Colegio Oficial de la Psicología de Madrid

Buenas Prácticas para la Protección de Datos en Telepsicología

www.copmadrid.org

Autores:
Nombre de los autores del documento

Colegio Oficial de la Psicología de Madrid
Cuesta de San Vicente, 4, 5º. 28008 Madrid
formacion.online@cop.es

Nota aclaratoria: En beneficio de una mayor facilidad y claridad en la lectura y comprensión del texto, se utilizará un lenguaje igualitario y no sexista. No obstante, se explicita que, en el uso de términos como los profesionales, los estudiantes, los responsables, los psicólogos, … y cualquier otro que se encuentre en este documento, se hace referencia a hombres y mujeres, e incluye el masculino y el femenino.

ÍNDICE

Buenas prácticas de Protección de datos en Psicología en Internet

Buenas prácticas de Protección de datos en Psicología en Internet

1. Principios deontológicos en la práctica online

Cumplimiento del Código Deontológico

El/la profesional deberá cumplir con todos los preceptos del **Código Deontológico** en su actuación profesional de la misma manera que se realiza cuando la modalidad de atención es presencial. Si bien, en la modalidad de asistencia psicológica a distancia deberá prestar especial atención a las siguientes cuestiones:

- *Recabará las autorizaciones correspondientes en los casos de clientes menores de edad o legalmente incapacitados/as.*
- *Deberá rechazar llevar a cabo la prestación de sus servicios cuando hay certeza de que puedan ser mal utilizados.*
- *Según el tipo de asistencia psicológica a proporcionar, será necesario recabar los recursos de emergencia y atención sanitaria del área donde esté ubicado/a (número de teléfono de ayuda, localización de hospitales y servicios médicos, preferiblemente con urgencias y atención psiquiátrica). Así como un contacto, en el entorno del cliente/clienta, mediante consentimiento previo.*
- *Ofrecerá información adecuada acerca del tipo de la atención psicológica que se prestará, la naturaleza de su relación, los propósitos de la atención a facilitar, el tipo de servicio de TelePsicología que se realizará, en qué momentos se producirá y qué limitaciones tendrá.*
- *En todo momento deberá valorar la modalidad de atención más eficaz para el cliente/clienta debiendo abandonar la modalidad a distancia, si fuera preciso, indicando al cliente la modalidad presencial y/o servicios alternativos.*

- *Deberá finalizar la asistencia psicológica y no prolongarla innecesariamente cuando se hayan cumplido los objetivos propuestos o si después de un tiempo razonable no se han alcanzado, indicando al cliente qué otros psicólogos/as o profesionales podrían hacerse cargo.*
- *La autoridad profesional del Psicólogo/a reside en las competencias acreditadas y cualificaciones alcanzadas para ofrecer los servicios psicológicos, debiendo reconocer los límites de su competencia.*

En este enlace se puede consultar el Código Deontológico.

2. Internet como herramienta de trabajo segura

Cuando utilizamos internet, además de respetar, por supuesto, **todos los principios de protección de datos y medidas de seguridad de la información indicadas por la legislación vigente,** hay que considerar las peculiaridades de este medio

Antes de nada, vamos a indicar las principales legislaciones y estándares de seguridad a tener en cuenta para el cumplimiento en esta materia:

Principal Legislación de Protección de Datos:

- Reglamento General de Protección de Datos.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Algunas de las principales nomas de seguridad de la información

- Esquema Nacional de Seguridad
- Familia de normas ISO 27000

Sociedad de la información y telecomunicaciones

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 11/2022, de 8 de junio, General de Telecomunicaciones

En la actualidad, es difícil concebir un mundo sin el uso de tecnologías de la información. En el área profesional, las tecnologías de la información ofrecen nuevas herramientas que nos permiten llegar a más gente y ofrecer nuevos servicios, reduciendo costes.

El uso de estas herramientas puede ir desde la comunicación con un simple correo electrónico, para facilitar una consulta aislada sobre el proceso terapéutico, a la intervención terapéutica online (TelePsicología/Psicología online), en los casos en los que es pertinente, o incluso a la utilización de realidad virtual y aumentada en determinadas terapias.

No cabe duda de que las tecnologías de la información tienen muchas ventajas, pero también conllevan riesgos añadidos.

3. Riesgos potenciales

A continuación, se muestran algunos aspectos en los que hay potenciales riesgos a la seguridad de los datos.

A. En la comunicación entre paciente/cliente y profesional

En la telecomunicación, pueden surgir dudas sobre si la persona con la que estamos hablando o enviando un mensaje **es la persona que dice ser**, así mismo, **se debe impedir que alguien se haga pasar por nosotros**.

Otra preocupación puede ser el que alguien ajeno pueda **interceptar la comunicación y acceder a la conversación** entre el profesional y el/la paciente/cliente o a la **documentación** que se intercambie.

