RESOLUCIÓN Nro. RES-SPDP-ICS-2025-0006

SUPERINTENDENCIA DE PROTECCIÓN DE DATOS PERSONALES. - INTENDENCIA GENERAL DE CONTROL Y SANCIÓN	
EXPEDIENTE ADMINISTRATIVO SANCIONATORIO NO.	EXP-SPDP-ICS-PASN-2025-0005
IDENTIFICACIÓN DE LA PERSONA PRESUNTAMENTE RESPONSABLE	FEDERACIÓN ECUATORIANA DE FÚTBOL RUC: 0990986665001
LUGAR Y FECHA	QUITO, 31 DE DICIEMBRE DE 2025

VISTOS. - En mi calidad de funcionario resolutor avoco conocimiento del presente procedimiento administrativo sancionador. Siendo el momento procedimental para resolver se considera lo siguiente:

I. COMPETENCIA

1. Que, el numeral 19) del artículo 66 de la Constitución de la República del Ecuador ("CRE"), reconoce y garantiza: *"(...) [e]l derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley (...)".*

2. Que, el numeral 1) del artículo 76 de la CRE determina que: *"[e]n todo proceso en el que se determinen derechos y obligaciones de cualquier orden, se asegurará el derecho al debido proceso que incluirá las siguientes garantías básicas: 1. Corresponde a toda autoridad administrativa o judicial, garantizar el cumplimiento de las normas y los derechos de las partes.. (...)".*

3. Que, el literal l) del numeral 7) del artículo 76 de la CRE determina que "*(...) 7. El derecho de las personas a la defensa incluirá las siguientes garantías: l) Las resoluciones de los poderes públicos deberán ser motivadas. No habrá motivación si en la resolución no se enuncian las normas o principios jurídicos en que se funda y no se explica la pertinencia de su aplicación a los antecedentes de hecho. Los actos administrativos, resoluciones o fallos que no se encuentren debidamente motivados se considerarán nulos. Las servidoras o servidores responsables serán sancionados".*

4. Que, el artículo 82 de la CRE establece que: *"[e]l derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes".*

5. Que, el artículo 213 de la CRE establece que: *"(...) [l]as superintendencias son organismos técnicos de vigilancia, auditoría, intervención y control de las actividades económicas, sociales y ambientales, y de los servicios que prestan las entidades públicas y privadas, con el propósito de que estas actividades y servicios se sujeten al ordenamiento jurídico y atiendan al interés general. Las*

superintendencias actuarán de oficio o por requerimiento ciudadano. Las facultades específicas de las superintendencias y las áreas que requieran del control, auditoría y vigilancia de cada una de ellas se determinarán de acuerdo con la ley (...)".

6. Que, el artículo 226 de la CRE, dispone que las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal, ejercerán solamente las competencias y facultades que les sean atribuidas en dicha Constitución y la ley. Tendrán, así mismo, el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos constitucionales.

7. Que, el artículo 14 del Código Orgánico Administrativo ("COA") consagra el principio de juridicidad, señalando que: *"[l]a actuación administrativa se somete a la Constitución, a los instrumentos internacionales, a la ley, a los principios, a la jurisprudencia aplicable y al presente Código".*

8. Que, el artículo 19 del COA establece el principio de imparcialidad e independencia, disponiendo que: *"[l]os servidores públicos evitarán resolver por afectos o desafectos que supongan un conflicto de intereses o generen actuaciones incompatibles con el interés general. Los servidores públicos tomarán sus resoluciones de manera autónoma".*

9. Que, el artículo 22 del COA regula los principios de seguridad jurídica y confianza legítima, indicando que: *"[l]as administraciones públicas actuarán bajo los criterios de certeza y previsibilidad. La actuación administrativa será respetuosa con las expectativas que razonablemente haya generado la propia administración pública en el pasado. La aplicación del principio de confianza legítima no impide que las administraciones puedan cambiar, de forma motivada, la política o el criterio que emplearán en el futuro. Los derechos de las personas no se afectarán por errores u omisiones de los servidores públicos en los procedimientos administrativos, salvo que el error u omisión haya sido inducido por culpa grave o dolo de la persona interesada".*

10. Que, el artículo 23 del COA establece el principio de racionalidad, mandando que: *"[l]a decisión de las administraciones públicas debe estar motivada".*

11. Que, el artículo 29 del COA define el principio de tipicidad, señalando que: *"[s]on infracciones administrativas las acciones u omisiones previstas en la ley. A cada infracción administrativa le corresponde una sanción administrativa. Las normas que prevén infracciones y sanciones no son susceptibles de aplicación analógica, tampoco de interpretación extensiva".*

12. Que, el artículo 99 determina: *"(...) [r]equisitos de validez del acto administrativo. Son requisitos de validez: 1. Competencia 2. Objeto 3. Voluntad 4. Procedimiento 5. Motivación (...)".*

13. Que, el artículo 100 del COA regula la motivación del acto administrativo, estableciendo que: *"[e]n la motivación del acto administrativo se observará: 1) El señalamiento de la norma jurídica o principios jurídicos aplicables y la*

determinación de su alcance. 2) La calificación de los hechos relevantes para la adopción de la decisión, sobre la base de la evidencia que conste en el expediente administrativo. 3) La explicación de la pertinencia del régimen jurídico invocado en relación con los hechos determinados. Se puede hacer remisión a otros documentos, siempre que la referencia se incorpore al texto del acto administrativo y conste en el expediente al que haya tenido acceso la persona interesada. Si la decisión que contiene el acto administrativo no se deriva del procedimiento o no se desprende lógicamente de los fundamentos expuestos, se entenderá que no ha sido motivado".

14. Que, el numeral 5) del artículo 201 del COA dispone sobre la terminación del procedimiento administrativo, indicando que: *"[e]l procedimiento administrativo termina por: (...) 1. El acto administrativo. (...)".*

15. Que, el artículo 202 del COA establece la obligación de resolver, señalando que: *"[e]l órgano competente resolverá el procedimiento mediante acto administrativo (...)".*

16. Que, el artículo 203 del COA determina el plazo de resolución, indicando que: *"[e]l acto administrativo en cualquier procedimiento será expreso, se expedirá y notificará en el plazo máximo de un mes, contado a partir de terminado el plazo de la prueba".*

17. Que, el artículo 248 del COA dispone: *"[g]arantías del procedimiento. El ejercicio de la potestad sancionadora requiere procedimiento legalmente previsto y se observará: **1.** En los procedimientos sancionadores se dispondrá la debida separación entre la función instructora y la sancionadora, que corresponderá a servidores públicos distintos. **2.** En ningún caso se impondrá una sanción sin que se haya tramitado el necesario procedimiento. **3**. El presunto responsable por ser notificado de los hechos que se le imputen, de las infracciones que tales hechos puedan constituir y de las sanciones que, en su caso, se le pueda imponer, así como de la identidad del instructor, de la autoridad competente para imponer la sanción y de la norma que atribuya tal competencia. **4**. Toda persona mantiene su estatus jurídico de inocencia y debe ser tratada como tal, mientras no exista un acto administrativo firme que resuelva lo contrario".*

18. Que, la Ley Orgánica de Protección de Datos Personales ("LOPDP"), fue publicada en el Registro Oficial Suplemento No. 459, el 26 mayo de 2021.

19. Que, la LOPDP estableció en su Disposición Transitoria Primera que lo relacionado a las medidas correctivas y régimen sancionatorio entraba en vigencia en 2 años a partir de su publicación en el Registro Oficial; esto es, 26 de mayo de 2023.

20. Que, la Superintendencia de Protección de Datos Personales ("SPDP", "Autoridad", y/o "Superintendencia") fue creada mediante la LOPDP como un órgano técnico de control, con capacidad sancionatoria, de administración desconcentrada, con personalidad jurídica, autonomía administrativa, técnica, operativa y financiera".

21. Que, el literal m) del artículo 10 de la LOPDP menciona que la misma se regirá por el principio de Independencia de Control, mismo que manifiesta que: *"[p]ara el efectivo ejercicio del derecho a la protección de datos personales, y en cumplimiento de las obligaciones de protección de los derechos que tiene el Estado, la Autoridad de Protección de Datos deberá ejercer un control independiente, imparcial y autónomo, así como llevar a cabo las respectivas acciones de prevención, investigación y sanción (...)".*

22. Que, el numeral 2) del artículo 76 de la LOPDP indica que las funciones, atribuciones y facultades de la SPDP incluye: *"(...) [e]jercer la potestad sancionadora respecto de responsables, delegados, encargados y terceros, conforme a lo establecido en la presente ley (...)."*

23. Que, el Reglamento General de la Ley Orgánica de Protección de Datos Personales ("RGLOPDP"), fue publicada en el Registro Oficial Suplemento No. 435, el 13 de noviembre de 2023*".*

24. Que, el artículo 90 del RGLOPDP, establece que: *"(...) [e]n los casos en que se presuma el cometimiento de alguna de las infracciones previstas en la Ley, la Autoridad de Protección de Datos iniciará el correspondiente procedimiento administrativo sancionatorio, de conformidad con las disposiciones establecidas en el Código Orgánico Administrativo. La resolución que ponga fin al procedimiento deberá estar debidamente fundamentada y motivada, de conformidad con lo establecido en la Ley. Las sanciones a las que hubiere lugar se impondrán sin perjuicio de la responsabilidad civil o penal que resulten del cometimiento de la infracción (...)*."

25. Que, el numeral 2 Procesos Sustantivos, Nivel Operativo, Intendencia General de Control y Sanción del Estatuto Orgánico de Gestión Organizacional por Procesos de Arranque de la Superintendencia de Protección de Datos Personales expedida mediante Resolución No SPDP-SPDP-2024-0001-R publicada en el Registro Oficial Tercer Suplemento 624 del 19 de agosto de 2024 establece que el responsable de la Intendencia General de Control y Sanción es el Intendente General de Control y Sanción.

26. Que, mediante acción de personal No. SPDP-0005-2024 de fecha 16 de septiembre de 2024 se nombró al Ab. René Francisco Orbe Pacheco como Intendente General de Control y Sanción.

