CONTENIDO

POLITICA DE TRATAMIENTO DE LA INFORMACIÓN – PTI

FOSCAL, persona jurídica identificada con Nit. 890.205.361-4 y cuyo domicilio social se encuentra ubicado en Floridablanca, departamento de Santander, debidamente constituida de conformidad con las leyes de la República de Colombia, ha desarrollado la política incorporada en el presente documento, para ser aplicada en el manejo de la información que sea tratada por la organización de acuerdo a la Ley 1581 de 2012 y su Decreto reglamentario.

FOSCAL cuenta con normas y procedimientos de seguridad, donde el objetivo principal es asegurar la confidencialidad, integridad y disponibilidad de la información y bases de datos de nuestros miembros de la organización y terceros, lo mismo que asegurar la estabilidad, disponibilidad de la infraestructura tecnológica y la operación.

Todas las medidas de seguridad que ha implementado y gestiona FOSCAL, buscan la protección de la información y la garantía de la dignidad de los titulares de los datos personales que trata. Tales medidas permiten el acceso de los usuarios autorizados de forma controlada e impiden que los no autorizados puedan llegar a acceder, bloquear, modificar, adulterar o suprimir la información y/o datos personales tratados por parte de FOSCAL como responsable, encargado o subencargado de los mismos según el caso.

En la presente política, FOSCAL ha instituido los principios, derechos y deberes necesarios para brindarle protección a Usted, como titular de los datos personales que se tratan dentro de la organización, de cualquier riesgo de vulneración de sus derechos, con miras a garantizar su Dignidad Humana a partir de la implementación de las medidas necesarias y efectivas para cumplir las obligaciones establecidas en la Ley 1581 de 2012 y su Decreto reglamentario.

En tal sentido, le informamos que este documento contiene las directrices generales que tendremos en cuenta para tratar sus datos personales cuando sean recolectados, almacenados, usados, circulados o suprimidos por nosotros.

1. DESTINATARIOS DE LA POLÍTICA DE TRATAMIENTO DE LA INFORMACIÓN

Esta política se ha establecido para otorgar protección a todas las personas naturales cuyos datos personales se encuentren en las bases de datos de FOSCAL, y tiene como destinatarios a todos los miembros de la organización, ya sea que esta actúe en calidad de responsable, encargada o subencargada del tratamiento de datos personales. Así mismo se destina a terceros que, al relacionarse con la organización, tengan acceso o relación con los datos personales por ella tratados.

2. MATRIZ DE TITULARES, DATOS Y FINALIDADES

Para el normal desarrollo de la misión, compromiso organizacional y el cumplimiento de las obligaciones adquiridas por FOSCAL, realiza el tratamiento (recolección, almacenamiento, uso, circulación y supresión) de los datos personales de los titulares mencionados a continuación, para las finalidades que se referencian en la siguiente tabla:

