Ciberseguridad

Para psicologxs

Conceptos, herramientas y recomendaciones

Tatiana X. Stacul

INDICE

Antes de Integrar Herramientas Digitales: Un Enfoque Consciente

Es muy probable que ya estés utilizando herramientas digitales en la práctica profesional, incluso sin haber considerado en profundidad los riesgos asociados a la privacidad. No estas solo: en un contexto de digitalización acelerada, el uso de plataformas tecnológicas en psicología y en muchas profesiones se ha vuelto prácticamente inevitable.

Frente a este escenario, es fundamental que la incorporación de tecnologías se realice con criterio clínico, mirada ética y foco en la **ciberseguridad**. No se trata solo de adaptarnos a lo nuevo, sino de hacerlo con responsabilidad profesional.

A continuación, Te presento **conceptos claves** que fui aprendiendo en mis estudios en este campo, que conviene tener claros antes de aceptar términos y condiciones, para que puedas reflexionar antes de responder "si" al primer servicio de software que promete optimizar tu práctica y alojar tus datos.

Luego de esto, se analizarán en detalle algunas de las **herramientas más utilizadas** en la práctica cotidiana, con consejos prácticos y se finalizará con **consideraciones sobre el uso de la IA** (Qué es importante saber de la misma como aproximación inicial.)

Es legítimo querer estar al día, explorar aplicaciones funcionales y elegir plataformas amigables, pero no alcanza con que algo sea "bonito", "fácil de usar" o que prometa privacidad sin explicar cómo. Es tiempo de hacerse las preguntas necesarias y perder el miedo a lo inexplorado.

Espero esta guía sirva y si tienes dudas, quieres comentar o sugerir modificaciones podemos conectar, seamos parte de un mundo ciberseguro!

LinkedIn

Entre el Yo, el Entorno y la Nube: Conocer las Herramientas, proteger la práctica

Como profesionales de la psicología, el coaching y la salud en general, estamos formados para comprender y acompañar la relación entre el mundo interno y el contexto social. Sin embargo, en el escenario actual, resulta imprescindible integrar un **tercer entorno estructurante**: el espacio digital.

No se trata solo de herramientas tecnológicas. Hablamos de un **ecosistema dinámico y complejo**, donde circulan datos sensibles, se construyen vínculos terapéuticos mediados por pantallas y se alojan decisiones clínicas que exigen el mismo nivel de resguardo ético y profesional que el consultorio presencial.

La ciberseguridad puede parecer un terreno ajeno, técnico o difícil de abordar. Pero lo cierto es que ya forma parte de nuestra práctica cotidiana. Desde una videollamada terapéutica hasta la plataforma donde gestionamos turnos o almacenamos historiales, cada decisión tecnológica implica **gestionar confianza, proteger la privacidad y garantizar derechos**.

Objetivo

Este recurso está pensado para **acompañar diferentes puntos de partida:** quienes recién comienzan a integrar lo digital, quienes enfrentan barreras económicas para acceder a herramientas especializadas, y también quienes ya trabajan con solvencia online y buscan revisar sus decisiones tecnológicas desde una mirada crítica y profesional.

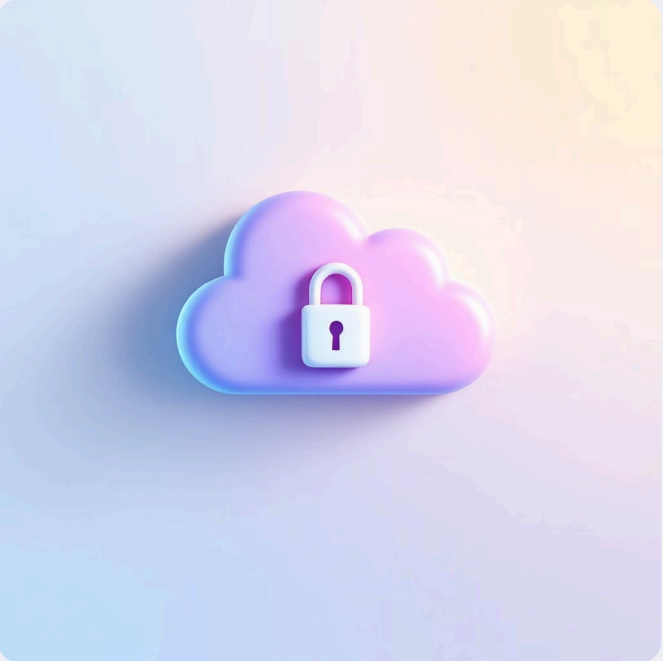
La intención es construir criterios claros, realistas y aplicables, que nos permitan fortalecer nuestra práctica digital desde un enfoque seguro, ético y colaborativo.