A continuación, veremos dichos riesgos y la forma de evitarlos.

Inseguridad sobre la identidad paciente/cliente y profesional

"Me preocupa que la persona con la que estoy intercambiando la información no sea realmente el/la paciente o que alguien pueda hacerse pasar por mí".

Medidas a tomar

Asegurar identidad del cliente/a. Hay que asegurar la identidad del cliente/a, puede ser con el uso de **certificado electrónico** a la hora de pedir los datos, o incluso solicitando que **enseñe el DNI** a la videocámara, en caso de duda se puede solicitar información complementaria, es muy importante en todo caso, pero sobre todo en el **caso de menores**.

Asegurar identidad del profesional. Hay que identificarse debidamente, incluyendo el **número de colegiación** y en su caso si se está habilitado/a para el ejercicio como **psicólogo/a clínico**, se puede mostrar el **carnet de colegiación** a la videocámara.

Riesgo de interceptación de las comunicaciones o la documentación

"*La información intercambiada entre profesional y el/la paciente/cliente puede ser muy íntima y delicada, ¿Cómo puedo asegurarme de que no acceda nadie ajeno a las comunicaciones?"*

Medidas a tomar

Utilizar aplicaciones para realizar llamadas o videollamadas y mensajería seguras, que cifren la información de punto a punto, tanto en los dispositivos móviles (Smartphone o Tablet), como en el ordenador, con autenticación de la identidad (del profesional y del cliente).

En este tipo de comunicaciones además del cifrado de punto a punto, es decir, que se encripta en el momento del envío y se descifra sólo cuando llega a su destino final, se debe garantizar que nadie pueda acceder a la comunicación, ni los mismos prestadores del servicio (es decir que el proveedor del servicio no tiene que tener acceso a la clave de cifrado).

Hay aplicaciones de este tipo que sí que garantizan el cifrado de punto a punto, pero ellos sí pueden interceptar y leer las comunicaciones, por lo que sería una conexión segura pero no privada. Para un nivel de seguridad alto, como exige los datos de la historia clínica, no nos serviría.

Se debe **cambiar las contraseñas con frecuencia** y usar, a ser posible, mecanismos de doble verificación para recuperar la contraseña en caso de olvido, siempre habrá que utilizar contraseñas robustas, con más de ocho dígitos y que combinen mayúsculas y minúsculas, símbolos y números.

Se deberán tener **antivirus y cortafuegos actualizados**, así como mantener actualizado el sistema operativo y software que se utilice, para contar con los últimos parches que solucionen problemas de seguridad detectados.

El software que se utilice para las videoconferencias **no debe permitir que haya varias sesiones abiertas**, una sesión deberá ser cerrada para poder abrir otra y siempre deberemos cerrar la sesión antes de salir.

No se deben realizar comunicaciones desde wifis públicas.

Los archivos que se intercambien deberán ser enviados de forma segura, por ejemplo, **encriptando la información**.

.

Cuidar el entorno dónde se realizan las comunicaciones para que no puedan ser oídas las conversaciones por terceros, **formando al cliente/a en dicho sentido** también, para que realice las comunicaciones desde un espacio privado y borre o almacene de forma segura la documentación a la que no quiera que accedan terceros.

En el almacenamiento de la información

"Me preocupa que, si utilizo dispositivos móviles o utilizo almacenamiento en la nube, se acceda a la información que almaceno, me preocupa que no esté tan segura como en el disco duro del ordenador del centro"

Otro riesgo potencial puede estar en el **almacenamiento de los datos**, tanto si es en dispositivos móviles como smartphones o tablets o en la nube

Medidas a tomar

Si se utilizan **servicios en la nube** para almacenar la información, habrá que asegurarse de que los prestadores del servicio tengan ubicados sus **servidores en países que garantizan la legislación europea de protección de datos**, así

mismo se deberán firmar los debidos contratos de prestación de servicios**,** con la información sobre las medidas de seguridad que se han de tomar. Se debe leer siempre atentamente las condiciones de privacidad y seguridad de servicios antes de contratarlos.

Es importante encriptar la información sensible antes de subir a la nube.

Los dispositivos externos que almacenen información, por ejemplo, las **copias de seguridad**, da igual en la forma que se almacene (CD o DVD, USB, Pen Drive, disco duro, etc.) deben estar por supuesto, encriptadas.

Los dispositivos, (sobre todo los móviles), se deberán configurar para que se **inactiven tras un periodo de inactividad y solicite contraseña** para volver a conectar, este periodo no deberá ser mayor de **15 minutos**, para que nadie acceda a la información cuando el/la profesional no está presente o si se pierde o se produce un robo.

Los dispositivos móviles deben poder ser **desactivados a distancia** en caso de pérdida o robo.

Se deberá **informar al paciente** de los aspectos comentados, para que la información que se almacene en móviles se realice de manera que no pueda ser accesible a otras personas.