27. Que, el literal h) del numeral 2 Procesos Sustantivos, Nivel Operativo, Intendencia General de Control y Sanción del Estatuto Orgánico de Gestión Organizacional por Procesos de Arranque de la Superintendencia de Protección de Datos Personales expedida mediante Resolución No SPDP-SPDP-2024-0001-R publicada en el Registro Oficial Tercer Suplemento 624 del 19 de agosto de 2024 establece: *"(...)[e]jercer la potestad sancionadora a través del conocimiento y sustanciación de los procedimientos administrativos de conformidad con la normativa vigente y la que se expida para el efecto (...)".*

28. Que, el artículo 22 de la Resolución No. SPDP-SPDP-2024-0013-R de fecha 25 de octubre de 2024, que expide el Reglamento para la Presentación, Recepción y

Trámite de Denuncias y Solicitudes, publicada en el Registro Oficial No. 683 del 14 de noviembre de 2024, dispone que: *"(...) [e]l procedimiento administrativo sancionador se regirá por lo dispuesto en el Título 1, Libro III del COA en todo lo que no se oponga con lo establecido en la LOPDP, el RGLOPDP, en las regulaciones expedidas por la SPDP y demás normativa aplicable (...)".*

29. Que, el literal b) del artículo 5 de la Resolución No. SPDP-SPD-2025-0001-R de fecha 31 de enero de 2025 por la cual se expidieron las disposiciones, delegaciones de facultades y atribuciones a las autoridades, funcionarios, y servidores públicos de la Superintendencia de Protección de Datos Personales, publicada en el Registro Oficial No. 750 del 24 de febrero de 2025, delega al Intendente General de Control y Sanción la atribución de: *"(...)[e]jercer la potestad sancionadora respecto de responsables, responsables conjuntos, delegados, encargados y terceros, conforme a lo establecido en la Ley Orgánica de Protección de Datos Personales (...)"*

II. LA DETERMINACIÓN DE LA PERSONA RESPONSABLE

RESPONSABLE: FEDERACIÓN ECUATORIANA DE FÚTBOL ("FEF")
RUC: 0990986665001
NOTIFICACIONES:
[redacted]

III. HECHOS RELEVANTES PARA LA ADOPCIÓN DE LA DECISIÓN

SOBRE LAS ACTUACIONES PREVIAS

30. De foja 1 a 2 del expediente Nro. SPDP-IGCS-2024-AP-008-PV, mediante Providencia No. SPDP-IGCS-2024-AP-008-PV de fecha 17 de diciembre de 2024, consta el inicio de la actuación previa No. SPDP-IGCS-2024-AP-008-PV que en su parte pertinente señala: *"a) el INICIO DE LA ACTUACIÓN PREVIA Nro. SPDP-IGCS-2024-AP-008-PV en contra de la FEDERACIÓN ECUATORIANA DE FÚTBOL ("FEF") Registro Único de Contribuyentes No.0990986665001 (...) b) La INSPECCIÓN in situ en las instalaciones de la FEF (...)",* debidamente notificada mediante Oficio Nro. SPDP-IGCS-2024-083 el 20 de diciembre de 2024 a las 12h17 que consta en la foja 5 del expediente.

31. De foja 6 a 13 del expediente consta el acta de inspección y su anexo de fecha 20 de diciembre de 2024 suscrita por los funcionarios de la SPDP, Diana Katherine Toapanta Pila, en calidad de Analista de Control y Sanción, Daniel Hernández y Alex Sotomayor en calidad de Especialista y Analista de Innovación Tecnológica y Seguridad de Datos Personales, respectivamente, y por parte de FEF, el señor [redacted] en calidad de Coordinador de Sistemas.

32. De foja 15 a 21 del expediente consta la Providencia Nro. PVD-SPDP-IGCS-2025-0007 de fecha 25 de febrero de 2025 y notificada el 25 y 27 de febrero de 2025 respectivamente, en donde la SPDP dispuso: *"(...) a) Una nueva INSPECCIÓN IN SITU en las instalaciones de FEF ubicadas en la* [redacted] *el día JUEVES 27 de febrero de 2025, a partir de las 14h00, de conformidad con lo establecido en el artículo 175 del COA, con el fin de constatar y verificar el cumplimiento de las*

medidas de seguridad de datos personales de naturaleza física, jurídica, administrativa y organizativa (...)".

33. De foja 22 a 56 del expediente consta el acta de inspección de fecha 27 de febrero de 2025 suscrita por los funcionarios de la SPDP, Diana Katherine Toapanta Pila, en calidad de Analista de Control y Sanción y Alex Sotomayor en calidad de Analista de Innovación Tecnológica y Seguridad de Datos Personales, respectivamente, y por parte de FEF, el señor [redacted] en calidad de Delegado de Protección de Datos Personales, [redacted] en calidad de Oficial de Integridad y Cumplimiento, [redacted] en calidad de Directo de Operaciones, [redacted] en calidad de Asesora Jurídica y donde se requiere a FEF el envío de la documentación respectiva.

34. De foja 59 a 121 del expediente consta el escrito 10 de marzo de 2025, debidamente notificado de manera electrónica el mismo día, mes y año, por medio del cual FEF remitió la documentación requerida a la SPDP.

35. De foja 122 a 124 del expediente consta la Providencia No. PVD-SPDP-ICS-2025-0013 de fecha 12 de marzo de 2025, notificada el mismo día, mes y año, donde esta autoridad requirió que la FEF proceda a legitimar la actuación del Secretario General que suscribió la comunicación de fecha 10 de marzo de 2025.

36. De foja 125 a 172 del expediente consta el escrito remitido por la FEF de fecha 14 de marzo de 2025, y notificado el mismo día, mes y año, en el cual da contestación a la Providencia No. PVD-SPDP-ICS-2025-0013.

37. De foja 174 a 213 del expediente consta el Informe Técnico-Jurídico Preliminar No. INFSPDP-ICS-2025-0014, emitido por la SPDP de fecha 13 de mayo de 2025, y la Providencia No. PVD-SPDP-ICS-2025-0050 de fecha 14 de mayo de 2025, notificada el mismo día, mes y año mediante la cual se dispone la notificación del informe mencionado y se da respuesta al escrito señalado en el numeral precedente.

38. De foja 214 a 215 del expediente consta el escrito presentado por FEF de fecha 28 de mayo de 2025, y debidamente notificado el 29 de mayo de 2025, en el cual solicitó: *"(...) se le conceda un término adicional de treinta (30) días, contados a partir de su pronunciamiento respecto de nuestras solicitudes de ampliación y aclaración previamente realizadas en el presente documento, con el objetivo de atender cabalmente los requerimientos formulados por su autoridad (...)".*

39. De foja 217 a 221 del expediente consta la Providencia No. PVD-SPDP-ICS-2025-0061 de fecha 29 de mayo de 2025, notificada el mismo día, mes y año, donde la SPDP negó la solicitud de prórroga.

40. De foja 223 a 229 del expediente consta el Memorando No. SPDP-ICS-2025-0059-M de fecha 02 de junio de 2025, notificado el mismo día, mes y año, donde el Intendente General de Control y Sanción solicitó al Director Administrativo Financiero y a la Especialista de Control y Sanción como responsable de administración del correo: control@spdp.gob.ec, que se informe y certifique si FEF ha presentado o ingresado alguna documentación entre el periodo de 30 de mayo de 2025 hasta el 02 de junio de 2025. Mediante Memorandos No. SPDP-ICS2025-0060-M, y No. SPDP-DAF-2025-0631-M, emitidos y notificados el 02 de junio de 2025, se certificó que la FEF no ingresó ningún documento en el periodo antes mencionado.

41. De foja 230 a 270 del expediente consta el Informe Técnico-Jurídico Preliminar No. INFSPDP-ICS-2025-0014, emitido por la SPDP de fecha 13 de mayo de 2025, y la Providencia No. PVD-SPDP-ICS-2025-0064 de fecha 02 de junio de 2025, y notificada el mismo día, mes y año, en la cual se ratifica que el informe técnico-jurídico preliminar notificado tiene la calidad de informe técnico-jurídico final, toda vez que el sujeto investigado no presentó criterios ni descargos dentro del término señalado de conformidad con el artículo 11 de la Resolución No. SPDP-SPDP-2024-0013-R y el artículo 178 del COA**.**

SOBRE LAS MEDIDAS CORRECTIVAS

42. De foja 1 a 48 del expediente No. EXP-SPDP-ICS-PAMC-2025-0003 consta la providencia No. PVD-SPDP-ICS-2025-0067 de fecha 04 de junio de 2025 y sus anexos, notificada el mismo día, mes y año.

43. De foja 49 a 57 del expediente consta Providencia No. PVD-SPDP-ICS-2025-0074 de fecha 13 de junio de 2025 y notificada el mismo día, mes y año, donde el Intendente General de Control y Sanción solicitó al Director Administrativo Financiero y a la Especialista de Control y Sanción como responsable de administración del correo: control@spdp.gob.ec , que se informe y certifique si FEF ha presentado o ingresado entre el periodo de 04 de junio de 2025 al 12 junio de 2025.

44. De foja 58 a 61 del expediente constan los Memorandos No. SPDP-ICS-2025-0071-M y No. SDPD-DAF-2025-0663-M de fecha 13 de junio de 2025 y notificados el mismo día mes y año, en el cual se certificó a esta Autoridad que la FEF no ingresó ningún documento en el periodo mencionado.

45. De foja 62 a la 76 del expediente consta el Informe de Supervisión de Medidas Correctivas Impuestas a la FEDERACIÓN ECUATORIANA DE FÚTBOL “FEF” No. INF-SPDP-ICS2025-0020, emitido por la SPDP de fecha 16 de junio de 2025, y la Providencia No. PVD-SPDPICS-2025-0075 de fecha 16 de junio de 2025, y notificada el mismo día, mes y año.

SOBRE EL PROCEDIMIENTO ADMINISTRATIVO SANCIONADOR

46. De foja 1 a 84 consta la Providencia No. PVD-SPDP-ICS-2025-0080 de fecha 16 de junio de 2025 y notificada el 18 de junio de 2025, donde se emitió el acto de iniciación del Procedimiento Administrativo Sancionador No. EXP-SPDP-ICS-PASN-2025-0005, acto mediante el cual se dispone: *“(…) el INICIO del PROCEDIMIENTO ADMINISTRATIVO SANCIONADOR No. EXP-SPDP-ICS-PASN-2025-0005 de conformidad con el numeral 4 del artículo 68, y el artículo 72 de la LOPDP (…)”.*

47. En foja 85 a 113 consta el escrito y anexos presentados por la FEF el día 02 de julio de 2025, mediante el cual el administrado comparece al procedimiento administrativo sancionador.

