"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año de la recuperación y consolidación de la economía peruana"

OPINIÓN CONSULTIVA N° 007-2025-JUS/DGTAIPD

ASUNTO	:	Sobre la atención de solicitudes referidas a las contraseñas de las redes de internet *"wifi"* de titularidad pública, contratadas con recursos públicos y para el ejercicio de funciones públicas
REFERENCIA	:	Carta s/n (HT. 001823281-2023)
FECHA	:	24 de enero de 2025

I. ANTECEDENTES

1. Mediante el documento de la referencia, la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, DGTAIPD), recepcionó una solicitud ciudadana para absolver la siguiente consulta:

> *En ejercicio del derecho de Acceso a la Información Pública y ante el requerimiento de un ciudadano, ¿Las entidades públicas se encuentran obligadas a suministrar la o las contraseñas de las redes wifi de su titularidad? ¿Las entidades podrían negarse a entregar dicha información basándose en la afiliación institucional del ciudadano solicitante? Ello, considerando que dichas redes son contratadas con recursos públicos y sirven para el ejercicio de la función pública.* (subrayado agregado).

II. MARCO NORMATIVO DE ACTUACIÓN

2. De conformidad con el artículo 4 inciso 4 del Decreto Legislativo 1353[1] que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, esta Autoridad tiene la función de absolver las consultas que las entidades o las personas jurídicas o naturales le formulen respecto de la aplicación de normas de transparencia y acceso a la información pública.

3. En esa medida, esta Dirección General, en tanto órgano de línea del Ministerio de Justicia y Derechos Humanos sobre el que recae la Autoridad Nacional de Transparencia y Acceso a la Información Pública (en adelante, Antaip), emite la presente Opinión Consultiva, en mérito a la normativa citada, en el ámbito de la interpretación en abstracto de las normas; es decir, como pauta de interpretación general y no como mandato específico de conducta para un caso en concreto.

4. En tal sentido, considerando la consulta ciudadana formulada, esta Dirección General se pronunciará sobre los siguientes aspectos:

[1] Decreto Legislativo que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la regulación de gestión de intereses.

- Sobre las redes de internet *"wifi"*, sus contraseñas de acceso y los riesgos de entregarla o publicarla: a propósito de aquellas redes de titularidad pública, contratadas con recursos públicos y para el ejercicio de funciones públicas.

- Sobre la flexibilización del régimen de excepciones para cautelar información que no debería entregarse por afectar otros principios dignos de tutela: a propósito de la atención de las solicitudes de contraseñas de las redes de internet *"wifi"* de titularidad pública, contratadas con recursos públicos y para el ejercicio de funciones públicas.

- Sobre la inviabilidad de denegar o entregar información alegando condiciones subjetivas del solicitante como la pertenencia o no a la entidad requerida u ostentar alguna afiliación institucional.

III. ANÁLISIS

A. Sobre las redes de internet "wifi", sus contraseñas de acceso y los riesgos de entregarla o publicarla: a propósito de aquellas redes de titularidad pública, contratadas con recursos públicos y para el ejercicio de funciones públicas

5. Actualmente, el uso intensivo de las *"tecnologías digitales"*[2] en la Administración Pública constituye una realidad innegable. Si bien estas recurren a dichas herramientas para optimizar sus procesos internos (dotar de celeridad y simplicidad a sus actos de administración interna) o relaciones con otras entidades (dinamizar la colaboración interinstitucional) su objetivo final es beneficiar a los ciudadanos mediante la prestación efectiva de más y mejores servicios públicos.

6. Una de estas tecnologías digitales es *"la internet"*, entendida como una *"red de telecomunicaciones a la cual están conectadas centenares de millones de personas, organismos y empresas en todo el mundo"*[3]. La conexión a esta red, en principio, puede realizarse de forma física (mediante el cableado) e inalámbrica mediante la tecnología *"wifi"*, el cual *"es un sistema que permite la interconexión inalámbrica, dentro de un área determinada, de dispositivos electrónicos, cuyo uso más común y extendido es el acceso a Internet"*[4]. (subrayado agregado).

---

[2] De conformidad con el artículo 3 numeral 1 del Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital las **tecnologías digitales** *"se refieren a las Tecnologías de la Información y la Comunicación - TIC, **incluidos Internet**, las tecnologías y dispositivos móviles, así como la analítica de datos utilizados para mejorar la generación, recopilación, intercambio, agregación, combinación, análisis, acceso, búsqueda y presentación de contenido digital, incluido el desarrollo de servicios y aplicaciones aplicables a la materia de gobierno digital"* (subrayado y negrita agregada).

