RESOLUCIÓN FINAL Nº 0026-2026/INDECOPI-CHT

DELEGACIÓN : **PROTECCIÓN AL CONSUMIDOR**
PROCEDENCIA : **ÓRGANO RESOLUTIVO DE PROCEDIMIENTOS SUMARÍSIMOS DE PROTECCIÓN AL CONSUMIDOR DE LA OFICINA REGIONAL DEL INDECOPI ÁNCASH – SEDE CHIMBOTE**
DENUNCIANTE : [redacted]
DENUNCIADO : **BANCO BBVA PERÚ S.A.**
MATERIA : **DEBER DE IDONEIDAD**
ACTIVIDAD : **OTROS TIPOS DE INTERMEDIACIÓN MONETARIA**

Chimbote, 20 de febrero de 2026

I. ANTECEDENTES

1. El 06 de junio de 2025, la señora [redacted][1] denunció a Banco BBVA Perú S.A. (en adelante el Banco)[2]; por infracción a la Ley 29571, Código de Protección y Defensa del Consumidor (en adelante, el Código)[3].

2. Mediante Resolución N° 01 del 27 de agosto de 2025, el Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor de la Oficina Regional del INDECOPI Áncash – Sede Chimbote (en adelante ORPS) [4] decidió iniciar procedimiento administrativo sancionador contra el Banco, de acuerdo al siguiente detalle:

> ***"PRIMERO:*** *Iniciar procedimiento administrativo sancionador contra el Banco BBVA Perú S.A. por presunta infracción a lo establecido en el artículo 195 del Código de Protección y Defensa del Consumidor, toda vez que no habría adoptado las medidas de seguridad necesarias para evitar que el 11 y 12 de abril del 2025, se realicen cuatro (04) operaciones por el importe total de S/ 5 700,00 con cargo a la Tarjeta de Débito* [redacted] *de titularidad de la denunciante, pues no fueron realizadas por su persona, y no corresponden a su comportamiento habitual, conforme al siguiente detalle:*

Fecha	*Detalle de transacción*	*Importe*
11/04/2025	**PAGOEFECTIVO SOLES*	*S/ 1 500,00*
11/04/2025	**PAGOEFECTIVO SOLES*	*S/ 1 000,00*
11/04/2025	**PAGOEFECTIVO SOLES*	*S/ 1 200,00*
12/04/2025	**PAGOEFECTIVO SOLES*	*S/ 2 000,00"*

1 DNI N° 10391758

2 RUC N° 20100130204

3 **LEY N° 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR**, publicado el 2 de septiembre de 2010 en el Diario Oficial El Peruano. Dicho código será aplicable a los supuestos de infracción que se configuren a partir del 2 de octubre de 2010, fecha en la cual entró en vigencia el mismo.

4 Ingreso en Comisión Nº 0085-2025-AP/CPC-INDECOPI-CHT

5 **LEY N° 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR**
Artículo 19.- Obligación de los proveedores
El proveedor responde por la idoneidad y calidad de los productos y servicios ofrecidos, por la autenticidad de las marcas y leyendas que exhiben sus productos o del signo que respalda al prestador del servicio, por la falta de conformidad entre la publicidad comercial de los productos y servicios y estos, así como por el contenido y la vida útil del producto indicado en el envase, en lo que corresponda.

3. El 11 de septiembre de 2025, el Banco presentó sus descargos, a través del cual, señaló lo siguiente:

(i) La denunciante no habría presentado ningún medio probatorio, ni si siquiera a nivel indiciario, que acredite no haber realizado las operaciones que no reconoce.
(ii) Las operaciones cuestionadas se realizaron a través de su Banca Móvil. En tal sentido, presentó el "Log afiliaciones", donde se verificaría que, al momento de la realización de las operaciones, la denunciante se encontraba correctamente enrolada, y con Token Digital como medida de seguridad para la validación de las transacciones.
(iii) En el "Histórico de Afiliaciones" se verificaría que, en el momento de la operación cuestionada, la denunciante contaba con el mecanismo de seguridad *Soft Token*, el cual es el encargado de generar las claves criptográficas para cada operación.
(iv) La usuaria habría iniciado sesión de manera válida en su Banca Móvil con sus credenciales, esto es, su DNI y clave de acceso, hecho que habría quedado registrado en su "Log Inicio de Sesión".
(v) Para la autorización de las operaciones de transferencia, se habría utilizado un código único de autenticación (CUA), al cual le denominan clave token, la misma que sería generada a partir de los datos de cada operación solicitada, es decir, de manera individual.
(vi) A través del "Log validación del token digital" se acreditaría la generación de un Código Único de Autenticación Criptográfica, a partir de los datos específicos de cada operación materia de denuncia, cumpliéndose así con tener un control ante ataques de hombre en el medio.
(vii) El Código Único de Autenticación debe ser obtenido luego de que el cliente siguió el procedimiento para efectuar una determinada transacción, pero de forma previa a la confirmación de que ésta ha sido autorizada, lo cual ocurriría antes de la ejecución final de la operación.
(viii) En el Reglamento de Ciberseguridad no existiría una prohibición o impedimento para que el Código Único Criptográfico pueda servirse o derivarse de alguno de alguno de los factores de autenticación que son utilizados por el Banco como parte de su procedimiento de autenticación reforzada.
(ix) Habrían procesado de manera válida la operación cuestionada, por lo que presentaron el Sistema Informático denominado "Log Canal", sistema que registraría todas las operaciones realizadas.
(x) Respecto al primer paso del proceso de autenticación reforzada, se encontraría acreditado que el Banco utilizó una combinación de dos factores de autenticación que corresponderían a categorías diferentes y serían independientes entre sí. Ello, en tanto el Banco cumplía con emplear: (i) la credencial o contraseña de acceso de seis dígitos; y (ii) el *Softoken* o Token digital de software activado como fuente o semilla.
(xi) El Softtoken o Token Digital sería un mecanismo de seguridad instaurado para que sus clientes lo puedan utilizar para concretar operaciones bancarias desde la Banca por Internet o Banca Digital. Dicho mecanismo se compondría de dos piezas: la parte servidora y la parte cliente, siendo esta última la que se encontraría instalada en el aplicativo móvil del Banco alojado en el celular del cliente.
(xii) Cumplió con notificar válidamente la operación a la señora Obo, tal como la misma denunciante habría reconocido expresamente en su escrito de denuncia. En tal sentido, presento el medio probatorio "Constancias de notificación".