48. A foja 114 consta el escrito de fecha 03 de julio de 2025 mediante el cual el administrado solicita copias del expediente administrativo sancionador.

49. De fojas 115 a 123 del expediente consta la providencia No. PVD-SPDP-ICS-2025-0100 de fecha 04 de julio de 2025 y notificada el 07 de julio de 2025, en la que se dispone: *"(...) Se requiere a la FFF que proceda a legitimar su actuación y el escrito presentado el 02 de julio de 2025 (...)".*

50. De foja 124 a 125 del expediente consta el formulario de solicitud de copias presentado el 07 de julio de 2025 por parte de FEF.

51. De foja 126 y 137 consta el escrito y anexos ingresados mediante correo electrónico: [redacted] de fecha 07 de julio de 2025 mediante el cual el administrado procede a legitimar su actuación dentro del procedimiento administrativo sancionador.

52. De foja 138 a 146 del expediente administrativo consta la providencia No. PVD-SPDP-ICS-2025-0102 de fecha 08 de julio de 2025 y notificada el 09 de julio, mediante el cual se dispone: *"(...) a) Aceptar el formulario de solicitud de copias, relacionado con las copias certificadas del expediente administrativo signado con el No. EXP-SPDP-ICS-PASN-2025-0005(...). (...) b) Validar la Procuración Judicial de Persona Jurídica, celebrada en la Notaría Quincuagésima Novena ante el Notario Jorge Geovanny Guzmán González el 26 de octubre de 2022 (...)".*

53. De foja 147 a 154 del expediente consta la providencia No. PVD-SPDP-ICS-2025-0153 de fecha 19 de septiembre de 2025 y notificada el 22 de septiembre de 2025, mediante el cual se dispone: *"(...) Con el fin de obtener mayores elementos de convicción dentro del presente procedimiento administrativo sancionador, esta Autoridad dispone la apertura del término probatorio de QUNCE DÍAS (15) a fin de evacuar y practicar la prueba necesaria, de conformidad con el numeral 7) del artículo 76 de la CRE, en concordancia con el inciso final del artículo 194 y el inciso segundo del artículo 256 del COA (...)".*

54. De foja 155 a 167 el SRI remitió el oficio No. 117012025OACI0026482 de fecha 03 de octubre de 2025, notificado el 08 de octubre de 2025, y el oficio No. 917012025OACN0004320 de fecha 21 de octubre de 2025, mediante el cual el SRI entrega la información solicitada.

55. De foja 169 a foja 174 consta el Memorando No. SPDP-IIT-2025-0157-M de fecha 11 de noviembre de 2025 que contiene el Informe técnico-jurídico No. SPDP-IIT-2025-0024-I del mismo mes y año.

56. De foja 175 a 178 del expediente consta la Providencia No. PVD-SPDP-ICS-2025-0176 de fecha 11 de noviembre de 2025, notificado el mismo día, mes y año, donde esta Autoridad corrió traslado a la FEF con la documentación remitida por el SRI, y el Memorando No. SPDP-IIT-2025-0157-M, junto con el informe el Informe técnico-jurídico No. SPDP-IIT-2025-0024-I de fecha 11 de noviembre de 2025, otorgándole un término de tres (3) días para que pueda pronunciarse.

57. A foja 180 del expediente consta el escrito de fecha 13 noviembre de 2025 mediante el cual la parte administrada solicita la clave para el acceso a la documentación remitida.

58. De foja 182 a 185 del expediente consta la PVD-SPDP-ICS-2025-0181 de fecha 13 de noviembre de 2025 y notificada el mismo día, mes y año, mediante el cual la SPDP remite lo solicitado.

59. De foja 186 a 188 del expediente consta el escrito de fecha 14 de noviembre de 2025 mediante el cual la parte administrada presenta sus observaciones a la prueba remitida para su contradicción.

60. De foja 189 a 190 consta el escrito y anexos ingresados mediante correo electrónico de fecha 18 de noviembre de 2025 mediante el cual el administrado solicita: *"(...) Que dicho informe cumpla con los requisitos de determinación del asunto, fundamentación y concluya inequívoca, conforme lo ordena el artículo 124 del COA.*

61. De foja 191 a 199 consta el escrito ingresado mediante correo electrónico: [redacted] por el cual el administrado indica: *"(...) Se agregue al expediente la copia de la demanda propuesta por la FEF y se tenga por acreditado que la fef ha presentado acción subjetiva de plena jurisdicción ante el Tribunal Distrital de lo Contencioso Administrativo (...)".*

62. De foja 200 a 205 del expediente consta la providencia No. PVD-SPDP-ICS-2025-0204 de fecha 18 de diciembre de 2025 mediante la que se dispone: *"(...)* ***QUINTO. -*** *Conforme lo dispone el artículo 251 inciso último, del COA, se informa al administrado su derecho a realizar su argumentación final en el término de* ***TRES DÍAS (3)****, los mismos que discurrirán a partir del día hábil siguiente de la notificación de la presente providencia, fenecido el término remítase el expediente integro al funcionario Decisor para que emita la correspondiente Resolución Administrativa en la presente causa. (...)".*

63. De foja 206 a foja 216 del expediente consta el Dictamen No. DIC-SPDP-ICS-2025-0006 de fecha 18 de diciembre de 2025.

IV. LA SINGULARIZACIÓN DE LA INFRACCIÓN COMETIDA

La infracción cometida que se atribuye al responsable corresponde a la prevista en el numeral 4) del artículo 68 de la LOPDP:

"(...) ***Art. 68.-Infracciones graves del Responsable de protección de datos.-****Se consideran infracciones graves las siguientes:* ***4)*** *No utilizar metodologías de análisis y gestión de riesgos adaptadas a la naturaleza de los datos personales las particularidades del tratamiento y de las partes involucradas; (...)".*

V. ANÁLISIS Y VALORACIÓN DE LA PRUEBA PRACTICADA

64. Conforme el artículo 47 de la LOPDP, señala las obligaciones que tiene el responsable del tratamiento, entre ellas están las siguientes:

> *El responsable del tratamiento de datos personales está obligado a:*
> *5) Utilizar metodologías de análisis y gestión de riesgos adaptadas a las particularidades del tratamiento y de las partes involucradas;*
>
> *6) Realizar evaluaciones de adecuación al nivel de seguridad previas al tratamiento de datos personales;*

> *7) Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas;*

65. Por lo tanto, era la obligación del responsable del tratamiento implementar una metodología de análisis y gestión de riesgos adecuada. Esta metodología debía ser relacionada con la naturaleza de datos personales, particularidades del tratamiento, características de los sujetos que intervienen y los elementos suficientes de pertinencia.

66. En este contexto, la metodología de análisis y gestión de riesgos exigida por la norma no puede entenderse como un mero formato, documento o declaración programática, sino que debe considerarse como una herramienta de decisión que articule criterios, reglas y parámetros orientados a identificar riesgos, ponderar su impacto, definir respuestas y justificar las medidas adoptadas. La exigencia de que la metodología se encuentre "adaptada" es esencial para el cumplimiento de la normativa, pues implica que dicha metodología debe ser funcionalmente idónea. Esto supone que la metodología sea capaz de generar evaluaciones coherentes y consistentes, que mantenga una lógica interna clara y que permita vincular de manera verificable los riesgos identificados con las medidas o acciones adoptadas para su gestión. Cuando estas condiciones no se verifican, la supuesta metodología pierde su función preventiva y se convierte en una formalidad vacía, insuficiente para satisfacer el estándar normativo que sustenta la infracción administrativa analizada.

67. Desde esta perspectiva, el cumplimiento efectivo de las obligaciones en materia de protección de datos personales se encuentra directamente vinculado a un enfoque de gestión de riesgos como eje estructurante del tratamiento. Dicho enfoque no se reduce a una declaración de principios, sino que supone un proceso continuo mediante el cual el responsable del tratamiento identifica los riesgos relevantes, evalúa su gravedad y probabilidad, y establece prioridades de actuación, con el objetivo de disminuir la incertidumbre inherente al tratamiento de datos personales.

68. La idoneidad de este enfoque se verifica cuando el responsable del tratamiento se encuentra en capacidad de justificar, de manera coherente y verificable, los criterios empleados para asignar niveles de riesgo, la selección de las medidas adoptadas y los mecanismos mediante los cuales evalúa periódicamente su eficacia. Solo bajo estas condiciones la gestión de riesgos cumple su función preventiva y evita convertirse en un ejercicio meramente formal, carente de incidencia real en la protección efectiva de los datos personales.

69. Resulta indispensable precisar el contenido y alcance de lo que debe entenderse por una metodología de análisis y gestión de riesgos que se encuentre verdaderamente ajustada a las particularidades del tratamiento de datos personales y a las características de las partes involucradas. Ello supone que dicha metodología incorpore elementos suficientes para permitir a los sujetos regulados adoptar decisiones fundadas y razonadas a lo largo de todas las fases que componen el ciclo de vida del tratamiento de datos personales.

70. El eje sobre el cual se articula el cumplimiento de las obligaciones previstas en el marco normativo vigente en materia de protección de datos personales es la gestión de riesgos. Esta no debe concebirse como un ejercicio abstracto, sino como un proceso estructurado orientado a identificar, analizar y jerarquizar los riesgos relevantes, con el objetivo de

reducir la incertidumbre asociada al tratamiento y habilitar la toma de decisiones informadas. A partir de dicho proceso, corresponde definir e implementar medidas de seguridad de naturaleza jurídica, organizativa y técnica destinadas a disminuir, en términos razonables, tanto la probabilidad de ocurrencia como el impacto de eventos no deseados que puedan afectar los derechos y libertades de los titulares de datos personales.