[3] Hernández Rodríguez, Rafael y otros. *"Glosario informático. Compendio de términos informáticos"*. México: Universidad de Guadalajara, 2018, p. 96

[4] INSTITUTO NACIONAL DE CIBERSEGURIDAD. *"Seguridad en redes wifi: una guía de aproximación para el empresario"*. p.6. Disponible en: https://acortar.link/uOsjlZ

7. Si bien las principales ventajas de la tecnología *"wifi"* radica en la flexibilidad de la instalación de los equipos en cuanto a su ubicación, salvo la distancia para evitar una excesiva atenuación de la señal; y, la movilidad de los equipos y usuarios, necesidad muy demanda en la actualidad, no está exenta de riesgos asociados a su uso, por lo que, sus titulares deben adoptar algunas medidas de seguridad para evitar que los ciberatacantes se filtren en ellas y tomen dominio de los dispositivos conectados[5].

8. Justamente, una de estas medidas de seguridad consiste en implementar *"procesos de autenticación para los usuarios"*, de tal modo que el acceso a la red *wifi* se realice previo ingreso de *"contraseñas o claves de acceso",* las cuales son códigos creados para acceder a un sistema restringido que contienen caracteres alfanuméricos e incluso algunos otros símbolos[6]*.* En caso de que el usuario no ingrese la clave correcta no se permitirá el acceso a *la red wifi.* Estas contraseñas o claves de acceso deben ser lo más robustas posibles[7].

9. Ahora bien, a juicio de la Autoridad Nacional de Protección de Datos Personales[8], no adoptar dichas medidas de seguridad *o entregar la contraseña de acceso a la red wifi a cualquier persona que la requiera (o hacerla pública)*, sin tener un esquema de control, imposibilita tener certeza respecto de la trazabilidad de las acciones realizadas en la red, incrementado los riesgos de ciberataques, máxime si la red de internet *"wifi" es uno de los componentes de arquitectura más vulnerables de cualquier institución*, por cuanto permite el acceso de dispositivos desconocidos a la red, con implicaciones y fines desconocidos. Por ello, compartir el acceso de una red de forma pública presenta los siguientes riesgos:

   - Robo de información transmitida.
   - Robo de información almacenada.
   - Infección por *malware*[9].

---

[5] INSTITUTO NACIONAL DE CIBERSEGURIDAD. *"Seguridad en redes wifi: una guía de aproximación para el empresario"*. p.4. Disponible en: https://acortar.link/uOsjlZ Asimismo, véase el documento denominado *"Redes de Ordenadores"*, P. 17. Disponible en: https://acortar.link/LNX7d

[6] HERNÁNDEZ RODRÍGUEZ, Rafael y otros. *"Glosario informático. Compendio de términos informáticos".* México: Universidad de Guadalajara, 2018, p. 52.

[7] Tipo de contraseña que se caracteriza por ser suficientemente larga, que se crea al azar o mediante la combinación de caracteres alfanuméricos (letras mayúsculas y minúsculas, números y caracteres especiales) que dificultan de forma clara su revelación, ya que se requiere un tiempo elevado de cálculo para lograrlo. INSTITUTO NACIONAL DE CIBERSEGURIDAD. Glosario de términos de ciberseguridad: Una guía de aproximación para el empresario. P.30. Disponible en: https://acortar.link/n6QkaD

[8] Informe Jurídico N° 03-2022-DGTAIPD. *"Sobre Proyecto de Ley N° 878/2021-CR que propone la Ley General de Internet"*. Disponible en: https://acortar.link/B9lmQZ

[9] Malware *"es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. (…) Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, troyanos, backdoors, spyware, etc. La nota común a todos estos programas es su carácter dañino o lesivo"*. INSTITUTO NACIONAL DE CIBERSEGURIDAD. *Glosario de términos de ciberseguridad: Una guía de aproximación para el empresario*. P.56. Disponible en: https://acortar.link/n6QkaD

- Uso ilegal de la red.