(xiii) De acuerdo al Estado de Cuenta, las operaciones cuestionadas se encontrarían dentro del patrón de consumo de la denunciante, realizándose operaciones incluso por importes mayores.

4. Por escrito del 23 de octubre de 2025, la señora Obo presentó los estados de cuenta de los meses de abril 2024 a marzo de 2025.

5. Por Resolución Final N° 0156-2025/PS0-INDECOPI-CHT del 31 de octubre de 2025, el ORPS decidió lo siguiente:

> *"**PRIMERO:** Sancionar a Banco BBVA Perú S.A. con multa de 3,78 UIT20 por haber incurrido en infracción a lo establecido en el artículo 19 del Código de Protección y Defensa del Consumidor, al haberse acreditado que permitió que en forma indebida el 11 y 12 de abril de 2025, se realicen cuatro (04) operaciones por el importe total de S/ 5 700,00 con cargo a la Tarjeta de Débito N° 4551-03**-****-7308, de titularidad de la denunciante, según el siguiente detalle:*
>
> | Fecha | Detalle de transacción | Importe |
> |---|---|---|
> | 11/04/2025 | *PAGOEFECTIVO SOLES | S/ 1 500,00 |
> | 11/04/2025 | *PAGOEFECTIVO SOLES | S/ 1 000,00 |
> | 11/04/2025 | *PAGOEFECTIVO SOLES | S/ 1 200,00 |
> | 12/04/2025 | *PAGOEFECTIVO SOLES | S/ 2 000,00" |
>
> ***SEGUNDO:** Requerir a Banco BBVA Perú S.A. el cumplimiento espontáneo de la multa21, de conformidad con lo establecido en el numeral 4 del artículo 205 del Texto Único Ordenado de la Ley del Procedimiento Administrativo General22, bajo apercibimiento de iniciarse el procedimiento de ejecución coactiva respectivo. El sancionado sólo pagará el 75% de la multa si consiente la presente resolución y procede a cancelarla en un plazo no mayor a quince (15) días hábiles contados a partir del día siguiente de la notificación de la presente Resolución, conforme a lo establecido en el artículo 113 del Código de Protección y Defensa del Consumidor.*
>
> ***TERCERO:** Ordenar al Banco BBVA Perú S.A. como medida correctiva que, en un plazo de quince (15) días hábiles, contados a partir del día siguiente de notificada la presente resolución, cumpla con devolver a la denunciante el importe total de S/ 5 700,00 que corresponde a las cuatro (04) operaciones cuestionadas del 11 y 12 de abril de 2025, efectuadas con cargo a su Tarjeta de Débito N° [redacted].*
>
> *Banco BBVA Perú S.A. deberá acreditar el cumplimiento de lo dispuesto en el presente artículo, ante este Órgano Resolutivo, en el plazo máximo de cinco (5) días, contados a partir del vencimiento de plazo otorgado en el párrafo precedente, bajo apercibimiento de imponerle una multa coercitiva por incumplimiento de mandato, conforme a lo señalado en el artículo 117 del Código de Protección y Defensa del Consumidor y en los términos y condiciones indicados en la presente resolución.*
>
> ***CUARTO:** Ordenar a Banco BBVA Perú S.A. al pago de las costas del procedimiento y disponer que en un plazo no mayor a quince (15) días hábiles contado a partir del día siguiente de la notificación de la presente resolución, cumpla con el pago de las costas de esta instancia a la denunciante ascendente a S/ 36,00, sin perjuicio del derecho de ésta de solicitar la liquidación de los costos una vez concluida la instancia administrativa. La*

evaluación de las solicitudes de liquidación estará a cargo del Órgano Resolutivo de Procedimientos Sumarísimos competente.

***QUINTO:** La presente resolución tiene vigencia desde el día de su notificación y no agota la vía administrativa. En tal sentido, se informa que de conformidad con lo dispuesto en el numeral 32.1 de la Directiva N° 001-2021/DIR-COD-INDECOPI, contra lo dispuesto por la presente jefatura procede el recurso impugnativo de apelación. Cabe señalar que dicho recurso deberá ser presentado ante el Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor de la Oficina Regional del Indecopi Ancash –Sede Chimbote en un plazo máximo de quince (15) días hábiles contados a partir del día siguiente de su notificación25, caso contrario la resolución quedará consentida."*

6. El 21 de noviembre de 2025, el Banco impugnó la Resolución Final N° 0156-2025/PS0-INDECOPI-CHT, manifestando lo siguiente:

(i) Sobre que, el Banco que permitió que en forma indebida el 11 y 12 de abril de 2025, se realicen cuatro (04) operaciones por el importe total de S/ 5 700,00 con cargo a la Tarjeta de Débito N° [redacted], de titularidad de la denunciante;
(ii) la Comisión ha señalado que su decisión se debe a que, el token no puede ser utilizado como segundo factor de autenticación y al mismo tiempo como código de autenticación mediante método criptográfico;
(iii) la autoridad ha realizado una interpretación incorrecta sobre los argumentos y medios probatorios presentados, pues ha entendido que, la clave token digital es un factor de autenticación y al mismo tiempo el código de autenticación, no obstante, esto se adecua a la realidad;
(iv) tal como se refirió en nuestro escrito de descargos, por un lado, tenemos el "Token Digital" el cual es el sistema de seguridad fuente el cual nuestros clientes POSEEN (tal como requiere el artículo 19 del Reglamento de Ciberseguridad), este elemento cumple la función del segundo factor de autenticación;
(v) Ahora bien, por otro lado, tenemos el OTP o "One Time Password" generado a partir del Token Digital. En tal sentido, el Soft Token o Token Digital (que posee el cliente) genera una respuesta y utiliza el OPT para realizar una autenticación exitosa;
(vi) En tal sentido, mal podría comprenderse que el Token Digital (parte servidora) y el OTP (código de autenticación de un solo uso) son lo mismo, pues se requiere de ambos en conjunto para validar correctamente el procesamiento de una operación.
(vii) Así, si el cliente tuviera activo el Token Digital pero no se generará válidamente el OTP no podría procesarse correctamente una operación.
(viii) No debe pasar desapercibido que, en nuestro escrito de descargos se presentó ante la autoridad – de manera confidencial – nuestro Informe de Ciberseguridad, en virtud del cual se explicó de manera técnica en qué consiste esta clave digital, cuál es su arquitectura digital y, finalmente, cuál es su funcionalidad dentro los canales digitales que son utilizados por nuestros clientes;
(ix) En consecuencia, parece ser que la interpretación de parte de la Comisión responde a una revisión parcial o incorrecta de nuestros medios probatorios, ignorando incluso que, en nuestro escrito de descargos hayamos hecho

referencia DIRECTA a que, el Softoken y la Clave no son lo mismo, sino factores diferentes;

