

# **Seguridad Informática a cumplir por las plataformas de Telepsicología**

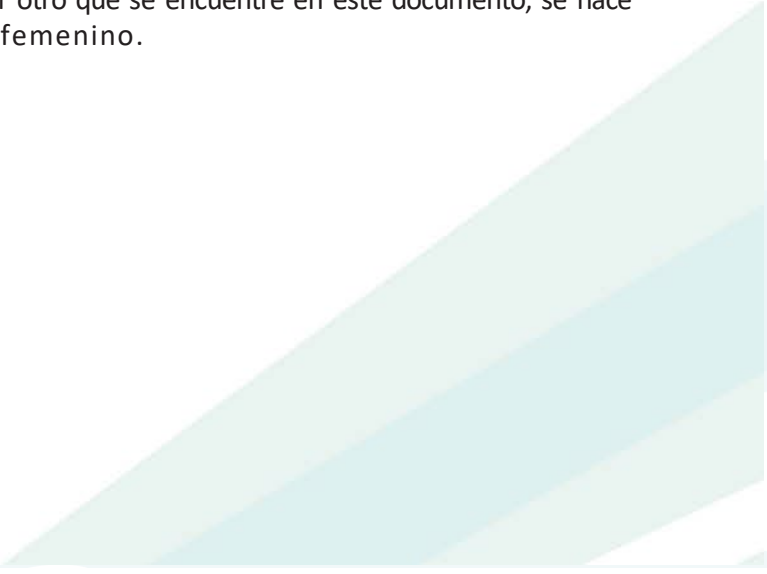
**Autores:**

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

**© Colegio Oficial de la Psicología de Madrid, 2023**

**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

## Dimensiones de Seguridad de la información a cumplir por las plataformas de Psicología online

1. Dimensiones de Seguridad de la información a cumplir por las plataformas de Psicología online principios deontológicos en la práctica online .....4

## Dimensiones de Seguridad de la información a cumplir por las plataformas de Psicología online

Es muy importante asegurar que las plataformas de TelePsicología o Terapia online que se utilicen, garanticen las pertinentes medidas de seguridad, por lo que debemos asegurar que implantan y mantienen los programas, controles, políticas, medidas de seguridad que garanticen la conservación de las siguientes Dimensiones de seguridad.

Dimensiones de seguridad de la información a garantizar	
<b>DISPONIBILIDAD</b>	Las plataformas de Psicología Online o TelePsicología deben garantizar la disposición de los servicios a ser usados cuando sea necesario evitando o reduciendo al mínimo las interrupciones del servicio.
<b>INTEGRIDAD</b>	Las plataformas de Psicología Online o TelePsicología deben permitir el mantenimiento de las características de completitud y corrección de los datos. Se debe impedir que la información pueda ser manipulada, o quede corrupta o incompleta
<b>CONFIDENCIALIDAD</b>	Las plataformas de Psicología Online o TelePsicología permiten que la información llegue solamente a las personas autorizadas. Se debe garantizar que no puedan darse fugas o filtraciones de información, así como accesos no autorizados.
<b>AUTENTICIDAD</b>	Las plataformas de Psicología Online o TelePsicología deben garantizar que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Se debe impedir que la información pueda tener alguna manipulación en el origen o en el contenido de los datos. Se deberá evitar en cualquier caso la suplantación de identidad.

## **TRAZABILIDAD**

Las plataformas de Psicología Online o TelePsicología deben determinar quién hizo qué y en qué momento. La trazabilidad es esencial para poder analizar cualquier incidente, localizar al responsable y poder implantar medidas correctivas y preventivas para evitar su repetición. Se establecerán medidas que permitan realizar registros de actividad.

Las plataformas pueden acreditar que garantizan el cumplimiento de las dimensiones de seguridad comentadas, si disponen de certificados de cumplimiento de normas de seguridad de la información como puede ser el Esquema Nacional de Seguridad o la ISO 27001.