10. Es, seguramente, por estas razones, que la *"seguridad"* o *"seguridad digital"*, como atributo de las tecnologías digitales, está presente en diversos artículos del Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital, su Reglamento[10] y el Decreto de Urgencia Nº 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento. Incluso la Secretaría de Gobierno y Transformación Digital, ente rector en materia de gobierno digital, que comprende, entre otros, a la seguridad digital, emitió la Resolución N° 003-2023-PCM/SGTD, que establece la implementación y mantenimiento del sistema de gestión de seguridad de la información en las entidades públicas.

11. Por otro lado, es preciso indicar que entregar la contraseña de acceso a una red de internet *wifi* a cualquier persona que la requiera *o hacerla pública*, también tendría como efecto sobrecargar excesivamente la red, debido a la conexión simultánea de diversos usuarios, a tal punto que la torne lenta y dificulte realizar *eficazmente las funciones de la institución titular de dicha red*, sobre todo, si se trata de una red de internet *"wifi"* de una entidad pública (es decir, de titularidad pública), contratada con recursos públicos y para el ejercicio de funciones públicas (*y no para satisfacer la necesidad de acceder a internet de los particulares*)[11], cuya finalidad, tal como se ha indicado *ut supra*, es beneficiar a los ciudadanos mediante la prestación *eficaz* de más y mejores servicios públicos, particularmente, mediante el uso intensivo de las *"tecnologías digitales".*

12. Finalmente, entregar la contraseña de acceso a una red de internet *wifi* a cualquier persona que la requiera o hacerla pública, en tanto es un código creado para acceder a un sistema restringido, *vulneraría la confidencialidad que posee cualquier contraseña como característica inherente* (es decir, que por su propia naturaleza no puede ser pública), circunstancia que, al ser un hecho notorio, no debería requerir de probanza alguna, de acuerdo a lo dispuesto por el artículo 176 del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aun cuando la carga de la prueba sobre su confidencialidad recaiga en quien posea dicha información[12], esto es, la entidad pública titular de la red de internet *"wifi".*

---

[10] Aprobado por Decreto Supremo N° 029-2021-PCM.

[11] Incluso en las mismas entidades existen prohibiciones para que los servidores públicos usen el internet en fines ajenos al cumplimiento de sus funciones como, por ejemplo, acceder a redes sociales o material para adultos, entre otras prohibiciones. Así, puede verse la Directiva N° 009-2018-MIDIS/PNPAIS-UTI *"Normas para el acceso a la red y uso de internet en el Programa Nacional Plataformas de Acción para la Inclusión Social-PAIS".* Disponible en: https://acortar.link/k4eZWz La Directiva N° 001-2020-UIEST/MDM *"Directiva que norma el adecuado uso del servicio de internet y correo electrónico institucional en la Municipalidad Distrital de Motupe".* Disponible en: https://acortar.link/nSNcT

[12] **Artículo 176.- Hechos no sujetos a actuación probatoria**
No será actuada prueba respecto a hechos públicos o notorios, respecto a hechos alegados por las partes cuya prueba consta en los archivos de la entidad, sobre los que se haya comprobado con ocasión del ejercicio de sus funciones, o sujetos a la presunción de veracidad, sin perjuicio de su fiscalización posterior.

B. *Sobre la flexibilización del régimen de excepciones para cautelar información que no debería entregarse por afectar otros principios dignos de tutela: a propósito de la atención de las solicitudes de contraseñas de las redes de internet "wifi" de titularidad pública, contratadas con recursos públicos y para el ejercicio de funciones públicas*

13. En virtud del principio de publicidad, regulado en el artículo 3 del Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública[13] (en adelante, TUO de la LTAIP), toda información obrante en las entidades se presume de acceso público, por lo que las entidades deben entregarla a quien la solicite, salvo que ella esté comprendida en algún supuesto de excepción regulado por los artículos 15, 16 o 17 del TUO de la LTAIP. Por ende, si la información requerida no se subsume en cualquiera de estos artículos deberá confirmarse su naturaleza pública y entregarse, sin mayores cuestionamientos. El análisis de subsunción se realiza bajo una interpretación restrictiva[14].

14. Sin embargo, también debe tenerse presente que el Legislador no es un ser omnisciente, por ello, al momento de regular el régimen de excepciones (artículos 15, 16 y 17 del TUO de la LTAIP), pudo, eventualmente, *no haber previsto todos los supuestos posibles de información protegida que puedan presentarse según cada momento determinado* (incluso que dichos supuestos merecedores de protección no sean cubiertos vía la remisión que efectúa el artículo 17 inciso 6 del TUO de la LTAIP a normas especiales[15]). Asimismo, tampoco pudo haber previsto las eventuales colisiones del derecho de acceso a la información pública con otros principios de máximo orden y dignos de legítima tutela.