(x) la Comisión también ha señalado – a pesar de que se presentaron válidamente las constancias de notificación de cada una de las operaciones – que el Banco no habría acreditado que el correo [redacted] sea de titularidad de la denunciante;

(xi) no se ha tomado en consideración que ha sido la misma denunciante quien ha incluido – a puño y letra - esta dirección electrónica en su escrito de denuncia;

(xii) carece de sentido que la Comisión desconozca un hecho que ha sido aceptado y convalidado por la misma denunciante;

(xiii) este hecho resulta inmotivado y genera que la decisión emitida por la autoridad sea totalmente arbitraria, por todo lo expuesto, corresponderá a la Sala revocar la Resolución cuestionada y declarar infundada la denuncia en todos sus extremos;

(xiv) la multa total de 3.78 UIT resulta desproporcionada y arbitraria a la materia discutida, y carecen de motivación, lógica y asidero jurídico; viola el denominado Principio de Razonabilidad y Presunción de Licitud; por lo que, solicitan a la Comisión desestimar el análisis de la Comisión en el extremo señalado y conforme a sus atribuciones deje sin efecto la sanción impuesta;

(xv) el Banco no cometió infracción alguna, corresponde a la Sala no dictar ningún tipo de medida correctiva;

(xvi) teniendo en cuenta que el Banco no cometió infracción alguna en referencia a la denuncia presentada y por consiguiente solicitan que, conforme a sus atribuciones deje sin efecto la Resolución respecto del pago de costas y costos del procedimiento;

(xvii) existe un daño patrimonial al haber multado al Banco inmotivadamente con 3.78 UIT, debiéndose declarar la nulidad de la Resolución Final materia de apelación, y declarar infundada la denuncia en todos sus extremos.

7. El 30 de diciembre de 2025, a través del Memorándum N° 0236-2025/PS0-INDECOPI-CHT, el ORPS remitió el expediente a la Comisión de la Oficina Regional del Indecopi Ancash – Sede Chimbote (en adelante, La Comisión).

II. ANÁLISIS

Sobre el deber de idoneidad

8. El artículo 18 del Código establece que la idoneidad es la correspondencia entre lo que un consumidor espera y lo que efectivamente recibe[6].

9. Por su parte, el artículo 19 del Código establece que los proveedores son responsables por la calidad e idoneidad de los productos y servicios que ofrecen en

6 **LEY 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR**
Artículo 18.- Idoneidad
Se entiende por idoneidad la correspondencia entre lo que un consumidor espera y lo que efectivamente recibe, en función a lo que se le hubiera ofrecido, la publicidad e información transmitida, las condiciones y circunstancias de la transacción, las características y naturaleza del producto o servicio, el precio, entre otros factores, atendiendo a las circunstancias del caso.
La idoneidad es evaluada en función a la propia naturaleza del producto o servicio y a su aptitud para satisfacer la finalidad para la cual ha sido puesto en el mercado.
Las autorizaciones por parte de los organismos del Estado para la fabricación de un producto o la prestación de un servicio, en los casos que sea necesario, no eximen de responsabilidad al proveedor frente al consumidor.

el mercado[7]. En aplicación de esta norma, los proveedores tienen el deber de entregar los productos y prestar los servicios al consumidor en las condiciones informadas o previsibles, atendiendo a la naturaleza de estos, la regulación que sobre el particular se haya establecido y, en general, a la información brindada por el proveedor o puesta a disposición.

10. Ante la denuncia de un consumidor insatisfecho que pruebe el defecto de un producto o servicio, se presume iuris tantum que el proveedor es responsable por la falta de idoneidad calidad del producto o servicio que pone en circulación en el mercado. Sin embargo, el proveedor podrá demostrar su falta de responsabilidad desvirtuando dicha presunción, es decir, acreditando que empleó la diligencia requerida en el caso concreto (y que actuó cumpliendo con las normas pertinentes) o probando la ruptura del nexo causal por caso fortuito, fuerza mayor, hecho determinante de un tercero o negligencia del propio consumidor afectado.

Aplicación al caso concreto

11. En el presente caso, el señor Obo denunció al Banco porque no habría adoptado las medidas de seguridad necesarias para evitar que el 11 y 12 de abril del 2025, se realicen cuatro (04) operaciones por el importe total de S/ 5 700,00 con cargo a la Tarjeta de Débito N° [redacted], de titularidad de la denunciante, pues no fueron realizadas por su persona, y no corresponden a su comportamiento habitual, conforme al siguiente detalle:

Fecha	Detalle de transacción	Importe
11/04/2025	*PAGOEFECTIVO SOLES	S/ 1 500,00
11/04/2025	*PAGOEFECTIVO SOLES	S/ 1 000,00
11/04/2025	*PAGOEFECTIVO SOLES	S/ 1 200,00
12/04/2025	*PAGOEFECTIVO SOLES	S/ 2 000,00

12. En primera instancia, el ORPS sancionó al Banco, en tanto consideró que quedó acreditado que permitió que en forma indebida el 11 y 12 de abril de 2025, se realicen cuatro (04) operaciones por el importe total de S/ 5 700,00 con cargo a la Tarjeta de Débito N° [redacted]8, de titularidad de la denunciante.

13. En su escrito de apelación, el Banco cuestionó únicamente dos puntos de la resolución, respecto de los cuales habrían sido malinterpretados: (i) la clave token digital, fue considerada que es un factor de autenticación y al mismo tiempo el código de autenticación, no obstante, esto no se adecua a la realidad, pues el token genera la clave OTP o “One Time Password”, para realizar una autenticación exitosa; asimismo, cuestionó (ii) el correo [redacted] al cual remitieron las constancias de notificación de las operaciones, el cual ha sido la misma denunciante quien ha incluido dicha dirección electrónica en su escrito de denuncia.

7 **LEY N° 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR**
Artículo 19.- Obligación de los proveedores
El proveedor responde por la idoneidad y calidad de los productos y servicios ofrecidos; por la autenticidad de las marcas y leyendas que exhiben sus productos o del signo que respalda al prestador del servicio, por la falta de conformidad entre la publicidad comercial de los productos y servicios y éstos, así como por el contenido y la vida útil del producto indicado en el envase, en lo que corresponda.