Conceptos Claves para la Ciberseguridad Profesional

1. Almacenamiento: ¿Dónde Residen los Datos de Tus Consultantes?

Los datos pueden estar almacenados en dispositivos personales, servidores locales o, más comúnmente, en la nube. Piensen en un consultorio físico: **¿se guardarían los expedientes en un lugar abierto, sin llave, donde cualquiera pudiera verlos?** Por supuesto que no. Con los datos digitales, la lógica es idéntica.

La mayoría de las plataformas actuales utilizan almacenamiento en la nube, lo que significa que los datos residen en servidores de terceros, a menudo en otros países. Esto plantea preguntas criticas sobre jurisdicción y protección.



Para asegurar la protección de los datos, aprende sobre la herramienta que quieres usar:

Cumplimiento Normativo

Normativas como el **RGPD** (Unión Europea), la **HIPAA** (Estados Unidos) o la **Ley 25.326** (Argentina) son marcos exigentes en materia de privacidad. Verificar este cumplimiento es clave para garantizar el resguardo

Residencia de Datos

La ubicación del servidor define qué leyes los protegen. Si se alojan en países sin marcos legales sólidos, **no hay garantías sobre su uso ni confidencialidad**, aunque la plataforma diga ser segura.

Medidas de Seguridad

¿Qué medidas de seguridad técnicas y organizativas se implementan para proteger los datos? Si usan cifrado, control de accesos y backups. Certificaciones como **ISO 27001** o **SOC 2**, garantizan buenas prácticas.

2. Accesos y Llaves: ¿Quién Tiene Acceso a la Información?

No siempre eres solo tú. La gestión de accesos es la primera línea de defensa para proteger la información clínica. A menudo, plataformas que usamos a diario permiten que otras personas (incluso sin que lo notemos) accedan a nuestros datos.

Checklist esencial para evaluar cualquier herramienta:

1 Políticas de privacidad y términos de servicio

Lee con atención qué actores tienen acceso a la información (por ejemplo, personal de soporte, desarrolladores o terceros con fines estadísticos). Si esto no está claro o es excesivamente amplio, es motivo de revisión.

2 Principio de mínimo privilegio

Cualquier acceso por parte de terceros — incluso del soporte técnico— debe estar limitado al mínimo necesario y por el menor tiempo posible. Si una plataforma requiere acceso total solo para resolver un ticket básico, es una señal de alerta.

3 Gestión de contraseñas

Usa contraseñas robustas, únicas por plataforma, y almacénalas en un gestor de contraseñas confiable. Nunca reutilices contraseñas entre cuentas personales y profesionales. (Nombre de mascota con fecha de nacimiento es demasiado vulnerable!)

4 Autenticación en Dos Pasos (2FA/MFA)

Activa siempre la autenticación en dos pasos (o multifactor) en todas las plataformas que lo permitan (mas adelante te cuento como). Es una capa de seguridad adicional vital.

"Me contactaron ofreciendo un software para mi practica"

Se están construyendo muy buenas opciones alrededor de esto. Para conocer y tener un entendimiento de como funcionan, te dejo algunas sugerencias para orientar tu exploración.

Puedes preguntar:

- ¿Dónde se guardan los datos?
- ¿Quién puede ver esa información?
- ¿Cómo usa la plataforma los datos?
- ¿Cómo puedo eliminar los datos?
- ¿Puedo exportar o borrar los datos fácilmente?