Tratamiento de Datos Personales por FOSCAL		
Titular	**Descripción**	
Pacientes	Datos personales	Nombre, número de identificación, ocupación, número de historia clínica, dirección, teléfono personal, celular, fecha de nacimiento, lugar de nacimiento, estado civil, dirección de residencia, correo electrónico personal, ocupación, entidad aseguradora, número de la historia clínica, EAPB, edad, género, número de cama, talla, peso, datos de salud, firma, EPS, IPS, tipo de sangre, religión, origen étnico, raza, fotografía, estrato, escolaridad, número de semanas cotizadas, cargo, beneficiario, tipo de régimen, calidad de beneficiario o cotizante, nacionalidad, parentesco, estado de salud, huella digital, discapacidades, condición de desplazado, vacunas, intervenciones quirúrgicas, uso de aparatos (oftalmológicos, ortopédicos, etc.).
	Finalidades	1. Incorporación y actualización de datos en bases de datos institucionales. 2. Elaboración de registros en procedimientos de auditoria. 3. Identificación de pacientes y/o usuarios. 4. Soporte recolección de consentimiento y/o disentimiento informado otorgado por los pacientes y/o usuarios. 5. Ejecución, registro y control de procedimientos, tratamientos, actividades y solicitudes propias de los servicios médicos prestados por la organización a pacientes. 6. Registro de evolución medica de los pacientes. 7. Registro de entrega de resultados médicos a pacientes. 8. Registro de valoraciones medicas realizadas a cada paciente. 9. Recolección de información relacionada con la caída de un paciente. 10. Autorización de servicios médicos a pacientes de conformidad con los contratos estatales vigentes. 11. Verificación del traslado de los pacientes entre servicios de la organización. 12. Autorización a proveedores para la ejecución de servicios. 13. Registro de autorizaciones emitidas por los pacientes para la prestación de servicios ofrecidos por la organización. 14. Registro y monitoreo de la información suministrada a los usuarios relativa a pagos. 15. Registro de información para ingreso de pacientes. 16. Soporte de compromiso de familiares para el pago de medicamentos, materiales, procedimientos y servicios suministrados no cubiertos o no autorizados. 17. Registro para cobro de honorarios médicos. 18. Reporte de incidentes que impliquen agresiones ya sea por parte de los usuarios o de los funcionarios. 19. Registro de lesionados durante emergencias o simulacros. 20. Registro de las personas evacuadas durante emergencias o simulacros. 21. Control de entrega de copias de historias clínicas y cumplimiento de los requisitos de la ley 23 de 1981. 22. Registro de préstamos y devoluciones de historias clínicas. 23. Registro de actividades de personal de atención al paciente y familiares de pacientes 24. Registro de socialización de derechos y deberes a usuarios y pacientes. 25. Medición de la percepción de los pacientes de los servicios prestados por la organización. 26. Registro de proyección de videos

		institucionales. 27. Control de apertura de buzones. 28. Control de ingreso a los servicios de la organización o zonas de acceso restringido. 29. Registro de pacientes beneficiados e ingresados al Programa Social Amigos. 30. Registro de ayudas prestadas a pacientes del Programa Social Amigos. 31. Educación y seguimiento de cancelaciones a pacientes. 32. Evaluación de cumplimiento y adherencia del personal a procedimientos, actividades y medidas de obligatorio cumplimiento. 33. Informe a familiares de los pacientes sobre el estado de estos. 34. Registro del proceso de simulación. 35. Notificación a usuarios de programas educativos. 36. Optimización de servicios de la organización. 37. Identificación de los costos del servicio que deben cancelar los usuarios al momento de solicitarlos 38. Registro y control de los cambios en el tratamiento de pacientes. 39. Notificación a los usuarios de servicios solicitados no contratados. 40. Registro de atención de urgencias. 41. Registro de pagos registrados por los servicios prestados por los profesionales a particulares. 42. Elaboración historias clínicas. 43. Registro de capacitaciones o talleres realizados por los usuarios. 44. Registro y control de peso y talla de menores de edad. 45. Certificación de presunción legal a pacientes que no se opusieron en vida a la donación de componentes anatómicos. 46. Registro y verificación de entendimiento de educación de los usuarios y/o sus familiares. 47. Control de indicadores médicos de pacientes bajo tratamiento u observación. 48. Registro del estado de salud de los pacientes antes, durante y después de la realización de procedimientos médicos. 49. Registro y control de funciones vitales neurológicas en los usuarios que presentan compromiso neurológico. 50. Control de devolución de insumos y medicamentos no utilizados. 51. Evaluación de educación impartida a usuarios, familiares y/o cuidadores sobre prevención de caídas. 52. Soporte de socialización de información y cuidados para prevenir riesgo de caídas a usuarios. 53. Control de inventario. 54. Registro de actividades efectuadas en el marco de programas de la organización. 55. Registro de educación e información otorgada a usuarios y familiares. 56. Registro de decisiones de junta médica. 94. Registro de urgencias 57. Medición de adherencia a manejo de pacientes víctimas de la violencia 58. Registro de resultados, procedimientos y actividades relacionados con el servicio de trasplante de órganos. 59. Elaboración de informes. 60. Registro de entrega de patologías. 61. Soporte de autorización de realización de procedimientos médicos. 62. Reporte de eventos de atención en salud. 63. Registro de requerimientos de información. 64. Verificación de cumplimiento de parámetros de seguridad para la realización de procedimientos médicos. 65. Autorización, prestación y facturación de servicios no incluidos en el POS. 66. Registro de órdenes verbales emitidas por el personal médico. 67. Consignación, registro y notificación de quejas o reclamos, sugerencias y felicitaciones o recomendaciones derivadas de la prestación de servicios en general. 68. Cumplimiento de obligaciones legales y/o contractuales.