15. Por ello, esta Autoridad Nacional, en reiteradas oportunidades[16], ha sostenido que de existir alguna información que deba ser excluida del acceso y conocimiento

---

[13] Aprobado por Decreto Supremo N° 021-2019-JUS.
[14] Artículo 18 del TUO de la LTAIP.
[15] El artículo 17 inciso 6 del TUO de la LTAIP considera como información confidencial *"aquellas materias cuyo acceso esté expresamente exceptuado por la Constitución o por una Ley aprobada por el Congreso de la República"*. De acuerdo con esta Autoridad también puede crearse supuestos de información confidencial a través de Decreto Legislativos. Opinión Consultiva N° 30-2019-JUS/DGTAIPD. *"Respecto al acceso a la información contenida en actas de sesiones de un órgano colegiado y en actas de un procedimiento administrativo sancionador y las excepciones al acceso público en virtud de lo establecido en el inciso 6 del artículo 17 de la Ley 27806"*. Disponible en: https://acortar.link/PqblJ3
[16] Así pueden verse los siguientes pronunciamientos:
- Opinión Consultiva N° 31-2018-JUS/DGTAIPD. *"Si la relación de «Activos de Información» que se encuentra en posesión o control de la Gerencia de Informática y Tecnología Electoral de la Oficina Nacional de Procesos Electorales puede ser información clasificada como excepción al acceso a la información pública"*. Disponible en: https://acortar.link/SDAHiq
- Opinión Consultiva N° 25-2022-JUS/DGTAIPD. *"Acceso a la información obtenida por la SUTRAN vía transmisión desde los sistemas de control y monitoreo inalámbrico de los vehículos de transporte de personas y mercancías, en el marco de sus funciones de supervisión"*. Disponible en: https://acortar.link/S7hMEs

público a efecto de cautelar otros bienes jurídicos relevantes del máximo orden corresponderá a las entidades, al momento de la atención de la solicitud de información pública, integrar en su análisis el principio de proporcionalidad y razonabilidad regulado por el artículo 200 *in fine* de la Constitución Política.

16. La aplicación de este principio (y los principios que lo integran: idoneidad, necesidad y proporcionalidad *stricto sensu*) permitirá modular el carácter restrictivo del régimen de excepciones y limitar el derecho de acceso a la información pública evitando que se acceda a toda aquella información cuya entrega, en los hechos, afecte otros bienes jurídicos dignos de tutela más allá del régimen de excepciones, es decir, de los supuestos comprendidos en los artículos 15, 16 o 17 del TUO de la LTAIP.

17. En ese marco, las contraseñas de las redes de internet *"wifi"* de titularidad pública, contratadas con recursos públicos y para el ejercicio de funciones públicas, no podrán ser entregadas a cualquier persona que lo requiera, si luego de la aplicación del principio de proporcionalidad y razonabilidad en el caso concreto, la entidad requerida determina que, entre el derecho de acceso a la información pública y *"la seguridad o seguridad digital"*, así como *"la eficacia de la actuación administrativa"*[17], principios, desarrollados ampliamente en el acápite A de la presente opinión, deben ser satisfechos u optimizados los últimos respecto del primero (derecho); máxime, si su entrega vulnera la confidencialidad (o tiene el potencial de hacerlo) que posee toda contraseña como característica inescindible y evidente.

18. Tratamiento distinto cabe respecto a las contraseñas de las redes de internet *"wifi"* de titularidad pública o parcialmente pública, contratadas con recursos públicos o no, ubicadas en espacios públicos *e implementadas por las entidades para garantizar el derecho de acceso al internet, reconocido en el artículo 14-A de la Constitución*[18], cuya interpretación de sus alcances no corresponde a esta

---

- Informe Jurídico N° 25-2022-JUS/DGTAIPD. *"Sobre la naturaleza pública de la información contenida en correos electrónicos institucionales, excepción de información reservada y alcances del término información"*. Disponible en: https://acortar.link/hlPZOX
- Opinión Consultiva N° 27-2023-JUS/DGTAIPD. *"Sobre la naturaleza de la información referida a las investigaciones y estudios realizadas por el IMARPE y la aplicación de las excepciones previstas en el artículo 17, numeral 1 y el artículo 16, numeral 2 literal a) del TUO de la LTAIP"*. Disponible en: https://acortar.link/7mIMlJ