B. Otros aspectos a tener en cuenta

Importancia de una formación tecnológica adecuada del profesional y del cliente

Como estamos viendo, es muy importante para garantizar todo lo anterior, que el/la profesional antes de empezar a utilizar este tipo de recursos, esté al día de los aspectos técnicos que hemos repasado, para poder garantizar la seguridad, y también valorar si será necesario informar/formar al cliente para que pueda hacer uso de los servicios con seguridad.

Si se considera que por sí mismo no va a poder mantenerse actualizado en estos aspectos, siempre se pueden contratar servicios de empresas especializadas en soluciones informáticas o de protección de datos.

Intervención psicológica online

En relación a la **intervención psicológica**, se pueden utilizar **plataformas seguras**, donde realizar la sesión con seguridad, y poder intercambiar comunicaciones y documentación sin salir de la plataforma.

En todo caso si se decide realizar la intervención psicológica a través de plataformas especializadas, se debe comprobar que ofrecen las debidas **garantías de seguridad**, verificando que cumplen con todos los aspectos que hemos ido mencionando.

Información sobre tratamiento y consentimiento en Internet

Un aspecto muy importante a tener en cuenta cuando realizamos intervención psicológica en internet es el tema de la **información sobre el tratamiento de datos** y el **consentimiento** tal y como indica la legislación de protección de datos. Si siempre es importante informar sobre el tratamiento de datos, en un

medio como internet donde se está expuesto a mayores riesgos, es aún más importante.

La información se deberá presentar antes de acceder al servicio, de forma que **sea ineludible leerla y dar los consentimientos pertinentes**, puede ser una **pantalla** en la que hay que leer y aceptar la información antes de seguir con el servicio.

En el *documento "Recomendaciones sobre la intervención psicológica mediante internet"* publicado por el **Colegio Oficial de Psicólogos de Andalucía Occidental** se recomienda:

"Al inicio se deberá proporcionar información sobre los siguientes aspectos: (1) la identidad del psicólogo/a, titulación que le habilita para el ejercicio profesional en el ámbito clínico, el número de colegiación y dirección de la consulta, (2) la forma en la que se van a ofrecer los servicios, si es a 'tiempo real', a través de programas interactivos o por correo electrónico, o de forma mixta, (3) el tiempo de espera para las respuestas a los mensajes de correo electrónico o disponibilidad para establecer sesiones a "tiempo real" mediante chats o videoconferencia, (4) la forma en la que se van a recoger y archivar los datos y sistemas establecidos para proteger la seguridad y confidencialidad de los mismos así como sobre los derechos de los usuarios para el acceso a los mismos, (5) los límites de la confidencialidad (en el caso de que los archivos sean exigidos judicialmente o tengamos conocimiento de situaciones en las que estaríamos obligados a notificar a las autoridades, por ej., abuso sexual de un menor, etc.), (6) los riesgos potenciales, posibles contraindicaciones y alternativas de tratamiento, (7) los procedimientos previstos si surgieran situaciones de crisis o de emergencia y (8) los honorarios establecidos para las distintas formas de intervención y la forma de cobro."

Tampoco hay que olvidar incluir en la página web, la correspondiente información sobre la política de privacidad, cookies y avisos legales.

Al enviar correos electrónicos, es importante recordar que **el asunto no debe dejar ver que se trata de una intervención psicológica**.

Otro aspecto que es importante cuidar, y que ya hemos mencionado en parte, es **informar de los riesgos al cliente/paciente**, y **de lo que pueden hacer** para evitar dichos riesgos. De nada sirve que el/la profesional cuide hasta el último detalle, si el/la cliente no respeta también las medidas de seguridad pertinentes.

Por tanto, habrá que verificar en la medida que se pueda, la información de la que dispone, para facilitarle pautas de seguridad.

Por ejemplo, se le puede advertir, entre otros, de los siguientes aspectos:

- De la necesidad de **elegir un lugar privado para la intervención psicológica**, asegurándose en la medida de lo posible de que eso sea así, por ejemplo, recordándole cerrar la puerta, si se ve abierta al empezar la videoconferencia, o preguntándolo si está sólo en la habitación.
- Sobre la importancia de **borrar la información o almacenar de forma segura**, de forma que no pueda ser accesible a terceros.
- Sobre la **importancia de los antivirus y contraseñas seguras** o proteger los dispositivos móviles.
- Recordar que es mejor **no utilizar wifis públicas** y si se hace, utilizar VPN y asegurarse de **cerrar la sesión**.

Por último, hay que tener en cuenta que, si se realiza intervención psicológica con personas ubicadas en **otros países**, habrá que **considerar las diferentes jurisdicciones**, por si variara algún aspecto legal.

Colegio Oficial de la Psicología de Madrid

www.copmadrid.org