Es posible que el asesor no tenga todas las respuestas, pero formular estas preguntas te permitirá evaluar con mayor precisión el nivel de cumplimiento normativo y las medidas de seguridad

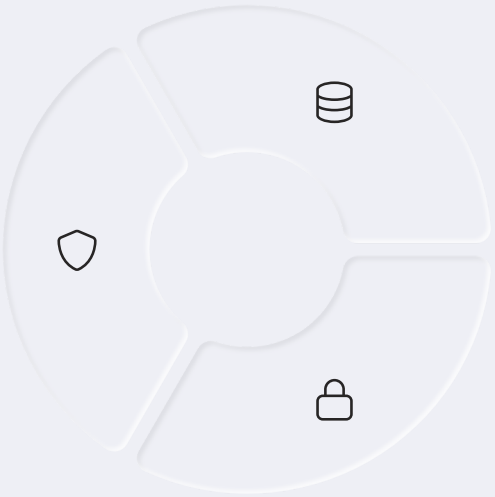
3. Cifrado

Si la información no está cifrada, no está protegida. El cifrado transforma los datos en un formato ilegible para cualquiera que no posea la clave de descifrado, convirtiéndolos en "jeroglíficos" si son interceptados.

Tres niveles de cifrado que deberías exigir:

En Tránsito

El cifrado protege los datos mientras viajan desde tu dispositivo hasta el servidor y viceversa (por ejemplo, mediante HTTPS/TLS). Es como un túnel seguro.



En Reposo

El cifrado protege los datos cuando están almacenados en los servidores. Aunque alguien acceda físicamente al servidor, los datos seguirán siendo ilegibles sin la clave.

De Extremo a Extremo (E2EE)

Es el nivel más alto de seguridad. Solo el emisor y el receptor tienen las claves para cifrar y descifrar la información. Ni siquiera el proveedor del servicio puede acceder al contenido.

Piensa así: Si alguien intercepta esa información, verá una serie de caracteres sin sentido. Eso es exactamente lo que quieres.

Presta atencion :

- **Acceso sin protocolos claros:** Si no te informan quién puede acceder a los datos y bajo qué condiciones, es una señal de alerta.
- **No pedir ni ofrecer transparencia:** La falta de documentación o información clara sobre la seguridad es un indicio de poco compromiso.
- **“Usamos servidores seguros”** (sin detalles).
- **“Cumplimos con estándares de la industria”** (pero no dicen cuáles).
- **“No compartimos datos”** (pero no explican cómo los protegen).

4. Gestión de Datos: ¿Si Quieres Eliminar o Modificar Información?

Los consultantes tienen derecho a solicitar la modificación o eliminación de sus datos. Como profesionales, se debe saber cómo gestionar estas solicitudes de manera segura y eficiente, y **asegurarse de que la plataforma lo permita.**

Claves fundamentales:

Borrado Seguro y Edición Clara

Optá por herramientas que permitan eliminar o modificar información de forma segura, sin dejar rastros ocultos ni versiones anteriores inaccesibles. La edición clara también ayuda a evitar confusiones o duplicidades.

Persistencia de Copias

Al eliminar datos, verificá que no permanezcan copias automáticas en respaldos (backups) que no controlás directamente. Siempre que sea posible, configurá eliminaciones programadas y revisá qué datos persisten.

Documentación de Acciones

Anotá y guardá evidencia cada vez que modifiques o elimines información. Esto no solo ordena tu trabajo, sino que garantiza trazabilidad ante cualquier revisión técnica, clínica o legal.

5. Uso de Datos Clínicos por la Plataforma: ¿Qué hace la plataforma con tu información?

Algunas plataformas no solo almacenan y gestionan datos clínicos, sino que también incorporan inteligencia artificial (IA) para analizarlos, generar reportes automáticos, elaborar estadísticas e incluso sugerir intervenciones o diagnósticos.

Si bien estas funcionalidades pueden optimizar el trabajo, su uso requiere una supervisión activa y consciente. Es fundamental que sepamos **qué tipo de procesos automatizados están en juego, qué datos se usan para entrenar esos algoritmos y cómo se generan las recomendaciones**.