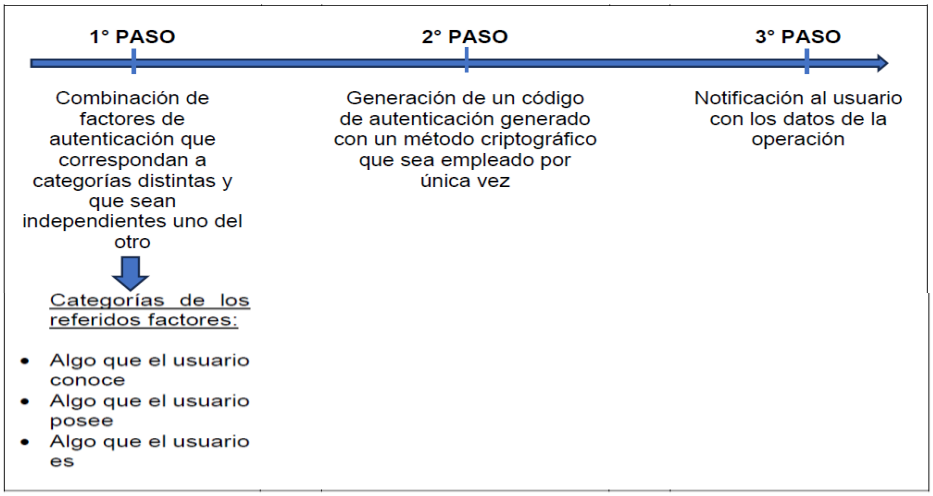
14. A efectos de poder realizar la validación correcta de las operaciones cuestionadas, se procederá a verificar el cumplimiento de los requisitos de validez exigidos por el artículo 19 del Reglamento de Ciberseguridad.

15. En este punto ha quedado acreditado que la señora Obo se encontraba afiliada a la banca móvil o banca por internet, además de la afiliación de la clave token digital, de manera previa a la realización de las operaciones cuestionadas. Cabe precisar que el denunciante no ha cuestionado su afiliación a la plataforma digital.

(i) Sobre la autenticación reforzada

16. Ahora bien, respecto de la autenticación reforzada, el artículo 19 del Reglamento de Ciberseguridad dispone que se deben emplear tres (3) pasos o requisitos cuyo cumplimiento se analizará en los numerales siguientes. Así, para una mejor comprensión, se ha elaborado el siguiente gráfico:

Gráfico N° 1: Tres (3) pasos que conforman la autenticación reforzada



17. En ese sentido, de conformidad con lo establecido por el artículo 19 concordado con el artículo 2, literal j) del Reglamento del Ciberseguridad, para que exista autenticación reforzada se requerirá cumplir con lo siguiente:

a) Utilizar una combinación de factores de autenticación que, por lo menos, correspondan a dos categorías distintas y que sean independientes uno del otro. Cabe precisar que, la SBS explicó las categorías de dichos factores; asimismo, brindó algunos ejemplos[8], conforme a lo que se detalla a continuación:

(i) Algo que el usuario conoce: contraseña, PIN, respuestas de preguntas clave, entre otros.

8 Ver la información detallada en el Boletín Semanal SBS Informa N° 16 de mayo de 2021, "Seguridad de la información y ciberseguridad: fortaleciendo los procesos de autenticación en beneficio de los usuarios de los sistemas supervisados", en el siguiente enlace: https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/1157?title=Seguridad%20de%20la%20informaci%C3%B3n%20y%20ciberseguridad:%20fortaleciendo%20los%20procesos%20de%20autenticaci%C3%B3n%20en%20beneficio%20de%20los%20usuarios%20de%20los%20sistemas%20supervisados

(ii) Algo que el usuario posee: certificado digital, token físico o de software, clave dinámica, entre otros.
(iii) Algo que el usuario es: huella digital, patrón de iris, reconocimiento facial, entre otros.

b) Generar un código de autenticación mediante métodos criptográficos, a partir de los datos específicos de cada operación, el cual debe utilizarse por única vez.

c) Cuando la operación sea exitosa, notificar los datos de la operación al usuario.

18. Así, conforme a lo señalado, se entenderá que el proveedor ha cumplido con aplicar la autenticación reforzada cuando demuestre haber efectuado los pasos antes señalados.

19. Por otro lado, con relación a la notificación de los datos de la operación al usuario, debe indicarse que la misma implica que el usuario pueda tomar conocimiento oportunamente de las transacciones fraudulentas y comunicarlas a la entidad financiera, a fin de que adopte las acciones para evitar que se efectúen nuevas operaciones. Cabe precisar que, pueden emplearse mecanismos de notificación alternativos al correo electrónico o mensaje de texto (SMS), siempre que tenga un propósito similar al requerimiento en la disposición legal.

20. Asimismo, la SBS señala, a modo de ejemplo, las siguientes consideraciones sobre los factores de autenticación[9]:

(i) El número de documento nacional de identidad (en adelante, DNI) no constituye un factor de autenticación de conocimiento admisible; y, si se utiliza el reconocimiento del DNI como factor de autenticación que solo el usuario posee, la entidad debe demostrar con evidencia razonable el éxito de autenticación del uso de este factor;

(ii) el CVV, número de tarjeta, nombre del titular y fecha de vencimiento, cuando estén contenidos en la tarjeta, constituyen un único factor de autenticación que demuestra la posesión de esta, por lo que se debe complementar con otro factor para aplicar la autenticación reforzada;

(iii) la contraseña de un solo uso (OTP) enviada mediante mensaje SMS no es considerada como un factor de autenticación válido, pues su transmisión no es segura y expone a los usuarios a incidentes de seguridad de la información;

(iv) las alternativas seguras que pueden considerarse como un factor de autenticación de posesión son las notificaciones push y el uso de tokens digitales; y,

(v) respecto al uso de factores de autenticación biométricos, como el escaneo de la huella digital o del rostro, las entidades preverán el uso de tecnologías con alto ratio de fiabilidad, donde se minimicen falsos positivos y falsos negativos.