[17] La doctrina apunta que *"el principio de eficacia de la actuación administrativa puede constituir, en ocasiones, un límite legítimo al alcance del principio de transparencia, pues es cierto que la eficacia de la administración precisa ciertos umbrales de confidencialidad (temporal)"*. (subrayado agregado)". FERNÁNDEZ RAMOS, Severiano. Algunas proposiciones para una Ley de Acceso a la Información. En: Boletín Mexicano de Derecho Comparado. Año XXV. Número 105. México: UNAM, 2002, p. 887.
El principio de eficacia también ha sido recogido en el artículo III literal b) de la Ley N° 30057, Ley del Servicio Civil en los siguientes términos: *"el Servicio Civil y su régimen buscan el logro de los objetivos del Estado y la realización de prestaciones de servicios públicos requeridos por el Estado (…)"*. De igual modo, en el artículo 4 de los Lineamientos de Organización del Estado, aprobado por Decreto Supremo N° 054-2018-PCM en los siguientes términos: *"las entidades se organizan para asegurar el cumplimiento de políticas, estrategias, metas y resultados"*.

[18] **Artículo 14-A.** El Estado garantiza, a través de la inversión pública o privada, el acceso a internet libre en todo el territorio nacional, con especial énfasis en las zonas rurales, comunidades campesinas y nativas".

Autoridad. No obstante, a modo de ejemplo, puede citarse las siguientes medidas adoptadas por algunas entidades: *"Internet wifi gratuito para todos los vecinos de SJL"*[19], *"Municipalidad de La Victoria ofrece WIFI gratis en 10 parques del distrito"*[20], "*Miraflores Wi-Fi"*[21], *"Disfruta de nuestra red WIFI Municipalidad Distrital de Lurín"*[22], entre otras.

19. Estas contraseñas, teniendo en cuenta que la finalidad de las redes internet *"wifi"* a la que permiten acceder es promover el derecho del acceso al internet y la reducción de la brecha digital, no generan los riesgos advertidos en el acápite A de la presente opinión para las entidades ni tampoco dificultarían el cumplimiento eficaz de sus funciones. Por ello, no solo debería ser entregado a cualquier persona que lo solicite ejerciendo su derecho de acceso a la información pública, sino incluso difundirse a través de cualquier medio dispuesto por la entidad a efecto de que su acceso se realice en condiciones de igualdad.

C. *Sobre la inviabilidad de denegar o entregar información alegando condiciones subjetivas del solicitante como la pertenencia o no a la entidad requerida u ostentar alguna afiliación institucional*

20. El artículo 7 del TUO de la LTAIP dispone que, "*toda persona tiene derecho a solicitar y recibir información de cualquier entidad de la Administración Pública. En ningún caso se exige expresión de causa para el ejercicio de este derecho*. Como correlato, el artículo 13 del TUO de la LTAIP establece que "*la entidad de la Administración Pública a la cual se solicite información no podrá negar la misma basando su decisión en la identidad del solicitante". (subrayado y negrita agregada).

21. Las disposiciones citadas no reconocen como titulares del derecho de acceso a la información pública a personas que ostentan determinada cualidad subjetiva, sino a *"toda persona"*, por lo que estamos frente a un derecho de titularidad universal. Esto implica que la decisión de denegar o entregar información únicamente debe estar basada en la aplicación o inaplicación de las excepciones de los artículos 15, 16 y 17 del TUO de LTAIP o, como se indicó en el acápite B de la presente opinión, en la imperiosa necesidad de cautelar otros principios dignos de tutela.

22. Por ende, la denegatoria de las solicitudes de contraseñas de las redes de internet *"wifi"* de titularidad pública, contratadas con recursos públicos y para el ejercicio de funciones públicas no puede estar justificada en la ausencia de alguna condición

---

(subrayado agregado). Anteriormente, el Tribunal Constitucional ya había sostenido que *"…le corresponde al Estado garantizar un acceso mínimo a los servicios de agua, energía eléctrica e internet, a todas las personas, particularmente a los más necesitados y a aquellos que viven en situación de extrema pobreza"* (subrayado agregado). Sentencia recaída en el Expediente N° 02151-2018-PA/TC.