71. Partiendo de la premisa de que una metodología de análisis y gestión de riesgos constituye un instrumento para la toma de decisiones y no una mención meramente formal incorporada en un documento, corresponde trasladar el análisis al plano normativo a fin de determinar el estándar exigido por el ordenamiento jurídico. En este ámbito, la LOPDP impone al responsable del tratamiento un deber continuo de implementar y ajustar medidas de seguridad aplicables tanto a la información como a los datos personales, las cuales deben mantener una relación directa y coherente con los procesos de gestión de riesgos previamente definidos.

72. En consecuencia, dichas medidas no pueden adoptarse de forma discrecional, fragmentada o desvinculada entre sí, sino que deben derivar de un proceso sistemático que permita identificar los riesgos asociados al tratamiento, evaluar su impacto y definir acciones orientadas a su mitigación. La gestión de riesgos se erige, así, como el marco lógico que da sentido y coherencia a las medidas de seguridad implementadas.

73. Desde esta perspectiva, la existencia de una metodología adecuada se configura como un presupuesto necesario para la validez material de las medidas adoptadas, en la medida en que solo a través de un análisis estructurado resulta posible garantizar que estas sean proporcionales y suficientes frente a los riesgos identificados. Bajo este entendimiento, corresponde examinar a continuación las disposiciones normativas aplicables que fundamentan dicha exigencia, entre ellas lo previsto en el artículo 37 de la LOPDP, que consagra el principio de seguridad de los datos personales y establece que:

> *"(...) [e]l responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos (...)".*

74. La referida disposición legal no se limita a exigir la adopción inicial de medidas de seguridad, sino que impone adicionalmente al responsable del tratamiento el deber de establecer mecanismos permanentes de revisión y control sobre dichas medidas. En particular, el ordenamiento exige la implementación de procesos continuos de verificación, evaluación y valoración que permitan comprobar, de manera sostenida en el tiempo, la eficiencia, eficacia y efectividad de las medidas de seguridad adoptadas, así como demostrar que estas responden de forma adecuada a los riesgos previamente identificados.

75. Esta exigencia normativa se desprende de manera expresa de lo dispuesto en el mismo artículo, que establece lo siguiente:

> *"(...) El responsable o encargado del tratamiento de datos personales, deberá implementar un proceso de verificación, evaluación y valoración continua y*

permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole (...)".

"(...) El responsable o encargado del tratamiento de datos personales deberá evidenciar que las medidas adoptadas e implementadas mitiguen de forma adecuada los riesgos identificados (...)".

76. De este modo, la obligación legal no se satisface con la mera declaración de medidas de seguridad, sino que exige la acreditación de su funcionamiento efectivo y de su capacidad real para mitigar los riesgos asociados al tratamiento de datos personales.

77. En línea con las consideraciones precedentes, la LOPDP concibe las medidas de seguridad no como actuaciones autónomas o desconectadas, sino como la consecuencia necesaria de un proceso previo y ordenado de identificación y valoración de riesgos, amenazas y vulnerabilidades. Bajo este entendimiento, el artículo 40 de la LOPDP dispone de manera expresa que dicho análisis debe llevarse a cabo a través de una metodología específica, la cual ha de incorporar, como mínimo, determinados elementos esenciales, entre los que se incluyen los siguientes:

"(...) Para el análisis de riesgos, amenazas y vulnerabilidades, el responsable y el encargado del tratamiento de los datos personales deberán utilizar una metodología que considere, entre otras:

1) Las particularidades del tratamiento;

2) Las particularidades de las partes involucradas; y,

3) Las categorías y el volumen de datos personales objeto de tratamiento (...)"

78. De manera complementaria, el artículo 41 de la Ley Orgánica de Protección de Datos Personales establece que la definición de las medidas de seguridad no puede efectuarse de forma abstracta ni desvinculada del análisis previo de riesgos, sino que debe sustentarse directamente en los resultados obtenidos de dicho análisis. En este sentido, la norma exige que los responsables y encargados del tratamiento consideren, de manera objetiva y sistemática, factores como la naturaleza de los datos personales tratados, las características de las partes involucradas y los antecedentes relacionados con incidentes de seguridad, incluidos supuestos de destrucción, pérdida, alteración, divulgación o acceso indebido a los datos personales, ya sea por causas accidentales o intencionales, por acción u omisión, así como situaciones de transferencia, comunicación o accesos no autorizados o en exceso de autorización. Sobre la base de estos elementos, el ordenamiento impone la adopción de medidas adecuadas y necesarias que, de forma permanente y continua, permitan evaluar, prevenir, impedir, reducir, mitigar y controlar los riesgos, amenazas y vulnerabilidades asociados al tratamiento, incluidos aquellos que puedan implicar un alto riesgo para los derechos y libertades de los titulares, conforme a la normativa que emita la Autoridad de Protección de Datos Personales.

79. La exigencia de contar con metodologías de análisis y gestión de riesgos no se presenta de manera aislada en el sistema normativo de protección de datos personales, sino que se integra como un componente central del régimen general de responsabilidades que recae sobre el responsable del tratamiento. Desde esta óptica, la LOPDP incorpora la gestión

de riesgos como una obligación estructural, vinculada directamente a la forma en que el responsable debe organizar, planificar y ejecutar el tratamiento de datos personales, asegurando que dicho tratamiento responda a las particularidades concretas del contexto en el que se desarrolla. En este marco, el artículo 47 de la LOPDP atribuye relevancia jurídica expresa a la utilización de metodologías de análisis y gestión de riesgos ajustadas al tratamiento y a las partes involucradas, disponiendo lo siguiente:

> *"(...) 2) Aplicar e implementar requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas (...);*
>
> *3) Aplicar e implementar procesos de verificación, evaluación, valoración periódica (...);*
>
> *5) Utilizar metodologías de análisis y gestión de riesgos adaptadas a las particularidades del tratamiento y de las partes involucradas;*
> *7) Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas (...);"*

80. El desarrollo reglamentario de la Ley Orgánica de Protección de Datos Personales profundiza y operacionaliza los deberes legales vinculados a la seguridad del tratamiento. En este sentido, el Reglamento General a la LOPDP precisa que la definición e implementación de medidas de seguridad debe efectuarse a partir de una evaluación contextual que tome en cuenta factores como el nivel de desarrollo tecnológico existente, los costos asociados a su aplicación y la probabilidad y gravedad de los riesgos identificados. Asimismo, el régimen reglamentario es claro en establecer que las limitaciones económicas o técnicas alegadas por el responsable no constituyen, por sí mismas, una justificación válida para el incumplimiento de las obligaciones impuestas en materia de protección de datos personales. Estas exigencias se encuentran desarrolladas de manera expresa en las disposiciones reglamentarias pertinentes, que disponen lo siguiente:

> ***"(…) Art. 33.- Obligaciones del responsable del tratamiento. -*** *El responsable del tratamiento deberá, tanto en el momento de la determinación de los medios para el tratamiento como en el momento mismo del procesamiento de datos personales, aplicar medidas apropiadas que sean adecuadas para la observancia efectiva de los principios de protección de datos, así como de los derechos reconocidos en la Ley. Para ello, tendrá en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, las circunstancias y los fines del tratamiento, así como la probabilidad y la gravedad de los riesgos para los intereses de los titulares. (...)"*
>
> ***"(…) Art. 34.- Estado de la técnica.*** *- Se entiende por estado de la técnica a los progresos actuales de la tecnología disponible en el mercado, que deberá ser considerado al determinar las medidas técnicas y organizativas adecuadas. El responsable del tratamiento deberá evaluar continuamente el estado de la técnica."*
>
> ***"(…) Art. 35.- Costos de aplicación. -*** *Los costos de aplicación no se limitan solamente a términos monetarios sino también a los recursos que, en general,*

deba invertir el responsable del tratamiento, incluidos el tiempo y el humano. El responsable del tratamiento deberá evaluar los riesgos que conlleva el tratamiento para los derechos y libertades de los titulares y estimar los costos de la aplicación de las medidas adecuadas para mitigar dichos riesgos. La incapacidad de asumir los costos no es excusa para el incumplimiento de la Ley y el presente Reglamento, para lo cual se observará el principio de proporcionalidad entre el volumen del tratamiento de los datos y la capacidad económica del responsable del tratamiento. (...)".

81. En el mismo sentido, el Reglamento General a la LOPDP introduce una exigencia adicional vinculada a la carga de acreditación del cumplimiento normativo. En particular, se impone al responsable del tratamiento el deber de demostrar de manera efectiva la aplicación de las medidas de protección de datos personales adoptadas, habilitando para ello el uso de indicadores y métricas tanto cuantitativas como cualitativas que permitan evidenciar, de forma objetiva y verificable, la observancia de sus obligaciones. Bajo este enfoque, no resulta suficiente la mera afirmación de cumplimiento, sino que se exige la capacidad de demostrar que las medidas necesarias han sido efectivamente implementadas, en los términos previstos por la normativa reglamentaria.

82. De forma complementaria, el Reglamento refuerza esta obligación al establecer, de manera expresa, el deber general de aplicar medidas apropiadas que aseguren la conformidad permanente del tratamiento de datos personales con el marco normativo vigente, incorporando además la exigencia de revisión, evaluación y actualización continua de dichas medidas. Este mandato pone de relieve que la seguridad del tratamiento no constituye un estado estático, sino un proceso dinámico que debe ajustarse de manera constante a la evolución de los riesgos, del contexto tecnológico y de las condiciones del tratamiento.

83. De forma adicional, el Reglamento General a la LOPDP introduce una exigencia específica en materia probatoria, al atribuir al responsable del tratamiento la obligación de acreditar de manera efectiva la implementación de las medidas de protección de datos personales adoptadas. Este deber supone que el cumplimiento normativo no puede quedar en el plano declarativo, sino que debe ser respaldado mediante elementos verificables, pudiendo para ello emplearse indicadores y métricas de naturaleza tanto cuantitativa como cualitativa que permitan evidenciar el grado real de observancia de dichas medidas. En este sentido, la disposición reglamentaria establece expresamente que: *"(...) Los responsables del tratamiento deberán demostrar que han aplicado todas las medidas necesarias para la protección de datos personales (...)".*

84. De manera complementaria, el propio Reglamento en su artículo 58 reafirma la obligación general de adoptar medidas apropiadas que aseguren la conformidad del tratamiento de datos personales con la normativa vigente, incorporando además el deber de que dichas medidas sean objeto de revisión y actualización continua, en atención a la evolución de los riesgos y de las condiciones del tratamiento. Al respecto, la disposición correspondiente señala que:

"(...) Art. 58.- Obligatoriedad. - El responsable del tratamiento está obligado a aplicar medidas técnicas, jurídicas, administrativas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento de datos que realiza es conforme con la normativa. Para ello se deberá atender:

1. La naturaleza;

2. El ámbito;

3. La finalidad del tratamiento; y,

4. Los riesgos.

Esta obligación implica también revisar y actualizar las medidas cuando sea necesario (...)".