Como ejemplo, en el siguiente [enlace](#), se puede consultar las medidas de seguridad establecidas por el Esquema Nacional de Seguridad.

Sin ser exhaustivos, **algunas buenas prácticas para garantizar las dimensiones comentadas son las siguientes:**

1. Que se realice un tratamiento de los datos adecuado según la legislación relacionada con protección de datos, seguridad de la información y servicios de la sociedad de la información y telecomunicaciones.
2. Informar debidamente en las políticas de privacidad, en la información sobre protección de datos, el aviso legal, cookies, etc. según la legislación del punto 1.
3. Deberá facilitar los derechos de protección de datos, es decir, los derechos de acceso a la información, rectificación, cancelación y en su caso oposición, limitación del tratamiento y portabilidad de los datos, por medios electrónicos, según lo determinado por el RGPD especialmente establecerá mecanismos para facilitar el derecho a la portabilidad de los datos.
4. La ubicación de los servidores será en territorio de la Unión Europea.

5. Las medidas de seguridad serán las adecuadas para garantizar la seguridad de las actividades de tratamiento realizadas.
6. Se establecerán mecanismos de identificación del paciente, (entrevista previa para confirmar identidad y recabar consentimientos o uso correo seguro, certificado electrónico, petición de datos completos para verificar la identidad, verificación de los datos de contacto, mecanismos de usuario contraseña y envío de link a correo para confirmar el registro).
7. Se establecerán mecanismos e Identificación del profesional (colegiación, habilitación) y se verificarán los datos de contacto.
8. Se establecerán mecanismos que impidan crear “salas de encuentro” con más usuarios.
9. La plataforma no dispondrá de funciones propias de redes sociales.
10. Se establecerán mecanismos que impidan que se abran sesiones múltiples de forma simultánea.
11. Se encriptarán las comunicaciones y la documentación intercambiada, cifrado de extremo a extremo.
12. No se permita la grabación de la videoconferencia sin consentimiento.
13. La anchura mínima de banda de 1.2 MBPS en ambas direcciones (carga y descarga) con una resolución mínima de 1080 imágenes por segundo,
14. Se dispondrá de mecanismos para probar la conexión (probar el ancho de banda, por ejemplo) para asegurar que tiene suficiente calidad, se recomendará la utilización de conexiones con cable preferentemente y la evitación de utilizar wifis públicas.
15. Se facilitará la realización de un protocolo de emergencias, ubicando al paciente, y personas de contacto, realizándolo con los debidos permisos para facilitar la información de terceros
16. Los/las profesionales deberán disponer de una competencia adecuada y, formación suficiente para este tipo de intervención online, así como información sobre seguridad en internet
17. Se deberá asegurar la competencia de los y las clientes/pacientes, la idoneidad para este tipo de intervención para el cliente/a, facilitando en su caso la debida formación e información sobre seguridad en internet,

requisitos sistema, sobre el entorno físico adecuado (entrevista previa o facilitación de información).

18. Se informará sobre los riesgos específicos y recomendaciones para la intervención online
19. Se informará adecuadamente sobre condiciones del servicio, procedimientos a seguir en caso interrupciones o dificultades tecnológicas, se facilitará un teléfono de asistencia o correo electrónico en la plataforma para la resolución de incidencias, los honorarios de las sesiones, así como la política de devolución del pago por servicio no realizado o interrumpido
20. Los pagos se realizarán a través de plataforma de pago seguras.
21. La conservación de la información (en el caso de la Comunidad de Madrid) se realizará conforme a la legislación que regula la historia clínica, Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente) que obliga a la conservación durante 5 años de la historia clínica desde la fecha de alta del proceso asistencial.
22. Se habilitará los mecanismos pertinentes que permitan la descarga de la información, para garantizar portabilidad de forma segura y gestión externa a la plataforma de la historia clínica.
23. La Destrucción de la información una vez finalizado el tratamiento se realizará según legislación de protección de datos.