La toma de decisiones clínicas no puede ser delegada a sistemas automáticos sin una evaluación crítica. La transparencia en el funcionamiento de estas herramientas, así como el control humano permanente, son condiciones básicas para resguardar la ética profesional y la seguridad de quienes confían en nosotras y nosotros.

Recomendaciones clave:

Transparencia en el consentimiento informado

Si la plataforma que eliges utiliza IA o algoritmos para procesar los datos clínicos de tus consultantes, esta información debe estar claramente explicitada en el consentimiento informado.

Supervisión profesional

Antes de incorporar plataformas que utilicen algoritmos para generar sugerencias clínicas o “insights”, asegurate de que estas herramientas hayan sido **desarrolladas, validadas y supervisadas por profesionales de la salud mental**.

Privacidad y anonimización

Asegúrate de que los análisis de datos, en caso de aceptarlos, se realicen bajo estrictos procesos de anonimización y que los datos no se utilicen para fines no autorizados ni comercializados.

Consultá directamente al proveedor sobre los criterios clínicos involucrados y verificá si esta información está detallada en los **términos y condiciones** o en la documentación técnica

6. Consentimiento Informado en la Era Digital: Un Requisito Más Exigente

En el contexto digital, el consentimiento informado adquiere un rol aún más crítico. No basta con una aceptación genérica. Debe ser **claro, explícito, comprensible y adaptado al entorno tecnológico en el que se desarrollará la intervención**.

Elementos esenciales que debe incluir:

Herramientas digitales utilizadas

Detalla las plataformas, softwares o herramientas digitales específicas que empleas en tu práctica.

Datos recolectados y duración

Especifica qué tipos de datos se recopilan (personales, clínicos, comunicaciones) y el tiempo durante el cual serán almacenados.

Acceso a la información

Informa quién tiene acceso a los datos (tú, personal de soporte técnico, terceros) y bajo qué condiciones.

Derechos del consultante

Explica claramente los derechos del consultante (acceso, rectificación, cancelación, oposición, etc) y cómo puede ejercerlos para modificar, eliminar o exportar su información.

Uso de inteligencia artificial (si aplica)

Indica expresamente si se utiliza IA y con qué propósito, detallando el procesamiento de datos.

Plan Mínimo para Profesionales ante Incidentes de Seguridad

Tener un consentimiento claro y bien informado es un pilar esencial, pero no suficiente por sí solo. **Incluso con las mejores prácticas, los riesgos existen.**
Y es justamente por eso que debemos estar preparados para actuar cuando algo falle. La ciberseguridad perfecta no existe, Pero sí podemos contar con un **protocolo de respuesta ante incidentes**. La preparación, más que la perfección, es lo que marca la diferencia cuando se produce una brecha de seguridad.

Plan mínimo ante incidentes de seguridad

1 Identificación

¿Qué pasó? ¿Qué tipo de incidente es (filtración, acceso no autorizado, ransomware, hackeo de mi cuenta)? ¿Qué datos se vieron comprometidos?

2 Contención y Actuación

- Cambia inmediatamente todas las contraseñas relevantes.
- Bloquea accesos sospechosos.
- Desconecta dispositivos afectados de la red si es necesario.
- Notifica al proveedor de la plataforma si la brecha es en su lado.

3 Comunicación Transparente

Informa a los consultantes afectados de manera clara, honesta y oportuna, siguiendo las directrices legales de tu jurisdicción. Ofrece apoyo y recursos.

4 Documentación y Lecciones Aprendidas

Documenta exhaustivamente qué ocurrió, qué acciones tomaste, el impacto y cómo se puede prevenir una recurrencia. Esto es vital para la mejora continua.