85. Del análisis conjunto de las disposiciones legales y reglamentarias previamente examinadas, esta Autoridad determina que el responsable del tratamiento no solo se encuentra obligado a adoptar metodologías de análisis y gestión de riesgos, sino también a definir, implementar, evaluar y acreditar medidas de seguridad que sean adecuadas y proporcionales al contexto del tratamiento, las cuales deben sustentarse necesariamente en un análisis previo, estructurado y documentado de los riesgos, amenazas y vulnerabilidades asociados al tratamiento de datos personales.

86. Bajo este marco normativo, y a partir de la valoración del Informe Técnico–Jurídico Preliminar No. INF-SPDP-ICS-2025-0014, de 13 de mayo de 2025, que consta a foja 19 del expediente administrativo, esta Autoridad advierte que la metodología de riesgos en materia de protección de datos personales ha sido planteada, en términos generales, sobre la base de referencias normativas y técnicas de reconocimiento internacional. En particular, a foja 103 y 104 del expediente se mencionan estándares como la ISO/IEC 27005, orientada a la gestión de riesgos de seguridad de la información; la ISO/IEC 29134, relativa a la evaluación de impacto en la privacidad; así como la metodología MAGERIT, desarrollada por el Gobierno de España, caracterizada por un enfoque estructurado en la identificación de activos, amenazas y salvaguardas. Asimismo, se reconoce la incorporación del marco jurídico nacional, especialmente de la Ley Orgánica de Protección de Datos Personales.

87. No obstante, del análisis efectuado se desprende que la sola referencia a estos estándares y marcos normativos no resulta suficiente para acreditar la efectiva implementación de una metodología de análisis y gestión de riesgos en los términos exigidos por el ordenamiento jurídico, en tanto su mera mención no permite verificar que dichos referentes hayan sido aplicados de manera concreta, adaptada y operativa al tratamiento específico de datos personales objeto de análisis.

88. De igual manera, a partir de la valoración del informe técnico incorporado al expediente específicamente a foja 18, esta Autoridad advierte que, si bien la metodología presentada se estructura correctamente sobre la distinción entre riesgo inherente y riesgo residual, e incorpora una matriz de análisis basada en la combinación de la probabilidad de ocurrencia y el nivel de impacto, su aplicación operativa presenta limitaciones relevantes. En particular, aunque la fórmula de cálculo del riesgo se encuentra definida, su utilización no se ve acompañada de ejemplos prácticos, rangos de valoración previamente estandarizados ni criterios objetivos que permitan sustentar de manera verificable las escalas cualitativas o semicuantitativas empleadas. Esta ausencia de parámetros claros impide garantizar la consistencia del análisis y la trazabilidad de las decisiones adoptadas, especialmente en aquellos supuestos en los que resulta necesario justificar tratamientos de datos personales que comportan un nivel elevado de riesgo.

89. En relación a la aplicación concreta de la metodología de riesgos en materia de datos personales y al resultado de la evaluación de impacto del aplicativo FANFEF constante a foja 18 del expediente, del análisis efectuado por el órgano técnico se desprende que, tras examinar la Evaluación de Impacto en la Protección de Datos Personales (EIPD), el análisis de riesgos realizado por la Federación Ecuatoriana de Fútbol concluye que no se habrían identificado riesgos asociados al tratamiento de datos personales en la plataforma FANFEF. Dicha conclusión supone que, conforme a la metodología aplicada, no subsistiría ningún nivel de exposición a amenazas una vez implementadas las medidas de control previstas.

90. Tal resultado plantea cuestionamientos relevantes a esta autoridad sobre la solidez técnica y metodológica del análisis efectuado, en la medida en que una conclusión de ausencia absoluta de riesgos dificulta comprobar la aplicación efectiva del enfoque basado en riesgos exigido por la normativa de protección de datos personales. En efecto, una Evaluación de Impacto en la Protección de Datos Personales solo cumple su finalidad cuando permite identificar, ponderar y dejar constancia de los riesgos que el tratamiento genera para los derechos y libertades de los titulares, así como sustentar la proporcionalidad y suficiencia de las medidas de seguridad implementadas.

91. Cuando la evaluación concluye que no existe riesgo alguno, se elimina el presupuesto que habilita el propio análisis de proporcionalidad, la adopción de medidas diferenciadas y la revisión continua del tratamiento. En tales condiciones, la EIPD se reduce a un ejercicio de carácter meramente formal, que no permite verificar si el responsable identificó de manera adecuada las amenazas, evaluó su impacto potencial ni gestionó de forma efectiva los riesgos derivados del tratamiento de datos personales.

92. Como consecuencia de lo expuesto, la Evaluación de Impacto en la Protección de Datos Personales pierde su aptitud para acreditar el cumplimiento de las obligaciones normativas y deja de cumplir su función como herramienta preventiva, lo que compromete su idoneidad como instrumento válido en los términos exigidos por la Ley Orgánica de Protección de Datos Personales.

93. En efecto, la determinación de un nivel de riesgo igual a cero dentro de una Evaluación de Impacto en Protección de Datos Personales constituye una deficiencia conceptual de especial gravedad, incompatible con el enfoque basado en riesgos que rige el régimen de protección de datos personales. Desde una perspectiva técnica, el riesgo no puede considerarse inexistente en operaciones de tratamiento de datos personales, en tanto toda actividad de tratamiento implica, por su propia naturaleza, una exposición a amenazas de índole técnica, organizativa, humana o jurídica. Incluso en contextos en los que se han implementado controles robustos y maduros, el riesgo puede ser reducido o mitigado, pero no eliminado de manera absoluta.

94. Sostener la inexistencia total de riesgo evidencia una aplicación incorrecta de los marcos de referencia invocados, tales como la ISO/IEC 27005 y la ISO/IEC 29134, los cuales se fundamentan precisamente en el reconocimiento del riesgo residual como un componente permanente del tratamiento, que debe ser objeto de seguimiento, revisión periódica y mejora continua, con el propósito de garantizar una protección efectiva de los derechos y libertades de los titulares de datos personales.

95. Desde una perspectiva normativa, dicha calificación resulta igualmente incompatible con el enfoque preventivo y basado en riesgos que exige la Ley Orgánica de Protección de

Datos Personales. En particular, el artículo 41 de la LOPDP establece una relación directa entre la determinación de las medidas de seguridad y los riesgos que se derivan del tratamiento de datos personales, de modo que la afirmación de una inexistencia absoluta de riesgo vacía de contenido el análisis de proporcionalidad y rompe la lógica de evaluación, prevención y mitigación continua que debe orientar la gestión de riesgos. De igual forma, esta conclusión incide negativamente en el deber de revisión permanente previsto en el artículo 47 de la LOPDP, debilitando el principio de responsabilidad proactiva que rige la actuación del responsable del tratamiento.

96. Más allá de una eventual inconsistencia aritmética, el resultado alcanzado pone de manifiesto una falencia metodológica de carácter estructural, evidenciada en la aplicación meramente mecánica de la matriz de riesgos, sin un ejercicio de valoración crítica de los resultados ni una adecuada contextualización del tratamiento evaluado. Un esquema metodológico que admite como resultado un riesgo nulo no permite una evaluación real de la naturaleza del tratamiento, de la sensibilidad de los datos personales involucrados ni de la posibilidad, aunque sea mínima, de materialización de amenazas. En el ámbito del cumplimiento regulatorio, este tipo de conclusiones no constituye un indicio de seguridad, sino un síntoma de una evaluación deficiente, con potenciales implicaciones jurídicas.

97. En este contexto, el Informe Técnico No. SPDP-IIT-2025-0024-I, de fecha 11 de noviembre de 2025 constante a foja 173 del expediente, fue emitido en atención al escrito presentado por la FEF el 2 de julio de 2025 constante a foja 113 del expediente, mediante el cual formuló sus descargos respecto de la metodología de análisis y gestión de riesgos en materia de protección de datos personales aplicada al tratamiento vinculado al aplicativo FANFEF. Dicho informe se pronuncia de manera específica sobre dos aspectos: i) el análisis de los descargos presentados por la administrada en relación con determinados cargos formulados durante la actuación previa; y ii) la Evaluación de Impacto de Protección de Datos Personales realizada por la FEF.

98. En relación con el primer aspecto abordado, el informe técnico se pronuncia de manera específica sobre los descargos presentados por la Federación Ecuatoriana de Fútbol respecto de determinados cargos formulados en la fase previa del procedimiento.

99. En cuanto a la alegada falta de diferenciación de activos, esta autoridad verifica que el órgano técnico concluye a foja 71 que, si bien la LOPDP no impone una clasificación rígida ni exige el uso de categorías terminológicas como “activos primarios” o “activos de soporte”, lo jurídicamente relevante es la identificación efectiva de los activos que intervienen en el tratamiento de datos personales. Bajo este criterio, del examen de la Matriz de Registro de Actividades de Tratamiento (RAT) y de la Evaluación de Impacto en Protección de Datos Personales (EIPD) se verificó que la administrada ha identificado tanto los activos que contienen datos personales como aquellos que posibilitan su tratamiento. En consecuencia, el informe técnico determina que la observación formulada inicialmente responde a una diferencia de naturaleza terminológica y no configura, por sí misma, un incumplimiento sustantivo de la obligación legal.

100. Por otra parte, en lo relativo a la supuesta ausencia de taxonomías específicas para la identificación de amenazas, el informe técnico señala que la metodología aplicada por la administrada sí incorpora una clasificación funcional de amenazas, distinguiendo, entre otros elementos, entre amenazas de origen interno y externo, así como vulnerabilidades asociadas al tratamiento de datos personales. Si bien dicha clasificación no se ajusta a una

taxonomía formal estandarizada, el órgano técnico concluye que a foja 171que resulta suficiente para efectos de la identificación de amenazas, descartando que este aspecto, considerado de manera aislada, comprometa la validez de la metodología empleada o configure un incumplimiento normativo.