Proveedores	Datos personales	Nombre, número de identificación, profesión, edad, fecha de nacimiento, género, dirección, teléfono corporativo, teléfono personal, celular, estado civil, seguridad social, cargo, profesión, registro médico o tarjeta profesional, código postal, certificados de estudio, AFP, EPS, ARL, correo electrónico personal, Inscripción ReTHUS, servicios contratados, firma.
	Finalidades	1. Incorporación y actualización de datos en bases de datos institucionales. 2. Registro de asistencia a reunión. 3. Registro de honorarios para su posterior cobro. 4. Reporte e investigación de incidentes y accidentes de trabajo. 5. Verificación de requisitos general de persona natural que realiza actividades en la organización. 6. Registro de lesionados durante emergencia o simulacro. 7. Registro de personal evacuado durante emergencias o simulacros. 8. Registro de préstamo de historias clínicas y documentos. 9. Suscripción de acuerdo de confidencialidad con terceros. 10. Suscripción de acuerdo de confidencialidad y acceso SAP y RUAF a personal médico que presta servicios médicos en la organización. 11. Notificación de acceso al sistema de información SAP, para funcionarios y personal externo. 12. Notificación de condiciones de privacidad y confidencialidad a personal externo que solicita instalación de SAP en equipos personales. 13. Ejecución, registro y control de procedimientos, tratamientos, actividades y solicitudes propias de los servicios médicos prestados por la organización a pacientes.14. Registro consentimiento y/o disentimiento informado del paciente. 15. Registro de órdenes verbales emitidas por personal médico. 16. Registro de decisiones de junta médica. 17. Control y registro de urgencias. 18. Registro de resultados, procedimientos y actividades relacionados con procedimientos de trasplante de órganos. 19. Registro de gastos en procedimientos médicos para posterior cobro. 20. Elaboración de informes. 21. Ejecución, registro y control de procedimientos, tratamientos, actividades y solicitudes propias de los servicios médicos prestados por la organización a pacientes. 22. Verificación de cumplimiento de parámetros de seguridad para la realización de procedimientos médicos. 23. Reporte de evento de atención en salud. 24. Consignación, registro y notificación de quejas o reclamos, sugerencias y felicitaciones o recomendaciones derivadas de la prestación de servicios en general. 25. Cumplimiento de obligaciones legales y/o contractuales.
Empleados de empresas proveedoras	Datos personales	Nombre, número de identificación, fecha de nacimiento, profesión, correo electrónico institucional, género, huella digital, teléfono personal, teléfono corporativo, celular, datos de salud, cargo, tarjeta profesional, servicios contratados, correo electrónico personal, dirección, firma.

