drive

Cuidado de niños y mascotas

- ☐ Calendarios compartidos
- ☐ Aplicaciones de rastreo de menores
- ☐ Monitor para bebés
- ☐ Compartir fotos
- ☐ Aplicaciones de programación
- ☐ Cámara para animales
- ☐ Rastreador de animales (ej. Dispositivo GPS en el collar)

Finanzas

- ☐ Cuentas bancarias (incluidas tarjetas de crédito)
- ☐ Cuentas de inversión (ej. Acciones, inversiones, jubilación, educación, etc.)
- ☐ PayPal
- ☐ Apple wallet
- ☐ Bitcoin Wallet
- ☐ OXF

Facturas y servicios

- ☐ Planes de telefonía
- ☐ Electricidad
- ☐ Gas
- ☐ Internet/Cable

Cuentas gubernamentales

- ☐ Agencia Tributaria
- ☐ Aplicaciones para reservar citas
- ☐ Cuenta de préstamo estudiantil

- ☐ My Account (CRA)
- ☐ Cuenta de servicios provinciales

Servicios de entrega de

- ☐ SkipTheDishes
- ☐ Uber Eats
- ☐ DoorDash
- ☐ Foodora
- ☐ Otras cuentas de restaurantes

Aplicaciones de

- ☐ Uber
- ☐ Lyft
- ☐ Aplicaciones de Taxis
- ☐ Waze
- ☐ Google maps
- ☐ Aplicaciones de transporte público

Aplicaciones de compras

- ☐ Amazon
- ☐ Tarjeta de puntos de supermercado
- ☐ PC Optimum
- ☐ Tarjeta de puntos para compra de café
- ☐ Aplicaciones Inmobiliarias
- ☐ Aplicaciones de cuentas/recompensas de tiendas en las que compra o en línea

Entretenimiento

- ☐ Spotify
- ☐ Netflix
- ☐ Crave
- ☐ Disney+
- ☐ Amazon Prime Video
- ☐ Apple Music and TV
- ☐ iTunes
- ☐ Aplicaciones de Podcast
- ☐ Audible
- ☐ PornHub

Videojuegos

- ☐ Discord
- ☐ Twitch

Salud y bienestar

- ☐ Fitbit
- ☐ Apple Watch

- ☐ Switch
- ☐ Steam
- ☐ Xbox Live
- ☐ Red de PlayStation
- ☐ Origin
- ☐ Juegos para teléfono inteligente
- ☐ Monitoreo de distancia (ej. Strava, MapMyRun)
- ☐ Dispositivos GPS (ej. Garmin, aplicaciones de senderismo)
- ☐ Aplicaciones de periodo o fertilidad
- ☐ De dieta o contadores de calorías
- ☐ Aplicaciones de monitoreo médico
- ☐ Aplicaciones de terapia

Viaje

- ☐ Tarjetas de puntos de viajes (ej. Aeroplan, Air Miles)
- ☐ Airbnb
- ☐ Expedia
- ☐ TripAdvisor
- ☐ HostelInternational
- ☐ Aerolíneas
- ☐ Trenes

Dispositivos inteligentes del hogar

- ☐ Amazon Echo
- ☐ Google Nest
- ☐ Alexa
- ☐ Siri
- ☐ Sonos One
- ☐ The Ring
- ☐ Sistemas de seguridad para el hogar
- ☐ Termostato inteligente
- ☐ Iluminación inteligente
- ☐ Chapa o cerradura inteligente

Dispositivos inteligentes portátiles

- ☐ Auto inteligente
- ☐ GPS en el auto
- ☐ Bluetooth en el auto
- ☐ Aplicación de rastreo para bicicleta
- ☐ Tiles
- ☐ Find my phone / Encuentra mi teléfono

Cuentas de educación y aprendizaje

- ☐ Correo electrónico del colegio
- ☐ Plataforma de tareas escolares en línea
- ☐ Tarjeta de la biblioteca
- ☐ Aplicaciones de idiomas