Aplicación Práctica: Herramientas Comunes y su Ciberseguridad

Como profesionales de la salud mental, manejamos información sensible que está protegida por el secreto profesional y por normativas legales. Sin embargo, muchas prácticas digitales cotidianas pueden comprometer esa privacidad si no se gestionan adecuadamente. Es probable que no se haya considerado antes, pero **con el avance tecnológico, los deepfakes y las estafas, es hora de agregar una capa extra de seguridad y comprender cómo.**

WhatsApp para comunicación clínica

Aunque es una herramienta práctica y de uso extendido, su uso debe limitarse a comunicaciones operativas.(ej. Horarios)

Riesgos frecuentes:

- Vista previa de mensajes en pantalla bloqueada.
- Copias de seguridad no cifradas en la nube.
- Envío de archivos o audios con información sensible.
- Descargas automáticas que pueden incluir archivos maliciosos.

Recomendación práctica: Utilizar dos cuentas de WhatsApp en el mismo dispositivo (una personal y otra con WhatsApp Business) esto permite:

- Tener el canal profesional activo y con sonido, y el personal silenciado.
- Gestionar mejor los límites, disponibilidad y accesos.
- Organizar contactos y mensajes con etiquetas dentro de WhatsApp Business.

Es una solución sencilla, eficiente y altamente recomendable para quienes trabajan con múltiples consultantes o instituciones.

Recomendación técnica:

- **Activar la verificación en dos pasos** (Si necesitas una guía paso a paso, puedes acceder al recurso oficial **aquí**).
- **Desactivar las descargas automáticas de archivos:** Ajustes > Almacenamiento y datos > Descarga automática > Desactivar todo. Evitar la descarga automática es muy útil y agrega seguridad, ya que nuestros números de contacto suelen estar a disposición de muchas personas.
- **Desactivar las copias de seguridad en la nube:** Ajustes > Chats > Copia de seguridad

Agenda Digital (Google Calendar, Calendly, entre otros)

El uso de agendas digitales es altamente funcional para la organización clínica, pero anotar nombres completos, diagnósticos o detalles del proceso terapéutico en plataformas sin configurar adecuadamente la privacidad puede exponer datos sensibles. En muchos casos, por omisión, los calendarios o enlaces pueden quedar visibles o accesibles para terceros, incluso sin que el profesional lo advierta.

Riesgos frecuentes:

Visualización pública de eventos o citas

Los calendarios pueden estar configurados como públicos por defecto, exponiendo información sensible.

Enlaces compartibles sin control de acceso

Los enlaces para agendar citas pueden ser accesibles para cualquiera que los tenga.

Sincronización automática con otros dispositivos o cuentas

La información puede sincronizarse con dispositivos no seguros o cuentas compartidas.

Recomendación práctica:

Una estrategia sencilla para reducir riesgos es evitar anotar nombres completos en la agenda. Se pueden usar iniciales, pseudónimos o códigos internos que solo el profesional comprenda. Esto permite mantener una buena organización sin comprometer la confidencialidad. En mi caso, utilizo abreviaturas y emojis. También se puede hacer por tipo de intervención (ej. "TCC - AB", "1°EVA - ACT") y reservar los detalles clínicos para el registro encriptado correspondiente.

Recomendación técnica:

- **Marcar eventos como privados:** al crear o editar el evento > opción "Privacidad" > seleccionar "Privado".
- **Revisar los permisos de calendario compartido:** Configuración (ícono de engranaje) > Configuración de mis calendarios > Compartir con personas específicas > Revisar quién tiene acceso y con qué nivel de visibilidad. Encuentra más sobre ajustes en Google Calendar: aquí)
- **En Calendly:** evitar enlaces abiertos en redes sociales o sitios web sin contraseña. Usar la opción de aprobación manual para cada cita y configurar recordatorios sin contenido sensible.

Notas clínicas en Google Docs, Notion o Evernote

Estas herramientas son super útiles para tomar notas, pero no fueron diseñadas específicamente para manejar información clínica protegida. Su uso, sin configurar adecuadamente la privacidad , puede generar riesgos.

Riesgos frecuentes:

Enlaces compartidos públicamente

Documentos compartidos mediante enlaces pueden ser accesibles para cualquiera que los tenga. Usa enlaces con acceso restringido por correo, contraseña o fecha de expiración.

Falta de cifrado en reposo o en tránsito

La información puede no estar adecuadamente protegida durante su almacenamiento o transmisión. Consulta directamente al proveedor o revisa su política de privacidad y seguridad. Elegí plataformas que indiquen explícitamente que usan cifrado.