	Finalidades	1. Incorporación y actualización de datos en bases de datos institucionales. 2. Registro de asistencia a reunión. 3. Registro de participación en acciones de formación, inducción o reinducción institucional. 4. Ejecución, verificación, registro y evaluación de actividades y procedimientos propios del Sistema de Seguridad y Salud en el Trabajo de la organización. 5. Registro de lesionados durante emergencias o simulacros. 6. Registro de personas evacuadas durante emergencias o simulacros. 7. Suscripción de acuerdo de confidencialidad con terceros. 8. Notificación de acceso al sistema de información SAP, para funcionarios y personal externo. 9. Notificación de condiciones de privacidad y confidencialidad a personal externo que solicita instalación de SAP en equipos personales. 10. Ejecución, Registro y control de procedimientos, actividades y solicitudes propias de los servicios médicos prestados por la organización a pacientes. 11. Registro de órdenes verbales emitidas por el personal médico. 13. Registro de gastos para posterior cobro. 14. Control de entrega de patologías. 15. Reporte de eventos de atención en salud. 18. Consignación, registro y notificación de quejas o reclamos, sugerencias y felicitaciones o recomendaciones derivadas de la prestación de servicios en general. 16. Cumplimiento de obligaciones legales y/o contractuales
Empleados de empresas clientes	Datos personales	Nombre, número de identificación, género, firma del auditor externo, celular personal, cargo, profesión, correo electrónico institucional, teléfono corporativo, teléfono personal, ocupación, profesión, servicios contratados, tarjeta profesional, fecha de nacimiento, lugar de nacimiento, estado civil, huella digital, firma.
	Finalidades	1. Incorporación y actualización de datos en bases de datos institucionales. 2. Registros en procedimientos de auditoria. 3. Registro de asistencia a reunión. 4. Registro y seguimiento de solicitud de servicios. 5. Registro de participación en acciones de formación, inducción o reinducción institucional 6. Registro de lesionados durante emergencias o simulacros. 7. Registro de personas evacuadas durante emergencias o simulacros. 8. Suscripción de terceros de acuerdo de confidencialidad. 9. Notificación de acceso al sistema de información SAP para funcionarios y personal externo. 10. Notificación de condiciones de privacidad y confidencialidad a personal externo que solicita instalación de SAP en equipos personales. 11. Reporte de eventos de atención en salud. 12. Consignación, registro y notificación de quejas o reclamos, sugerencias y felicitaciones o recomendaciones derivadas de la prestación de servicios en general. 13. Cumplimiento de obligaciones legales y/o contractuales.
Familiares de pacientes	Datos personales	Nombre, número de identificación, parentesco, teléfono personal, celular personal, dirección, edad, correo electrónico personal, EPS, aseguradora, género, firma.

	Finalidades	1. Incorporación y actualización de datos en bases de datos institucionales. 2. Registro de autorizaciones emitidas por el paciente para la prestación de servicios. 3. Registro y monitoreo de información suministrada a los usuarios. 4. Ejecución, registro y control de procedimientos, tratamientos, actividades y solicitudes propias de los servicios médicos prestados por la organización a pacientes. 5. Soporte de autorización de los pacientes para la realización de acciones médicas. 6. Soporte de compromiso de familiares para el pago de medicamentos, materiales, procedimientos y servicios suministrados no cubiertos o no autorizados. 7. Reporte de incidentes que impliquen agresión por parte de los usuarios o de los funcionarios. 8. Registro de lesionados durante emergencias o simulacros. 9. Registro de personas evacuadas durante emergencias o simulacros. 10. Control de préstamo de historias clínicas. 11. Autorización de ingreso de familiares en horario diferenciado. 12. Registro de socialización de derechos y deberes a pacientes y familiares. 13. Medición del nivel de percepción de los pacientes que recibieron servicios en la organización. 14. Registro de proyección de videos institucionales. 15. Registro de contenido de buzones. 16. Registro de familiares de pacientes beneficiarios del Programa Social Amigos. 17. Registro de ayudas otorgadas a los familiares de pacientes beneficiarios del Programa Social Amigos. 18. Educación y seguimiento de pacientes. 19. Información a familiares de pacientes quirúrgicos. 20. Registro de consentimiento informado. 21. Registro de disentimiento informado. 22. Verificación de entendimiento de educación a pacientes y/o familiares. 23. Soporte de consentimiento informado del paciente. 24. Verificación y registro de ofrecimiento de información y cuidados para prevenir el riesgo de caídas en usuarios y usuarios pediátricos. 25. Registro de actividades del personal médico. 26. Soporte de la información ofrecida al usuario y a su familiar. 27. Registro y control de la educación brindada a los cuidadores de los pacientes. 28. Reporte de eventos de atención en salud. 29. Consignación, registro y notificación de quejas o reclamos, sugerencias y felicitaciones o recomendaciones derivadas de la prestación de servicios en general. 30. Cumplimiento de obligaciones legales y/o contractuales.
Cuidadores de paciente	Datos personales	Nombre, número de identificación, parentesco, aseguradora, género, teléfono personal, celular personal edad, EPS, dirección, correo electrónico, huella digital, género, firma.