9 Ver la información detallada en el Boletín Semanal SBS Informa N° 24 de julio de 2022, “Autenticación reforzada: mayor seguridad para operaciones que puedan generar perjuicio al usuario”, en el siguiente enlace: https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/1222

21. Adicionalmente, el artículo 20 del Reglamento de Ciberseguridad[10], como excepción a la aplicación de lo indicado en el literal c) del artículo 19 de la referida disposición legal, describe exenciones a la autenticación reforzada, entre las cuales se encuentran:

    (i) Las operaciones de pago realizadas a un beneficiario, el cual está registrado como usuario de confianza, como destinatario usual de dichas operaciones;

    (ii) operaciones de pago realizadas entre cuentas donde el cliente y el beneficiario sean la misma persona, además, dichas cuentas deben pertenecer a la misma empresa; y,

    (iii) operaciones de pago y transferencias realizadas debajo del umbral por operación establecido por la empresa, entre otros requerimientos.

22. En virtud a lo expuesto, y conforme a lo establecido en el Reglamento de Ciberseguridad, para operaciones realizadas desde el 1 de julio de 2022, la norma exige a las empresas supervisadas de Régimen General y Régimen Simplificado una autenticación reforzada, a fin de garantizar que los usuarios realicen operaciones por canales digitales en un entorno seguro y evitar situaciones que generen un abuso del servicio en perjuicio del cliente.

23. Por ello, ante el cuestionamiento de un consumidor, la entidad debe estar en la posibilidad de acreditar de manera suficiente y fehaciente que la operación cargada ha sido debidamente autorizada por este, conforme a lo establecido en el Reglamento de Ciberseguridad, lo cual será analizado a partir de los medios probatorios que obran en el expediente; ello en el marco de una adecuada gestión de los riesgos asociados a la seguridad de las operaciones realizadas por canal digital autorizadas por las empresas del sistema financiero.

---

10 **RESOLUCIÓN SBS N° 504-2021, REGLAMENTO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD**, publicada el 23 de febrero de 2021, modificada mediante Resolución SBS N° 03240-2023, publicada el 3 de octubre de 2023 y vigente, en este artículo, desde el 4 de octubre de 2023

Artículo 20. Exenciones de autenticación reforzada para operaciones por canal digital
20.1 Están exentas del requisito de autenticación reforzada indicado en el artículo 19 del presente Reglamento, a excepción del indicado en el literal c), las siguientes operaciones realizadas por canal digital:
a) Las operaciones de pago, pagos periódicos o transferencia hacia un beneficiario registrado previamente por el usuario como beneficiario de confianza, como destinatario usual de dichas operaciones.
b) Las operaciones de pago, pagos periódicos o transferencias a cuentas en las que el cliente y el beneficiario sean la misma persona, sea natural o jurídica, y siempre que dichas cuentas se mantengan en la misma empresa.
20.2 Las operaciones de pago y transferencia que presenten un nivel de riesgo de fraude bajo, como resultado de un análisis del riesgo en línea por operación, están exentas de la autenticación reforzada, siempre que la empresa cumpla con:
i. Implementar alguno de los estándares de la industria de pagos, EMV 3DS y tokenización de pagos EMV, en sus versiones más recientes.
ii. Definir el monto de umbral por operación por debajo del cual aplicará la exención por el citado análisis de riesgos.
iii. Medir periódicamente el ratio de fraude de las operaciones de pago por canal y tipo de operación.
iv. Actualizar periódicamente las reglas aplicables en el análisis de riesgo en función al indicador de riesgo de fraude.
v. Utilizar los datos que estén disponibles por cada tipo de operación, que incluye, pero no se limita a, los asociados al comportamiento del usuario, al medio utilizado y los que de este se pueda obtener para fines del análisis de riesgo.
20.3 Las operaciones no reconocidas por los clientes que hayan sido efectuadas en aplicación de la exención señalada en el párrafo 20.2 del presente artículo, o que fueron realizadas luego de que el usuario reportara el robo o pérdida de sus credenciales, son responsabilidad de la empresa, para lo cual deben implementar mecanismos que ante el repudio de la operación por parte del usuario garanticen su aplicación inmediata.

La utilización de, por lo menos, 2 factores de autenticación que correspondan a categorías distintas

24. El Banco sostuvo que, la usuaria inició sesión con sus credenciales; esto es, su DNI y clave de acceso (*"Algo que el usuario conoce"* como 1° Factor de Autenticación); para acreditar sus afirmaciones presentó sus reportes "Log inicio de sesión", conforme se muestra en las siguientes imágenes:

Tipo Documento	Nro Documento	ID Servicio	Nombre del Servicio	Canal	Fecha
DNI	[redacted]		createTicket	BM	11/04/2025
DNI			createTicket	BM	11/04/2025
DNI			createTicket	BM	11/04/2025
DNI			createTicket	BM	11/04/2025
DNI			createTicket	BM	11/04/2025
DNI			createTicket	BM	12/04/2025

Hora	consumerRequestId	aap	responseType
10:35:25 a. m.	[redacted]		OK
10:47:08 a. m.			OK
10:48:12 a. m.			OK
10:51:25 a. m.			OK
11:14:26 a. m.			OK
8:48:57 a. m.			OK

25. El Banco indicó que la señora Obo tenía activado el Token Digital o Softoken (STKN) ("Algo que el usuario posee" como 2° Factor de Autenticación) para realizar operaciones, para acreditar sus afirmación presentó las capturas de pantalla de sus sistemas; de cuya revisión se observa que con los datos del DNI y Softoken de la denunciante se realizaron las 4 operaciones no reconocidas; conforme se muestra en la siguiente imagen:

Tipo Documento	Nro Documento	ID Servicio	Nombre del Servicio	Canal
DNI	[redacted]			BM
DNI				BM
DNI				BM
DNI				BM

FEC_OPER	HMS_OPER	COD_PERSONOR	COD_TRANSAC	COD_DIVIOPER	IMP_IMPOPER	COD_ESTADO	COD_NUCONORD	COD_NUCONDES	COD_CANTRANSAC	COD_CNL_APT	X
4/11/2025	104913	[redacted]							0000	GNET	x
4/11/2025	105021								0000	GNET	x
4/11/2025	111522								0000	GNET	x
4/12/2025	084954								0000	GNET	x

La generación de un código de autenticación mediante métodos criptográficos, cuyo uso debe ser por única vez; y, la notificación al usuario de los datos de la operación exitosa

26. En lo referido al requisito consignado en el literal b) del considerando 18, el Banco, en su apelación, señaló que, las operaciones cuestionadas fueron realizadas válidamente con el ingreso de la clave token, la cual constituye el código de autenticación criptográfico de uso único One Time Password (OTP).