Sincronización automática con cuentas o dispositivos no protegidos

Los datos pueden sincronizarse con dispositivos o cuentas que no tienen medidas de seguridad adecuadas. Revisá qué dispositivos o cuentas están vinculados y si tienen configuraciones de seguridad activas.

Recomendación práctica:

Si se decide usar estas herramientas, evita registrar datos identificatorios (nombre, DNI, dirección, etc.) y usa claves internas o codificación, (Repito el ejemplo "AV-TCC" siglas y tipo de abordaje). Además, ten siempre un respaldo cifrado en un entorno profesional y separado, como un disco aparte o un USB cifrado.

Recomendación técnica:

- **Google Docs:** revisar que el documento no esté en "Cualquiera con el enlace" > Archivo > Compartir > Ajustar permisos a "Personas específicas".
- **Notion:** desactivar la opción "Share to web" desde el botón "Compartir" en la parte superior derecha.
- **Evernote:** usar contraseña en el dispositivo, y si se comparte, hacerlo solo con usuarios específicos desde Archivo > Compartir nota.

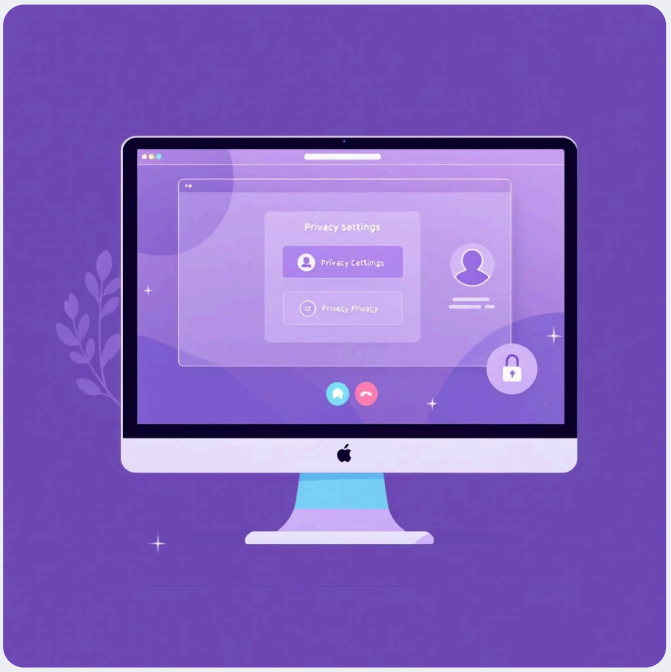
Sesiones virtuales por Zoom, Meet u otras plataformas gratuitas

Muchas plataformas gratuitas no garantizan un nivel de seguridad adecuado para proteger la privacidad de una sesión clínica. Esto no significa que no puedan usarse, pero sí que **deben configurarse cuidadosamente para minimizar riesgos.**

A continuación, te explico **cuáles son los principales puntos vulnerables** y cómo reducir la probabilidad de que un riesgo se transforme en una amenaza real para tu práctica y la confidencialidad de tus consultantes.

Riesgos frecuentes:

- Accesos no autorizados a las sesiones.
- Grabaciones automáticas sin control.
- Almacenamiento de datos en la nube sin cifrado.



Recomendación práctica:

Nunca grabes sesiones salvo consentimiento informado y justificación clínica. Para mayor protección, considera explorar plataformas diseñadas para profesionales de la salud.

Tip: un ejemplo en USA es Theraplatform que cumple con la normativa HIPAA (Health Insurance Portability and Accountability Act) que si bien es una normativa de Estados Unidos, es relevante como estándar de referencia en protección de datos en salud.

Recomendación técnica:

Zoom

Activar sala de espera y contraseña y desactiva grabación automática, normalmente en Configuración > Grabación.

Google Meet

No graba por defecto, pero asegúrate de que el enlace no se distribuya libremente y se mantenga bajo control como hicimos con Google Calendar. Usa cuentas de Google Workspace si están disponibles.