	Finalidades	1. Incorporación y actualización de datos en bases de datos institucionales. 2. Soporte de autorización de los pacientes para la realización de acciones médicas. 3. Soporte de compromiso de familiares para el pago de medicamentos, materiales, procedimientos y servicios suministrados no cubiertos o no autorizados. 4. Reporte de incidentes que impliquen agresión por parte de los usuarios o de los funcionarios. 5. Registro de lesionados durante emergencias o simulacros. 6. Registro de personas evacuadas durante emergencias o simulacros. 7. Soporte de préstamo de historias clínicas y documentos. 8. Registro de socialización de derechos y deberes a pacientes y familiares. 9. Medición del nivel de percepción de los pacientes que recibieron servicios en la organización. 10. Registro de familiares de pacientes beneficiarios del Programa Social Amigos. 11. Registro de ayudas otorgadas a los familiares de pacientes beneficiarios del Programa Social Amigos. 12. Registro de consentimiento y/o disentimiento informado. 13. Verificación de entendimiento de educación a pacientes y/o familiares. 14. Verificación y registro de ofrecimiento de información y cuidados para prevenir el riesgo de caídas en usuarios y usuarios pediátricos. 15. Registro de Educación a usuarios del plan de egreso hospitalario y familiares. 16. Registro y control de la educación brindada por el personal de enfermería a los cuidadores de los pacientes. 17. Reporte de eventos de atención en salud. 18. Consignación, registro y notificación de quejas o reclamos, sugerencias y felicitaciones o recomendaciones derivadas de la prestación de servicios en general. 19. Cumplimiento de obligaciones legales y/o contractuales.
Trabajadores	Datos personales	Nombre, número de identificación, profesión, correo electrónico institucional, teléfono corporativo, títulos, servicios contratados, número de cuenta bancaria, estrato, EAPB, EPS, ARL, AFP, experiencia laboral, afiliación a caja de compensación, tarjeta profesional, correo electrónico personal, estado civil, lugar de nacimiento, fecha de nacimiento, dirección, teléfono personal, hobbies, datos familiares, género, edad, grupo sanguíneo, escolaridad, fotografía, datos de salud ocupacionales, celular, cargo, firma.
	Finalidades	1. Incorporación y actualización de datos en bases de datos institucionales. 2. Ejecución, registro y control de procedimientos, tratamientos, actividades y solicitudes propias de Gestión Interna de la organización. 3. Registro de procesos de Referenciación competitiva solicitadas a la organización. 4. Control de distribución de documentos controlados. 5. Control de análisis de eventos reportados. 6. Registro de asistencia a reuniones.7. Documentación de políticas institucionales. 8. Registro y control de actividades propias del rol o cargo. 9. Constancia y monitoreo de eventos reportados a la oficina de atención segura. 10. Registro de realización procedimientos institucionales para el cumplimiento de exigencias legales. 11. Autorización para la prestación de servicios a pacientes que requieren servicios médicos de acuerdo a contratos estatales suscritos. 12. Verificación de cumplimiento por parte de pacientes de requisitos para la realización de procedimientos médicos.