101. En relación con los argumentos mediante los cuales se ha pretendido justificar el cumplimiento de las obligaciones en materia de protección de datos personales a través de la invocación de estándares de seguridad de la información como la ISO/IEC 27005, orientada a la gestión de riesgos de seguridad de la información; la ISO/IEC 29134, relativa a la evaluación de impacto en la privacidad; y la metodología MAGERIT alegada a fojas 103 y 104, resulta necesario efectuar una precisión conceptual de fondo. En efecto, una metodología de análisis y gestión de riesgos en seguridad de la información no es equivalente, ni puede asimilarse sin más, a una metodología de análisis y gestión de riesgos en protección de datos personales. Si bien ambas comparten ciertos elementos estructurales y un lenguaje común, difieren sustancialmente en su objeto de protección, en los vectores de análisis que emplean y en los criterios conforme a los cuales se valora el riesgo.

102. La seguridad de la información constituye, sin duda, un componente transversal e interdependiente de la protección de datos personales, en la medida en que vulneraciones a la confidencialidad, integridad o disponibilidad de los sistemas que soportan el tratamiento pueden derivar en afectaciones a los derechos de los titulares. No obstante, esta relación técnica no autoriza a subsumir una disciplina en la otra ni a trasladar de manera mecánica marcos de referencia propios de la seguridad de la información, como ISO 27001 o ISO 27005, sin una reconfiguración metodológica acorde con la finalidad tutelar propia del régimen de protección de datos personales. En este ámbito, lo que debe garantizar una metodología de riesgos no es únicamente la preservación de activos informacionales frente a amenazas técnicas, sino la protección efectiva de los derechos y libertades de las personas frente a los riesgos inherentes al tratamiento de sus datos personales.

103. Esta distinción no reviste un carácter meramente teórico, sino que incide directamente en la validez del instrumento metodológico y en su idoneidad para cumplir la función que el ordenamiento jurídico le asigna. Mientras que la gestión de riesgos de seguridad de la información sitúa a la organización como eje central del análisis y orienta la protección hacia sus activos como, infraestructura tecnológica, sistemas, aplicaciones, bases de datos, redes y comunicaciones, priorizando la preservación de su confidencialidad, integridad y disponibilidad, la gestión de riesgos en protección de datos personales debe estructurarse desde una lógica distinta. En este último caso, el punto de partida es el titular como sujeto de derechos, y el criterio rector de valoración es el impacto que el tratamiento puede generar en su esfera personal, jurídica y social.

104. Bajo esta óptica, el órgano técnico concluyó a foja 170, que la metodología aplicada incurre en una confusión sustantiva entre la existencia formal de determinados instrumentos y la efectividad real del modelo de gestión de riesgos. En particular, se determinó que la mera presencia de matrices de riesgos, planes de acción o documentos análogos no resulta suficiente para acreditar el cumplimiento de una metodología adecuada, en tanto dichos elementos no sustituyen la necesidad de contar con un esquema de decisión estructurado que permita vincular de forma clara, coherente y verificable los resultados de la evaluación de riesgos con las acciones de gestión adoptadas.

105. El análisis efectuado por esta autoridad pone de manifiesto que la metodología examinada no define umbrales, condiciones ni criterios de decisión, ni establece relaciones de trazabilidad entre la valoración del riesgo y las respuestas adoptadas tales como la mitigación, aceptación, modificación o supresión del tratamiento. En ausencia de estos elementos, las decisiones quedan sujetas al criterio individual de quienes aplican la metodología, lo que priva al modelo de su valor como evidencia objetiva de una gestión de riesgos sistemática, controlada y jurídicamente exigible.

106. A partir de lo anteriormente expuesto, esta Autoridad acoge la conclusión del órgano técnico en el sentido de que la metodología analizada no satisface el estándar técnico exigido por la LOPDP ni por el régimen aplicable a la Evaluación de Impacto en la Protección de Datos Personales. En particular, se constata que dicha metodología no permite acreditar que los resultados del análisis de riesgos se traduzcan en decisiones concretas, coherentes y trazables, orientadas a garantizar de manera efectiva la protección de los derechos y libertades de los titulares de datos personales.

107. En un segundo orden de análisis, el Informe Técnico Jurídico No. SPDP-IIT-2025-0024-I se pronuncia a foja 170 de forma específica sobre la Evaluación de Impacto en la Protección de Datos Personales elaborada por la Federación Ecuatoriana de Fútbol, en atención a los argumentos de descargo formulados por la parte administrada. Del examen de dicha evaluación se desprende que ésta concluye en la asignación de un nivel de riesgo residual igual a cero, conclusión que el administrado pretende sustentar afirmando que dicha calificación no implica la inexistencia del riesgo, sino su adecuado control y monitoreo.

108. No obstante, esta Autoridad, en concordancia con el criterio técnico expuesto, determina que tal razonamiento resulta incompatible con la naturaleza y función de una EIPD, en tanto este instrumento tiene por finalidad identificar, analizar, evaluar y tratar riesgos dentro de un marco necesariamente probabilístico, en el que siempre subsiste un riesgo residual. En este sentido, declarar un riesgo igual a cero no constituye la fijación de un umbral de aceptación del riesgo, sino que impide demostrar que los riesgos han sido efectivamente identificados, analizados y evaluados, así como que las medidas de seguridad adoptadas sean adecuadas y proporcionales al contexto del tratamiento.

109. Esta deficiencia incide de manera directa en la capacidad de la EIPD para cumplir su función preventiva y para servir como herramienta de toma de decisiones informadas, orientadas a la protección efectiva de los derechos y libertades de los titulares de datos personales. En consecuencia, esta Autoridad concluye que los argumentos expuestos por el administrado en sus descargos no logran desvirtuar las observaciones formuladas. La línea argumental desarrollada pretendía sostener que la interpretación efectuada por esta Autoridad respecto de la metodología de gestión de riesgos en protección de datos personales y de la asignación de un resultado de “riesgo igual a cero” constituía un error, al calificarla como reduccionista o meramente semántica. Sin embargo, del análisis integral realizado se evidencia que dicha postura parte de una falsa equivalencia entre los conceptos de “riesgo residual” y “riesgo cero”, al asumir erróneamente que este último podría derivarse de la aplicación de medidas de mitigación, lo cual no resulta compatible con el enfoque basado en riesgos que rige la materia.

110. No obstante, del examen integral de las actuaciones se constata que, a lo largo del procedimiento, el administrado no aportó sustento técnico ni documental que permita respaldar la conclusión de “riesgo cero”, razón por la cual dicha afirmación carece de

fundamento verificable, incluso si se pretende reconducirla conceptualmente al ámbito del riesgo residual. En tales condiciones, la calificación efectuada no satisface los estándares técnicos ni normativos exigidos por el ordenamiento jurídico, configurándose un incumplimiento del principio de seguridad de los datos personales, previsto en el literal j) del artículo 10 de la Ley Orgánica de Protección de Datos Personales.

111. Sobre este punto, resulta pertinente recordar que el artículo 42 de la LOPDP impone la obligación de realizar una Evaluación de Impacto en la Protección de Datos Personales cuando el tratamiento implique un alto riesgo para los derechos y libertades de los titulares. La finalidad de dicho instrumento es evaluar las posibles consecuencias derivadas de la materialización de los riesgos identificados y, sobre esa base, habilitar la adopción de decisiones informadas respecto de la implementación de medidas jurídicas, organizativas y técnicas adecuadas para la protección efectiva de tales derechos.

112. En este contexto, la utilización de una metodología que permite arribar a conclusiones incompatibles con los principios esenciales de la gestión de riesgos y con el marco normativo vigente revela, de manera preliminar, un incumplimiento del deber de emplear metodologías de análisis y gestión de riesgos que sean adecuadas y proporcionales, conforme lo exige la LOPDP.

113. Cabe precisar que la antijuridicidad material de la conducta tipificada en el numeral 4 del artículo 68 de la LOPDP no se sustenta en la inexistencia de una metodología, sino en su ineficacia preventiva. El régimen sancionador no reprocha un déficit meramente documental, esto es, la ausencia de un instrumento formal susceptible de exhibición, sino un déficit funcional, consistente en la implementación de una metodología incapaz de orientar una gestión de riesgos efectiva. Cuando el instrumento empleado no permite identificar riesgos reales, carece de criterios objetivos para su valoración o conduce a conclusiones incompatibles con la naturaleza del tratamiento, como la determinación de un riesgo residual igual a cero, su existencia formal resulta irrelevante a efectos jurídicos.

114. La antijuridicidad se configura, entonces, en la falta de idoneidad estructural del instrumento utilizado: el responsable del tratamiento dispone de una metodología que no anticipa escenarios de posible afectación, no sustenta de manera racional las medidas de seguridad adoptadas y, en definitiva, no garantiza la protección de los derechos y libertades de los titulares de datos personales. El bien jurídico tutelado no resulta lesionado por la producción de un daño concreto, sino por la frustración de la función preventiva que el ordenamiento exige como condición para un tratamiento lícito de datos personales. Este es el nexo causal que sustenta la imputación: la decisión de implementar una metodología funcionalmente inadecuada genera como resultado lesivo la pérdida de la capacidad preventiva que la normativa impone como presupuesto indispensable del tratamiento.

115. Por lo expuesto, esta Autoridad concluye que FEF incurrió en la infracción establecida en el numeral 4) del artículo 68 de la LOPDP, la cual se vincula de manera directa con el incumplimiento de esta obligación, en tanto constituye un requisito previo, expreso y exigible para la adopción de medidas de seguridad adecuadas y para la garantía efectiva de los derechos de los titulares de datos personales.

VI. DETERMINACIÓN DE LAS MEDIDAS CORRECTIVAS

116. Mediante Providencia No. PVD-SPDP-ICS-2025-0064 notificada el 02 de junio de 2025 se puso en conocimiento de la parte administrada el Informe Técnico-Jurídico No. INF-SPDPICS-2025-0014 fecha 13 de mayo de 2025 dentro de la Actuación Previa No. SPDP-IGCS-2024- AP-008-PV, el cual señala dentro de sus recomendaciones las presuntas infracciones identificadas y la sugerencia de imposición de medidas correctivas.