Dispositivos personales (móviles, tablets, laptops)

Trabajar desde dispositivos personales es habitual, pero sin medidas de protección adecuadas, pueden convertirse en una puerta de entrada a violaciones de confidencialidad.

Riesgos frecuentes:

Acceso no autorizado

Por pérdida, robo o uso compartido del equipo.

Exposición en redes Wi-Fi públicas

Las redes públicas son especialmente vulnerables a ataques.

Infección por malware o ransomware

Software malicioso que puede comprometer la seguridad de los datos.

Recomendación práctica:

Separá tu entorno laboral del personal siempre que sea posible. Si compartís dispositivo, creá usuarios diferenciados y protegé carpetas sensibles con contraseña o cifrado básico. Esto reduce el riesgo de accesos no autorizados a información clínica.

Recomendación técnica:

- **Activar bloqueo automático con PIN, patrón o biometría:** Configuración > Seguridad.
- **Evitar redes Wi-Fi públicas o usar VPN** Si es necesario, usá una **VPN confiable** (como NordVPN) para proteger la conexión. Si puedes, evita conectarte a ellas durante el trabajo.
- **Instalar un antivirus profesional** (Bitdefender, Kaspersky, etc.)) y asegurate de **mantener todo el software actualizado**, incluyendo el sistema operativo y las aplicaciones que usás en tu práctica.

¿Qué es la IA y Cómo Puede Asistirnos?

En la era digital, la Inteligencia Artificial (IA) emerge como una herramienta con un potencial transformador para diversas profesiones, incluida la psicología. Es crucial entender que la IA es una asistencia, no un reemplazo de la experticia, el juicio clínico y la empatía humana.

La Inteligencia Artificial se refiere a sistemas o máquinas que imitan la inteligencia humana para realizar tareas y pueden mejorar iterativamente a partir de la información que recopilan. En nuestra práctica, la IA puede asistir en:

Tareas Administrativas

Gestión de agendas, recordatorios de citas, transcripción de notas (siempre con consentimiento explícito y bajo estrictos protocolos de privacidad).

Análisis de Datos (con cautela)

Herramientas que pueden identificar patrones en grandes volúmenes de datos (por ejemplo, tendencias en la investigación) o generar resúmenes de literatura científica, siempre bajo la supervisión y validación del profesional.

Generación de Contenido (con supervisión)

Asistencia en la redacción de informes no clínicos, materiales educativos para consultantes o borradores de artículos, que deben ser revisados, editados y aprobados por el profesional de la psicología.

Herramientas de Apoyo

Esto si encuentras app que usan IA y que ayuden a la persona en el proceso de recuperacion, considera que sean verificadas, pruebalas primero y saca una opinion profesional antes de recomendar.

La Inteligencia Artificial ofrece oportunidades para optimizar y enriquecer nuestra práctica. Esta guia tan organizada no hubiese sido posible sin su asistencia. Sin embargo, su implementación en la practica clinica debe ser consciente, ética y siempre subordinada a la primacía del bienestar del consultante y la responsabilidad profesional.

Ética en el Uso de Plataformas con IA

Algunas plataformas no solo almacenan y gestionan datos, sino que además emplean inteligencia artificial (IA) **para analizar información, generar reportes automáticos, producir estadísticas** o incluso brindar recomendaciones clínicas.

Consideraciones Éticas y de Ciberseguridad en el Uso de Inteligencia Artificial (IA)

El uso de IA en una disciplina tan sensible como la psicología requiere una reflexión ética profunda y un estricto cumplimiento de principios de ciberseguridad para proteger tanto al profesional como a los consultantes.

Entiendo que a veces puede parecer difícil, pero con prácticas como estas podemos **reducir riesgos, proteger la confidencialidad** y fortalecer la seguridad digital en nuestro ejercicio profesional. No se trata de saberlo todo, sino de incorporar criterios informados y actuar con responsabilidad clínica también en el entorno virtual.

1. Privacidad de Datos

Anonimización

Asegúrate de que cualquier dato de consultante que se procese mediante IA esté completamente anonimizado o pseudonimizado, minimizando riesgos de identificación directa.