27. Por lo señalado, indicó que el token digital generaba una clave única por operación y era generada a través del método de encriptación, el Banco afirmó que las claves token empleadas para autorizar cada operación cumplían con el requisito previsto en el numeral b) del artículo 19 del Reglamento de Ciberseguridad.

28. No obstante, el artículo 19 del Reglamento de Ciberseguridad es claro al diferenciar tres requisitos que deben cumplirse de manera concurrente, para la validez de operaciones que impliquen –entre otros, pagos. Bajo esa línea, si la clave token ha sido utilizada como uno de los factores de autenticación establecidos en el literal a) del mismo considerando, no puede ser utilizado como "control ante ataques de hombre en el medio", previsto en el literal b); toda vez que se ha contemplado que pueda emplearse para dos propósitos distintos y en cumplimiento de dos requisitos diferentes de la normativa.

29. Una lectura distinta implicaría que, bajo una interpretación libre de los administrados como la planteada por la parte denunciada, se aplicase el Reglamento de Ciberseguridad con alcances distintos a los expresamente previstos, lo que acarrearía a vaciarlo de contenido. Por tanto, esta instancia se ha limitado a aplicar dicha normativa conforme a sus términos, sin que deba acogerse ninguna interpretación alternativa o distinta que no provenga de su propio contenido.

30. Asimismo, si bien mediante Oficio 32655-2025-SBS del 20 de junio de 2025[11], documento que no comprende una interpretación vinculante del Reglamento de Ciberseguridad, la SBS señaló que la clave *token* podía ser considerada un mecanismo válido para evitar ataques de tipo "hombre en el medio", esta interpretación no resulta vinculante para el Indecopi e, incluso de considerarse como aplicable, dicha entidad determinó que, para tal fin, la clave *token* debía ser generada fuera de banda, dado que *"si todo ocurre en el mismo canal (por ejemplo, todo en el navegador, todo en la aplicación), un atacante podría capturar tanto la contraseña como el código OTP"* y no ha sido probado que las claves *token* se hayan generado de dicha manera.

31. En este sentido, en la medida que no fue acreditado el requisito b) del Reglamento de Ciberseguridad, no corresponde continuar con el análisis del requisito c) (notificación al usuario de los datos de la operación exitosa); y, consecuentemente, no corresponde analizar los demás medios probatorios que obran en el expediente a fin de verificar su cumplimiento, toda vez que la norma es clara en señalar que las entidades del sistema financiero deben cumplir con todos los requisitos indicados.

11 Documento analizado en el marco de la denuncia tramitada en el Expediente 2762-2024/CC1.

32. Por tanto, corresponde confirmar la resolución venida en grado que declaró fundada la denuncia interpuesta contra el Banco por infracción a lo establecido en el artículo 19 del Código, al haberse acreditado que permitió que en forma indebida el 11 y 12 de abril de 2025, se realicen cuatro (04) operaciones por el importe total de S/ 5 700,00 con cargo a la Tarjeta de Débito N° [redacted], de titularidad de la denunciante, según el siguiente detalle:

Fecha	Detalle de transacción	Importe
11/04/2025	*PAGOEFECTIVO SOLES	S/ 1 500,00
11/04/2025	*PAGOEFECTIVO SOLES	S/ 1 000,00
11/04/2025	*PAGOEFECTIVO SOLES	S/ 1 200,00
12/04/2025	*PAGOEFECTIVO SOLES	S/ 2 000,00

Graduación de la sanción

33. De conformidad con lo dispuesto en el Decreto Supremo 032-2021-PCM, vigente a partir del 15 de junio de 2021, y aplicable a los procedimientos iniciados a partir de dicha fecha, la multa a imponer por infracciones al Código se calculará en base a la fórmula "M = m x F" donde "m" representa la multa base y "F" la sumatoria de los factores agravantes y atenuantes.

34. Siguiendo el orden previsto en la referida norma, corresponde establecer, en primer lugar, la multa base, para cuyo efecto, se deberá determinar (i) el nivel de afectación en función al tipo de infracción, esto es, si es muy baja, baja, moderada, alta o muy alta; (ii) el tamaño del infractor, verificando, si a la fecha en que cometió la infracción tenía la condición de micro, pequeña, mediana o gran empresa; y, (iii) el periodo de duración de la infracción cometida, que podría ser hasta 24 meses.

35. De la revisión de la Resolución venida en grado, se verifica que el ORPS consideró los siguientes criterios para establecer el monto correspondiente a la multa:

> *“*
>
> ***(i) Nivel de afectación:*** *La infracción cometida está referida a que el Banco permitió que en forma indebida el 11 y 12 de abril de 2025, se realicen cuatro (04) operaciones por los importes de S/ 1 500,00, S/ 1 000,00, S/ 1 200,00 y S/ 2 000,00 con cargo a la Tarjeta de Débito N° [redacted] de titularidad de la denunciante. Al respecto, se determina que el tipo de afectación es "moderada", según el valor preestablecido en el cuadro 16 del Decreto Supremo 032-2021-PCM.*
>
> ***(ii) Tamaño del infractor:*** *El artículo 5 del Texto Único Ordenado de la Ley de Impulso al Desarrollo Productivo y al Crecimiento Empresarial, norma modificada por la Ley 30056, prevé que la condición de micro, pequeña, mediana y gran empresa se obtiene a partir de las ventas anuales (microempresa: ventas anuales de 1 a 150 UIT; pequeña empresa: ventas anuales de 150 a 1 700 UIT; mediana empresa: ventas anuales de 1 700 a 2 300 UIT; y, si las ventas anuales superan las 2 300 UIT se trata de una gran empresa.*
>
> *De acuerdo con la información económica reportada por el denunciado ante la Superintendencia de Mercados y Valores, en particular, su*

estado de resultados correspondiente al ejercicio 2024 (año anterior a la fecha de comisión de la infracción), se verifica que sus ventas anuales superaron las 2 300 UIT, considerando para este cálculo la UIT fijada para el 2024 (S/ 5 150,00); por lo que, se ha acreditado su condición de gran empresa.
Considerando el nivel de afectación y el tamaño del infractor, el valor preestablecido conforme al cuadro 18 previsto en el Decreto Supremo 032-2021-PCM es de 3,78.