117. Conforme se recoge en el Informe de Supervisión del Cumplimiento de Medidas Correctivas Impuestas a FEF No. INF-SPDP-ICS-2025-0020 del 16 de junio de 2025, con Providencia No. PVD-SPDP-ICS-2025-0075 dentro del Expediente No. EXP-SPDP-ICSPAMC-2025-0003, esta Autoridad dispuso acoger las medidas correctivas indicadas en el Informe No. INF-SPDP-ICS-2025-0014 y su cumplimiento.

118. Así mismo, como se recoge en el Informe de Supervisión del Cumplimiento de Medidas Correctivas Impuestas a FEF, informe No. INF-SPDP-ICS-2025-0020 del 16 de junio de 2025, a través de Providencia No. PVD-SPDP-ICS-2025-0074 notificada el 13 de junio de 2025, la SPDP dispuso el cierre del término otorgado para la implementación de las medidas correctivas y que la Supervisora del Cumplimiento de Medidas Correctivas elabore su correspondiente Informe en el término de un (1) día para la continuación de dicho procedimiento.

119. Con Providencia No. PVD-SPDP-ICS-2025-0075 notificada el 16 de junio de 2025, esta Autoridad dispuso acoger la recomendación de terminación del Procedimiento de Medidas Correctivas No. EXP-SPDP-ICS-PAMC-2025-0003 según Informe de Supervisión del Cumplimiento de Medidas Correctivas Impuestas a FEF No. INF-SPDP-ICS-2025-0020 del 16 de junio de 2025, en donde se detallaron que todas las medidas correctivas dispuestas fueron incumplidas.

120. De conformidad con el artículo 65 de la LOPDP, la SPDP tiene la facultad y atribución para expedir medidas correctivas que tengan por objeto evitar que se continúe cometiendo la infracción y que la conducta se produzca nuevamente; además de corregir, revertir o eliminar, previo informe de la unidad administrativa respectiva, frente al incumplimiento de la normativa de protección de datos personales.

121. En otro aspecto, el numeral 2) del artículo 66 de la LOPDP establece que en caso de que las medidas correctivas impuestas al administrado fueren cumplidas de forma tardía, parcial o defectuosa, esta Autoridad deberá aplicar las sanciones correspondientes a infracciones graves a través del procedimiento administrativo sancionador y que junto con la presente Resolución se hará constar las medidas correctivas aplicables como la sanción respectiva según la infracción cometida.

122. Dentro del análisis para la expedición de la presente Resolución, lo señalado en los párrafos anteriores constituyen motivos por los cuales las medidas correctivas aplicables incumplidas, previamente por el administrado, deben ser aplicadas junto con la sanción que se imponga.

VII. DETERMINACIÓN DE LA SANCIÓN

123. Conforme a lo dispuesto en el artículo 72 de la LOPDP, una vez verificado el cometimiento de una infracción grave, corresponde a esta Autoridad imponer la sanción

administrativa que prevé la norma. Dicho artículo establece textualmente que: *"[...] si el responsable, encargado del tratamiento de datos personales o de ser el caso un tercero, es una entidad de derecho privado o una empresa pública se aplicará una multa de entre el 0.7% y el 1% calculada sobre su volumen de negocios, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa. La Autoridad de Protección de Datos Personales establecerá la multa aplicable en función del principio de proporcionalidad [...]".*

124. En el presente caso, el procedimiento administrativo sancionador se ha iniciado en contra de la FEF por el presunto cometimiento de la infracción prevista en el numeral 4) del artículo 68 de la LOPDP, el cual determina de manera expresa: *"(...) 4) No utilizar metodologías de análisis y gestión de riesgos adaptadas a la naturaleza de los datos personales las particularidades del tratamiento y de las partes involucradas (...)";*

125. El artículo 73 de la LOPDP define al volumen del negocio como: *"(...) la cuantía resultante de la venta de productos y de la prestación de servicios realizados por operadores económicos, durante el último ejercicio que corresponda a sus actividades, previa deducción del Impuesto al Valor Agregado y de otros impuestos directamente relacionados con la operación económica (...)*".

126. Para la correcta determinación del volumen del negocio, mediante Providencia No. PVDSPDP-ICS-2025-0153 de fecha 19 de septiembre de 2025, la funcionaria instructora dispuso la suspensión de términos y plazos a fin de requerir al SRI, como autoridad tributaria competente, la remisión de la información declarada en los casilleros correspondientes a la venta de productos y a la prestación de servicios realizada por la parte administrada durante el ejercicio fiscal 2024. Tales casilleros, por su propia naturaleza, se encuentran exentos del Impuesto al Valor Agregado, lo que permite identificar con precisión el volumen de operaciones generadas por el administrado. Esta información resulta indispensable para establecer el volumen de negocios conforme exige el artículo 72 de la LOPDP.

127. Mediante Oficio No. 917012025OACN0004320, de fecha 21 de octubre de 2025, el SRI remitió a esta Autoridad la totalidad de la información requerida, permitiendo proceder al cálculo de la sanción aplicable, de conformidad con lo dispuesto en la LOPDP, así como en el Modelo para el Cálculo de Multas Administrativas, aprobado mediante Resolución No. SPDPSPD-2025-0022-R:

SOBRE EL VOLUMEN DEL NEGOCIO

128. De conformidad con la información recopilada por esta Autoridad, el volumen de negocio a utilizar para efectos del cálculo de la sanción corresponde a USD [redacted]

SOBRE LA CATEGORÍA DE LA INFRACCIÓN

Rango de la multa

129. Conforme a lo dispuesto en el régimen sancionatorio de la LOPDP, las infracciones administrativas pueden clasificarse como leves o graves. En el presente caso, la conducta

atribuida a la FEF corresponde a la infracción prevista en el numeral 4) del artículo 68 de la LOPDP, la cual se encuentra categorizada expresamente por la Ley como una infracción grave, activando con ello el régimen sancionatorio aplicable a esta clase de incumplimientos.

130. El rango aplicable para una infracción grave está expresamente previsto en el tercer inciso del artículo 72 de la LOPDP, que dispone que la multa debe situarse entre el 0,7% y el 1% del volumen de negocio correspondiente al ejercicio fiscal inmediatamente anterior a su imposición, cuando el responsable del tratamiento sea una entidad de derecho privado. Este margen constituye el parámetro legal dentro del cual la Autoridad debe graduar la sanción, observando el principio de proporcionalidad.

Peso de la infracción

131. El peso de la infracción constituye un parámetro esencial para estimar el impacto regulatorio derivado del incumplimiento, y comprende tanto el grado de madurez de conformidad con la LOPDP; así como las medidas correctivas implementadas, de ser el caso. A continuación, su análisis:

Medidas Correctivas

132. A foja 10 del expediente sancionador consta la copia del Informe de Supervisión de Medidas Correctivas No. INF-SPDP-ICS-2025-0020 de fecha 16 de junio de 2025, emitida dentro del procedimiento de medidas correctivas signado con el No. EXP-SPDP-ICS-PAMC-0003, mediante la que se dispuso la adopción de una (1) medida correctiva relacionada a la metodología de riesgos y evaluación de impacto de protección de datos y en dicho informe la funcionaria encargada de la supervisión del cumplimiento de las medidas correctivas verificó el incumplimiento de la medida dispuesta.

Grado de Madurez

133. En el presente caso, se evidencia que el responsable del tratamiento no alcanzó un nivel adecuado de madurez regulatoria respecto de la obligación de aplicar metodologías de análisis y gestión de riesgos adaptadas a la naturaleza de los datos personales, las características del tratamiento y las partes involucradas.

134. La gestión de riesgos constituye un pilar esencial del modelo preventivo previsto en la LOPDP, ya que permite anticipar, evaluar y mitigar los impactos que el tratamiento de datos personales puede generar sobre los derechos y libertades de los titulares. Sin embargo, del análisis realizado se desprende que la metodología utilizada carece de la estructura, profundidad y coherencia necesarias para cumplir esta función preventiva, limitándose a una formulación meramente formal, sin traducirse en decisiones de gestión verificables ni en medidas de seguridad debidamente justificadas.

135. Esta falta de madurez se refleja, entre otros aspectos, la incapacidad para identificar y valorar razonablemente los riesgos asociados al tratamiento, llegando incluso a conclusiones incompatibles con el enfoque basado en riesgos, como la determinación de un riesgo residual igual a cero y la ausencia de criterios objetivos, umbrales de decisión y mecanismos de trazabilidad que permitan vincular los resultados del análisis con

acciones concretas de mitigación, aceptación, modificación o eliminación del tratamiento.

136. Lo anterior demuestra que el modelo adoptado no operó como un verdadero instrumento decisional, sino como un esquema aplicado de manera mecánica, sin una valoración crítica ni contextual del tratamiento evaluado.

137. Todo lo anterior permite concluir que el responsable del tratamiento no contaba con una metodología de análisis y gestión de riesgos técnicamente idónea ni jurídicamente adecuada, capaz de sostener una gestión preventiva y continua conforme a los estándares exigidos por la LOPDP. Si bien el responsable invocó estándares y marcos de referencia reconocidos, la madurez regulatoria no se acredita mediante referencias formales, sino a través de la aplicación efectiva y contextualizada de una metodología funcional. Por ello, la deficiente implementación de una metodología de análisis y gestión de riesgos confirma un bajo grado de madurez, en relación con la infracción prevista en el numeral 4 del artículo 68 de la LOPDP.

SERIEDAD DE LA INFRACCIÓN

Impacto de derechos

138. Es el factor que considera el impacto que pueden sufrir los titulares de datos personales ante la infracción cometida por un responsable o encargado del tratamiento. Este impacto se estima en función de los siguientes cuatro factores: 1) tipos de datos personales; 2) número de titulares afectados y volumen de datos; 3) naturaleza de la vulneración; y 4) grupos de titulares especialmente vulnerables. La ponderación de estos elementos permite determinar la magnitud del riesgo o afectación generada por el incumplimiento identificado:

Tipos de datos personales

139. Los datos personales tratados por FEF a través del sistema FAN FEF comprenden datos personales de carácter general que hacen identificables a las personas naturales de manera directa.