Políticas de datos del proveedor de IA

Investiga cómo la plataforma gestiona, almacena y utiliza los datos. **¿Se emplean para entrenar modelos futuros? ¿Se comparten con terceros?** Este aspecto debe ser transparente y acorde con normativas vigentes.

Consentimiento informado

El uso de IA debe estar claramente explicitado en el consentimiento informado, detallando qué datos serán procesados y con qué propósito.

2. Sesgos Algorítmicos

Los modelos de IA se entrenan con grandes volúmenes de datos. Si esos datos de entrenamiento contienen sesgos (sociales, culturales, demográficos, etc.), la IA puede aprender y replicar esos sesgos, lo que podría llevar a resultados inexactos, injustos o discriminatorios en sus análisis o sugerencias.

- **Alucinaciones y Precisión**

  Las IA generativas pueden producir información que parece plausible, pero que en realidad es incorrecta o inventada ("alucinaciones").

- **La IA no es Infalible**

  La precisión de la IA no es absoluta y requiere de la validación final por parte de un ser humano.

- **Validación Humana**

  Toda salida generada por IA debe ser rigurosamente verificada y validada por un profesional antes de su uso o comunicación.

3. Seguridad de la Plataforma de IA

- Verifica que la plataforma cumpla con estándares sólidos de cifrado, control de accesos y almacenamiento seguro, equivalentes a cualquier herramienta digital profesional.
- En caso de integraciones con otros sistemas (por ejemplo, software de gestión de consultantes), asegúrate que sean seguras y cumplan con protocolos de protección de datos.

4. Responsabilidad Profesional

- La responsabilidad última sobre la atención, diagnósticos y manejo de la información recae siempre en la psicóloga o el psicólogo.
- La IA debe ser entendida como un apoyo tecnológico, nunca un sustituto del juicio clínico ni de la ética profesional.

5. Formación Continua

Mantente al día sobre las capacidades, limitaciones y riesgos éticos asociados al uso de IA en salud mental, para asegurar una práctica responsable y segura.

No es solo Tecnología. Es Confianza.

La digitalización llegó para quedarse. Pero como psicólogas, psicólogos y profesionales de la salud, no estamos solo para adaptarnos, sino para liderar una práctica ética, informada y humana en el entorno digital.

Este es tu nuevo espacio clínico. Protégelo con la misma rigurosidad, el mismo cuidado y la misma dedicación con la que proteges tus sesiones presenciales. La confianza de tus consultantes es tu activo más valioso, y en la era digital, esa confianza se construye también a través de la ciberseguridad.

Seguimos construyendo entornos digitales más seguros, éticos y humanos.

Declaración sobre el uso de inteligencia artificial

En la elaboración de esta guía se incorporó, de manera complementaria y bajo supervisión profesional, el uso de herramientas de inteligencia artificial generativa: **ChatGPT (OpenAI, versión GPT-4.5, 2025)** para apoyo editorial, y **Gamma App** para diseño visual.
Su participación se limitó a funciones de mejora expositiva, consistencia terminológica y precisión técnica en temas vinculados a **ciberseguridad aplicada al ejercicio psicológico**.

¿Te gustaría acercar esta guía a tu equipo, colegas o estudiantes?

Si estás trabajando en proyectos de ciberseguridad, bienestar digital o cultura organizacional, me interesa colaborar desde una perspectiva psicológica. Estoy abierta a sumarme a equipos de Security Awareness y a iniciativas interdisciplinarias donde la tecnología y el cuidado de las personas se encuentren.

Me motiva co-crear soluciones que integren tecnología, bienestar laboral y ética digital. Puedo aportar mi experiencia y conocimientos para desarrollar estrategias que ayuden a proteger a las personas y fomentar un uso consciente y responsable de las herramientas digitales.

Podés explorar mis recursos y publicaciones en:
www.codigocalma.com
Y si te interesa que conversemos, escribime por mensaje directo o conectemos en LinkedIn:
linkedin.com/in/tatiana-staculpsi

Tatiana Stacul
Cyberpsychology | Cybersecurity