(iii) ***Periodo de duración de la infracción:*** *La infracción se cometió en un solo acto, dada su naturaleza instantánea; por lo que, el factor de duración conforme al valor preestablecido en el cuadro 23 del Decreto Supremo 032-2021-PCM es 1. Al multiplicar el monto preestablecido (3,78) por el factor de duración (1), se determina que la multa base es de 3,78 UIT.*

59. Definida la muta base, corresponderá establecer el factor "F", para lo cual se podrán considerar las circunstancias atenuantes y agravantes previstas en el Código, cuyos valores preestablecidos se han recogido en el cuadro 2 del Decreto Supremo 032-2021- PCM. Como las circunstancias atenuantes (AT) solo pueden reducir la multa base hasta en un 50%, es decir, la mitad (el valor en este caso es 0,5); y, las circunstancias agravantes (AG) solo pueden incrementarla hasta en un 100%, es decir, el doble (el valor en este caso es 2,0); el resultado total de sumar los valores asignados a cada circunstancia no podrá exceder dichos topes. En el presente caso, este OPS no verifica la existencia de circunstancias atenuantes ni agravantes.

60. Por tanto, corresponde sancionar al Banco con multa de 3,78 UIT por infracción al artículo 19 del Código, en este extremo de la denuncia."

36. El Banco indicó que el ORPS no ha realizado un análisis adecuado sobre la graduación de las multa impuesta, vulnerando así el principio de razonabilidad y Presunción de Licitud; al respecto, es importante precisar que, de la revisión de los factores determinantes usados para la fórmula de la multa, se verifica que están acorde con el Decreto Supremo 032-2021-PCM y se sustentó cada criterio aplicado, tales como el factor de duración y el tamaño del infractor.

37. En ese sentido, corresponde confirmar la sanción impuesta al Banco con multa de 3,78 UIT por infracción al artículo 19 del Código.

Sobre la medida correctiva, el pago de costos y costas y la inscripción en el Registro de Infracciones y Sanciones

38. En la medida que el Banco no ha fundamento su apelación respecto de los extremos referidos a: (i) la medida correctiva ordenada; (ii) la condena al pago de las costas y costos del procedimiento; y, (iii) su inscripción en el Registro de Infracciones y Sanciones del Indecopi - más allá de la alegada ausencia de responsabilidad desvirtuada precedentemente- se asumen como propias las consideraciones de la recurrida sobre tales puntos.

39. En ese sentido, se confirma la resolución venida en grado en los extremos que: (i) ordenó al Banco como medida correctiva cumpla con devolver a la denunciante el

importe total de S/ 5 700,00 que corresponde a las cuatro (04) operaciones cuestionadas del 11 y 12 de abril de 2025, efectuadas con cargo a su Tarjeta de Débito N° [redacted]; asimismo se confirma el extremo que (ii) condenó al Banco al pago de las costas y costos del procedimiento; y, (iii) dispuso la inscripción del Banco en el Registro de Infracciones y Sanciones del INDECOPI.

40. Por los fundamentos expuestos y en aplicación de lo establecido en los artículos 105 del Código y 21 literal b) del Decreto Legislativo N° 1033, Decreto Legislativo que aprueba la Ley de Organización y Funciones del Indecopi, la Autoridad Administrativa decide lo siguiente,

III. SE RESUELVE:

PRIMERO: Confirmar la Resolución Final N° 0156-2025/PS0-INDECOPI-CHT del 31 de octubre de 2025, emitida por el Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor de la Oficina Regional del Indecopi Ancash – Sede Chimbote, que resolvió sancionar a Banco BBVA Perú S.A. con multa de 3,78 UIT[12] por haber incurrido en infracción a lo establecido en el artículo 19 del Código de Protección y Defensa del Consumidor, al haberse acreditado que permitió que en forma indebida el 11 y 12 de abril de 2025, se realicen cuatro (04) operaciones por el importe total de S/ 5 700,00 con cargo a la Tarjeta de Débito N° [redacted], de titularidad de la denunciante, según el siguiente detalle:

Fecha	Detalle de transacción	Importe
11/04/2025	*PAGOEFECTIVO SOLES	S/ 1 500,00
11/04/2025	*PAGOEFECTIVO SOLES	S/ 1 000,00
11/04/2025	*PAGOEFECTIVO SOLES	S/ 1 200,00
12/04/2025	*PAGOEFECTIVO SOLES	S/ 2 000,00

SEGUNDO: Requerir a Banco BBVA Perú S.A. el cumplimiento espontáneo de la multa[13], de conformidad con lo establecido en el numeral 4 del artículo 205 del Texto Único

12 Dicha cantidad deberá ser abonada en la Tesorería del Instituto Nacional de Defensa de la Competencia y de Protección de la Propiedad Intelectual - INDECOPI - sito en Calle La Prosa 104, San Borja.

13 Los únicos medios de pago son los siguientes y debe proporcionar para estos efectos el número de CUM para identificar la multa:

Pago en ventanilla en el **Banco de la Nación y Banco de Crédito del Perú**	Pago en línea – Internet **(solo para clientes de Banco de Crédito del Perú)**
1. Indicar que realizará en pago de una multa impuesta por el Indecopi. Cuenta "Indecopi-Multas". 2. Brindar el número de CUM correspondiente. Si paga en Banco de la Nación, deberá indicar el código de transacción 3711 + el número de CUM. 3. Verificar que la constancia del pago indique el número de CUM correcto.	Seguir los siguientes pasos: 1. Seleccionar pagos y transferencias. 2. Seleccionar pago de servicios. 3. Seleccionar Instituciones (Indecopi). 4. Seleccionar el concepto de pago (multas). 5. Ingresar el número de CUM. 6. Ingresar el monto a pagar.

Cualquier abono que no se efectúe en la forma señalada en el cuadro anterior, no será considerado para efectos de la cancelación de la multa. En caso no se cuente con el número de CUM o se presente cualquier inconveniente al pretender efectuar el pago en las modalidades indicadas, será necesario que se comunique inmediatamente a los anexos 7814, 7825 y 7829, así como a la siguiente dirección: controldemultas@indecopi.gob.pe.

Ordenado de la Ley del Procedimiento Administrativo General[14], bajo apercibimiento de iniciarse el procedimiento de ejecución coactiva respectivo[15].

TERCERO: Confirmar la Resolución Final N° 0156-2025/PS0-INDECOPI-CHT del 31 de octubre de 2025, emitida por el Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor de la Oficina Regional del Indecopi Ancash – Sede Chimbote, que ordenó a Banco BBVA Perú S.A. como medida correctiva que en un plazo de quince (15) días hábiles, contados a partir del día siguiente de notificada la presente resolución, cumpla con devolver a la denunciante el importe total de S/ 5 700,00 que corresponde a las cuatro (04) operaciones cuestionadas del 11 y 12 de abril de 2025, efectuadas con cargo a su Tarjeta de Débito N° [redacted].