[19] Mayores detalles en el siguiente enlace: https://acortar.link/1Iqp7w
[20] Mayores detalles en el siguiente enlace: https://acortar.link/Uj2opS
[21] Mayores detalles en el siguiente enlace: https://acortar.link/aHFVmR
[22] Mayores detalles en el siguiente enlace: https://acortar.link/jZRDqF

subjetiva por el solicitante como, por ejemplo, no pertenecer a la entidad requerida o carecer de afiliación institucional, sino en el régimen de excepciones o la imperiosa necesidad de cautelar otros principios merecedores de legítima tutela.

23. Lo mismo sucede tratándose de información de carácter público, como las contraseñas de las redes de internet *"wifi"* implementadas por las entidades para garantizar el derecho de acceso al internet, en cuyo caso, *debe entregarse a cualquier persona que la requiera*, sin perjuicio de que pertenezca o no a la entidad requerida o esté afiliada institucionalmente a ella.

IV. CONCLUSIONES

1. Las entidades públicas recurren a las tecnologías digitales como el internet, cuya conexión puede realizarse mediante el cableado o por la tecnología *"wifi"*. Si bien esta tecnología reporta ventajas, no está exenta de riesgos, por lo que sus titulares deben adoptar algunas medidas de seguridad como los *"procesos de autenticación"*, de modo que el acceso a la red *wifi* se realice mediante el ingreso *"contraseñas o claves".*

2. No adoptar procesos de autenticación a la red *wifi* o entregar la contraseña a cualquier persona que la requiera o hacerla pública, incrementa los riesgos de ciberataques (robo de información transmitida y de información almacenada, infección por malware o uso ilegal de la red), por cuanto, la red "*wifi"* es uno de los componentes de arquitectura más vulnerables. Por ello, la *"seguridad"* o *"seguridad digital"* está prevista en la normativa nacional de gobierno digital.

3. Entregar la contraseña de una red de internet *wifi* a cualquier persona que la requiera o hacerla pública, también sobrecarga dicha red, dificultando así realizar eficazmente las funciones por la entidad que lo contrató con cargo a sus recursos, *para el ejercicio de sus funciones públicas*; y, no para brindar servicio de internet a los particulares. Incluso vulnera la confidencialidad natural y evidente que posee cualquier contraseña o tiene el potencial de hacerlo.

4. Las entidades pueden denegar las solicitudes de contraseñas de las redes de internet *"wifi"* de titularidad pública, contratadas con recursos públicos y para el ejercicio de funciones públicas, si aplicando el principio de proporcionalidad y razonabilidad en el caso concreto, determinan la prevalencia de otros principios dignos de legítima tutela como *"la seguridad o seguridad digital"* y *"la eficacia de la actuación administrativa"*, los que podrán ser optimizados en perjuicio del derecho de acceso a la información pública, máxime si entregarla también vulnera la confidencialidad (o tiene el potencial de hacerlo) que posee toda contraseña como característica inherente y evidente.

5. La denegatoria de las solicitudes de contraseñas de las redes de internet *"wifi"* de titularidad pública, contratadas con recursos públicos y para el ejercicio de funciones públicas, de corresponder, únicamente puede estar motivada en las excepciones de los artículos 15, 16 y 17 del TUO de LTAIP o, como se indicó en el acápite B de la presente opinión, en la imperiosa necesidad de cautelar otros principios dignos de tutela. No puede estar justificada en la ausencia de una condición subjetiva del solicitante.

6. Las contraseñas de las redes de internet *"wifi"* implementadas por las entidades en espacios públicos para garantizar el derecho de acceso al internet y reducir la brecha digital, pueden ser entregadas a cualquier persona que la requiera ejerciendo su derecho de acceso a la información pública, sin perjuicio de que pertenezca o no a la entidad requerida o esté afiliada institucionalmente a ella, incluso debería difundirse a efecto de que su acceso se realice en condiciones de igualdad.

Aprobado por:	**Aprobado por:**
PERÚ MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS Firmado digitalmente por LUNA CERVANTES Eduardo Javier FAU 20131371617 soft **Eduardo Luna Cervantes** Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales	PERÚ MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS Firmado digitalmente por AGUILA SALAZAR Marcia Anabel FAU 20131371617 soft Fecha: 2025.01.24 12:32:04 -05'00' **Marcia Aguila Salazar** Directora (e) de la Dirección de Transparencia y Acceso a la Información Pública