Número de titulares afectados y volumen de datos

140. De la revisión íntegra del expediente, esta Autoridad no ha podido determinar un número específico de titulares cuyos datos personales pudieron haberse visto afectados. No obstante, esta ausencia de cuantificación no afecta la verificación ni la configuración jurídica de la infracción, puesto que el número de titulares únicamente incide en la determinación de agravantes o atenuantes dentro de la graduación de la sanción, mas no en el cometimiento mismo de la conducta infractora.

Naturaleza de la infracción

141. En lo que respecta a la naturaleza de la vulneración, esta Autoridad advierte que la conducta atribuida al responsable del tratamiento se manifiesta en deficiencias sustanciales vinculadas al cumplimiento del deber de utilizar metodologías adecuadas y proporcionales de análisis y gestión de riesgos en materia de protección de datos

personales. En particular, se constató que la metodología aplicada no permite identificar, evaluar ni documentar de manera razonable los riesgos derivados del tratamiento, ni traducir los resultados del análisis en decisiones coherentes y verificables orientadas a la adopción de medidas de seguridad efectivas. La asignación de un resultado de "riesgo residual igual a cero" conforme consta a foja 102 del expediente, la ausencia de criterios objetivos de valoración, de umbrales de decisión y de mecanismos de trazabilidad entre riesgos y medidas, evidencian que el tratamiento carece de un soporte metodológico idóneo conforme a las exigencias de la LOPDP.

142. La vulneración constatada no se limita a una falencia puntual o aislada, sino que incide de manera estructural en el modelo de gestión de riesgos del tratamiento, afectando etapas esenciales como la evaluación previa de riesgos, la determinación de medidas de seguridad, la revisión continua del tratamiento y la capacidad de demostrar cumplimiento normativo. Esta situación compromete la función preventiva que la normativa asigna a la gestión de riesgos y a la Evaluación de Impacto en la Protección de Datos Personales, generando un escenario en el que los riesgos inherentes al tratamiento no son adecuadamente identificados ni gestionados, lo que incrementa la exposición de los titulares a posibles afectaciones de sus derechos y libertades.

143. En consecuencia, la vulneración analizada constituye una afectación grave y sustantiva al principio de seguridad de los datos personales y al enfoque preventivo basado en riesgos que rige el régimen de protección de datos personales, al evidenciar que el tratamiento se ejecutó sin contar con una metodología funcionalmente idónea que permita anticipar escenarios de riesgo, justificar la proporcionalidad de las medidas adoptadas y garantizar una gestión continua y responsable del tratamiento. Ello incrementa de manera significativa los riesgos para los derechos de los titulares, en tanto las garantías mínimas exigidas por la normativa para un tratamiento lícito y seguro no fueron implementadas de forma efectiva

Grupos de titulares especialmente vulnerables

144. Respecto a los grupos de titulares especialmente vulnerables, esta Autoridad no ha verificado la existencia de tales grupos dentro del universo de afectados, ni consta en el expediente información aportada por la parte administrada que permita identificar o corroborar la presencia de titulares que puedan ser considerados especialmente vulnerables conforme a los criterios previstos en la normativa aplicable por lo que dicho criterio no será considerado en la valoración del impacto de derechos.

Intencionalidad

145. En relación con el criterio de intencionalidad para la valoración de la gravedad de la infracción, corresponde precisar que este no se limita a la existencia de una voluntad consciente de infringir la normativa, sino que también comprende la conducta del responsable cuando, aun sin una intención directa de incumplir, actúa sin observar el nivel de diligencia que la Ley Orgánica de Protección de Datos Personales exige en función de la naturaleza del tratamiento y de los riesgos asociados. En este sentido, la infracción no intencional se configura cuando el responsable omite adoptar las medidas razonablemente exigibles para garantizar el cumplimiento efectivo de sus obligaciones legales.

146. En el presente caso, del análisis integral del expediente se evidencia que la conducta del responsable del tratamiento no se sustenta en una actuación orientada al cumplimiento

diligente de la obligación de implementar metodologías adecuadas y proporcionales de análisis y gestión de riesgos. Si bien el responsable invocó la existencia de metodologías, estándares internacionales y herramientas de gestión de riesgos, así como la realización formal de una Evaluación de Impacto en la Protección de Datos Personales, la forma en que dichos instrumentos fueron aplicados revela una falta de diligencia relevante en su diseño, ejecución y validación

147. En particular, la adopción de una metodología que concluye en la inexistencia de riesgo residual, sin respaldo técnico ni documental suficiente, así como la ausencia de criterios objetivos de valoración, umbrales de decisión y mecanismos de trazabilidad entre los riesgos identificados y las medidas adoptadas, ponen de manifiesto que el responsable no verificó de manera adecuada la idoneidad y eficacia del modelo aplicado. Esta conducta evidencia una omisión en el cumplimiento del deber de diligencia que rige la gestión de riesgos en materia de protección de datos personales, especialmente cuando el tratamiento involucra datos que pueden generar impactos relevantes en los derechos y libertades de los titulares.

148. En consecuencia, aun cuando no se advierte una actuación dirigida a infringir deliberadamente la normativa, la conducta analizada resulta jurídicamente reprochable por cuanto el responsable asumió el tratamiento de datos personales sin asegurar que la metodología empleada fuese técnicamente adecuada y funcionalmente eficaz para cumplir su finalidad preventiva. Esta falta de diligencia resulta relevante para la valoración de la gravedad de la infracción prevista en el numeral 4 del artículo 68 de la LOPDP, al haber comprometido la capacidad del tratamiento para anticipar, evaluar y mitigar los riesgos derivados del tratamiento de datos personales.

REITERACIÓN Y REINCIDENCIA

149. En cuanto al criterio de reiteración y reincidencia, esta Autoridad procede a efectuar la valoración conforme a lo dispuesto en el artículo 71 numeral 2 literal b) de la LOPDP, el cual establece que existe reiteración cuando el responsable del tratamiento de datos personales ha sido previamente sancionado por dos o más infracciones de menor gravedad, o cuando ha sido sancionado con anterioridad por una infracción cuya sanción sea de igual o mayor gravedad a la que se pretende aplicar.

150. De conformidad con la certificación emitida por la Dirección de Asesoría Jurídica mediante Memorando No. SPDP-DAJ-2025-0135-M de fecha 30 de diciembre de 2025, se verifica que en contra de la Resolución No. RES-SPDP-ICS-2025-0003 ha sido interpuesto recurso de apelación. En consecuencia, al no haber causado estado dicho acto administrativo, el mismo no será considerado como antecedente ni tomado en cuenta para efectos del cálculo de la sanción en el presente procedimiento.

151. Una vez ponderados en su conjunto los criterios de graduación aplicables, esta Autoridad utilizó el sistema informático institucional que permitirá la aplicación del Anexo I en los procesos administrativos sancionadores denominado “Mpriv”, elaborado por la Intendencia General de Innovación Tecnológica y Seguridad de Datos Personales de conformidad con la Disposición Transitoria de la Resolución No. SPDP-SPD-2025-0022-R.

152. Tras aplicar la metodología sancionadora y una vez incorporados los valores pertinentes en cada uno de los campos correspondientes, el sistema genera una curva de distribución de probabilidades Monte Carlo con sus valores mínimo, medio y máximo, conforme a la tabla que se presenta a continuación:

153. Sobre esta base, y con el propósito de reducir la discrecionalidad en la determinación de la sanción, esta Autoridad adopta el valor medio como referencia para la fijación de la multa, al considerarlo el parámetro más equitativo. En virtud de ello, el valor de la sanción determinado por esta Autoridad asciende a USD$ 194,496.85 (Ciento noventa y cuatro mil cuatrocientos noventa y seis dólares de los Estados Unidos de América con ochenta y cinco centavos).

VIII. RESOLUCIÓN

En ejercicio de las atribuciones constitucionales, legales y reglamentarias conferidas a este funcionario resolutor, esta Autoridad **RESUELVE**:

154. **DECLARAR** la responsabilidad administrativa de **FEDERACIÓN ECUATORIANA DE FÚTBOL** con **RUC No. 0990986665001**, como responsable del cometimiento de la infracción tipificada en el numeral 4) del artículo 68 de la LOPDP.

155. **IMPONER** la sanción administrativa a **FEDERACIÓN ECUATORIANA DE FÚTBOL con RUC No. 0990986665001**, aplicando la multa de USD$ 194,496.85 (Ciento noventa y cuatro mil cuatrocientos noventa y seis dólares de los Estados Unidos de América con ochenta y cinco centavos).

156. **INFORMAR** a **FEDERACIÓN ECUATORIANA DE FÚTBOL con RUC No. 0990986665001**, que el pago de la multa impuesta en este procedimiento administrativo sancionador, deberá ser realizado en el término de diez (10) días contados a partir de la notificación de la presente Resolución, previniendo que de no hacerlo se procederá con la ejecución coactiva de conformidad con lo establecido en el artículo 271 del COA.

1. **REQUERIR** a **FEDERACIÓN ECUATORIANA DE FÚTBOL con RUC No. 0990986665001**, el cumplimiento de las siguientes medidas correctivas: a) Reformular la metodología de riesgos y evaluación de impacto para que se calibre de manera adecuada los componentes que erróneamente concluyen en la evaluación de impacto los riesgos

con resultado cero, conforme a la normativa vigente en materia de protección de datos personales. **LA FEF** deberá cumplir y demostrar en el plazo de UN (1) mes lo señalado en este numeral, contado a partir de la notificación de la presente Resolución; previniendo que de no ser así se dictarán las medidas cautelares necesarias para garantizar su cumplimiento.

IX. MEDIDAS CAUTELARES PARA LA EFICACIA DE LA RESOLUCIÓN

157. En el presente caso, esta Autoridad no ha ordenado la aplicación de ninguna de las medidas cautelares previstas en el artículo 189 del COA.

158. Notificar la presente Resolución a la parte administrada al correo electrónico: [redacted] **CÚMPLASE, OFÍCIESE Y NOTIFÍQUESE. –**

AB. RENÉ ORBE PACHECO
INTENDENTE GENERAL DE CONTROL Y SANCIÓN
SUPERINTENDENCIA DE PROTECCIÓN DE DATOS PERSONALES