CUARTO: Requerir a Banco BBVA Perú S.A. presentar los medios probatorios que acrediten el cumplimiento de la medida correctiva ordenada por el Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor de la Oficina Regional del Indecopi Ancash – sede Chimbote, en el plazo máximo de cinco (5) días hábiles, contado a partir del vencimiento del plazo otorgado para tal fin; bajo apercibimiento de imponer una multa coercitiva conforme a lo establecido en el artículo 117 del Código. De otro lado, se informa a la parte denunciante, que en caso se produzca el incumplimiento del mandato, deberá comunicarlo al Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor de la Oficina Regional del Indecopi Ancash – sede Chimbote, quien evaluará la imposición de la multa coercitiva por incumplimiento de medida correctiva conforme a lo establecido en el numeral 4.11 de la Directiva 006 -2017/DIR-COD-INDECOPI.

QUINTO: Confirmar la Resolución Final N° 0156-2025/PS0-INDECOPI-CHT del 31 de octubre de 2025, en el extremo que condenó a Banco BBVA Perú S.A. al pago de las costas del procedimiento y disponer que en un plazo no mayor a quince (15) días hábiles contado a partir del día siguiente de la notificación de la presente resolución, cumpla con el pago de las costas de esta instancia a la denunciante ascendente a S/ 36,00, sin perjuicio del derecho de ésta de solicitar la liquidación de los costos una vez concluida la instancia administrativa. La evaluación de las solicitudes de liquidación estará a cargo del Órgano Resolutivo de Procedimientos Sumarísimos competente.

SEXTO: Confirmar la Resolución Final N° 0156-2025/PS0-INDECOPI-CHT del 31 de octubre de 2025, emitida por el Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor de la Oficina Regional del Indecopi Ancash – Sede Chimbote, que dispuso la inscripción de Banco BBVA Perú S.A. en el Registro de Infracciones y Sanciones del Indecopi, una vez que la resolución quede firme en sede administrativa, conforme a lo establecido en el artículo 119[16] del Código de Protección y Defensa del Consumidor.

---

14 Sin perjuicio de ello, se le informa que la presente resolución será puesta en conocimiento del Área de Ejecución Coactiva del Indecopi a efectos de que ejerza las funciones que la Ley le otorga.

15 El procedimiento de ejecución coactiva se encuentra bajo la competencia del Ejecutor Coactivo del Indecopi, y se regula conforma a las normas establecidas en el Texto Único Ordenado de la Ley del procedimiento de ejecución coactiva, aprobado por D.S. N° 018-2008-JUS.

16 **LEY Nº 29751, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR**
Artículo 119º.- Registro de infracciones y sanciones
El Indecopi lleva un registro de infracciones y sanciones a las disposiciones del presente Código con la finalidad de contribuir a la transparencia de las transacciones entre proveedores y consumidores y orientar a estos en la toma de sus decisiones de consumo. Los proveedores que sean sancionados mediante resolución firme en sede administrativa quedan automáticamente registrados por el lapso de cuatro (4) años contados a partir de la fecha de dicha resolución. La información del registro es de acceso público y gratuito.

SÉTIMO: Informar a las partes que la presente resolución tiene vigencia desde el día de su notificación y agota la vía administrativa, por lo que solo puede ser cuestionada en vía de proceso contencioso administrativo ante el Poder Judicial[17].

Con la intervención de los señores miembros: Said Giuliano Trujillo Ripamontti, Manuel Ulises Urcia Quispe, Mario Merchán Gordillo y Sadie María Velásquez Contreras.

SAID GIULIANO TRUJILLO RIPAMONTTI
PRESIDENTE

Corresponde informar que la presente Resolución fue firmada de forma digital, ello de conformidad con lo establecido en los artículos 1 y 3 del Reglamento de la Ley de Firmas y Certificados Digitales aprobado por Decreto Supremo 052-2008-PCM, conforme puede verificarse en el presente documento que se encuentra en formato PDF[18].

17 **LEY Nº 29571. CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR, modificada por el Decreto Legislativo N° 1308.**
Artículo 125° (…)
La Comisión de Protección al Consumidor del Indecopi o la comisión con facultades desconcentradas en esta materia, según corresponda, constituye la segunda instancia administrativa en este procedimiento sumarísimo, que se tramita bajo las reglas establecidas por el presente subcapítulo y por la directiva que para tal efecto debe aprobar y publicar el Consejo Directivo del Indecopi.
La resolución que emita la correspondiente Comisión agota la vía administrativa y puede ser cuestionada mediante el proceso contencioso administrativo.

18 **REGLAMENTO DE LA LEY DE FIRMAS Y CERTIFICADOS DIGITALES (DECRETO SUPREMO Nº 052-2008-PCM)**
TÍTULO I DISPOSICIONES GENERALES
Artículo 1.- Del objeto
El objeto de la presente norma es regular, para los sectores público y privado, la utilización de las firmas digitales y el régimen de la Infraestructura Oficial de Firma Electrónica, que comprende la acreditación y supervisión de las Entidades de Certificación, las Entidades de Registro o Verificación, y los Prestadores de Servicios de Valor Añadido; de acuerdo a lo establecido en la Ley Nº 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley Nº 27310, en adelante la Ley. Reconociendo la variedad de modalidades de firmas electrónicas, la diversidad de garantías que ofrecen, los diversos niveles de seguridad y la heterogeneidad de las necesidades de sus potenciales usuarios, la Infraestructura Oficial de Firma Electrónica no excluye ninguna modalidad, ni combinación de modalidades de firmas electrónicas, siempre que cumplan los requisitos establecidos en el artículo 2 de la Ley.
(…)
Artículo 3.- De la validez y eficacia de la firma digital
La firma digital generada dentro de la Infraestructura Oficial de Firma Electrónica tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita. En tal sentido, cuando la ley exija la firma de una persona, ese requisito se entenderá cumplido en relación con un documento electrónico si se utiliza una firma digital generada en el marco de la Infraestructura Oficial de la Firma Electrónica. Lo establecido en el presente artículo y las demás disposiciones del presente Reglamento no excluyen el cumplimiento de las formalidades específicas requeridas para los actos jurídicos y el otorgamiento de fe pública.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
Web: www.indecopi.gob.pe