		13. Registro de entrega de paciente a otra institución para manejo. 14. Ejecución, verificación y registro de actividades y procedimientos internos propios de la Gestión del Talento Humano de la organización. 15. Registro de participación en acciones de formación, inducción o reinducción institucional. 16. Ejecución, verificación, registro y evaluación de actividades y procedimientos propios del Sistema de Seguridad y Salud en el Trabajo de la organización. 17. Verificación de cumplimiento de procedimiento de movilización de pacientes. 18. Verificación de requisitos generales de persona natural. 19. Registro de lesionados durante emergencias o simulacros. 20. Registro de personas evacuadas durante emergencias o simulacros. 21. Soporte de aceptación de participación dentro del programa de manejo de riesgos psicosociales. 22. Soporte de autorización de eliminación de documentos. 23. Soporte de préstamo de historias clínicas y documentos. 24. Autorización y control de ingreso de familiares de pacientes en horarios diferenciados. 25. Suscripción de acuerdo de confidencialidad por parte del personal de nómina. 26. Suscripción de acuerdo de confidencialidad y acceso SAP y RUAF. 27. Notificación a funcionarios y personal externo de recomendaciones sobre instalación de SAP en equipos personales. 28. Control de ingreso de familiares de pacientes a servicios o instalaciones de la organización. 29. Evaluación de adherencia del personal de enfermería a procedimientos o medidas de obligatorio cumplimiento. 30. Información a familiares de pacientes de la organización. 31. Identificación de usuarios que no pueden acceder a servicios de la organización. 32. Control de entrega de historias clínicas. 33. Soporte de consentimiento o disentimiento informado. 34. Certificación de presunción legal de donación de órganos. 35. Registro y control de indicadores y datos médicos de los pacientes. 36. Verificación de traslado de pacientes entre servicios. 37. Control de inventario. 38. Valoraciones medicas a usuarios o pacientes. 39. Registro de órdenes verbales emitidas por el personal médico. 40. Verificación de cumplimiento de parámetros de seguridad para la realización de procedimientos médicos. 41. Registro de decisiones de junta médica. 42. Establecimiento de nivel de cumplimiento de procedimiento de manejo de usuarios víctimas de violencia. 43. Registro de resultados, procedimientos y actividades relacionados con el servicio de trasplante de órganos. 44. Ejecución, registro y control de resultados, procedimientos y actividades de la Unidad de Estudios Clínicos. 45. Registro de visitas. 46. Suscripción de acuerdo de confidencial con equipo de investigaciones. 46. Registro de órdenes verbales. 47. Elaboración de registros para casos de contingencia. 48. Control de información a familiares usuarios. 49. Reporte de evento de atención en salud. 50. Ejecución, registro y control de procedimientos, tratamientos, actividades y solicitudes propias de los servicios médicos prestados por la organización a pacientes. 51. Consignación, registro y notificación de quejas o reclamos, sugerencias y felicitaciones o recomendaciones derivadas de la prestación de servicios en general. 52. Cumplimiento de obligaciones legales y/o contractuales.

Familiares de trabajadores	Datos personales	Nombre, número de identificación, dirección, correo electrónico personal, fecha de nacimiento, parentesco, nacionalidad, teléfono personal, origen étnico, fotografía, género.
	Finalidades	1. Incorporación y actualización de datos en bases de datos institucionales. 2. Registro de lesionados durante emergencias o simulacros. 3. Consignación, registro y notificación de quejas o reclamos, sugerencias y felicitaciones o recomendaciones derivadas de la prestación de servicios en general. 4. Cumplimiento de obligaciones legales y/o contractuales.
Estudiantes	Datos personales	Nombre, número de identificación, género, fotografía, teléfono personal, celular, entidad educativa, firma.
	Finalidades	1. Incorporación y actualización de datos en bases de datos institucionales. 2. Registro de participación en acciones de formación, inducción o reinducción institucional. 3. Verificación de documentos requeridos para el proceso de vinculación a las prácticas empresariales. 4. Registro de lesionados durante emergencias o simulacros. 5. Registro de personas evacuadas durante emergencias o simulacros. 6. Suscripción con terceros de acuerdo de confidencialidad. 7. Evaluación de opinión de los estudiantes con relación al desarrollo de la práctica docente. 8. Reporte de eventos de atención en salud. 9. Consignación, registro y notificación de quejas o reclamos, sugerencias y felicitaciones o recomendaciones derivadas de la prestación de servicios en general.10. Cumplimiento de obligaciones legales y/o contractuales.
Docentes	Datos personales	Nombre, número de identificación, género, teléfono personal, celular, fotografía, firma.
	Finalidades	1. Incorporación y actualización de datos en bases de datos institucionales. 2. Registro de participación en acciones de formación, inducción o reinducción institucional 3. Registro de lesionados en emergencias o simulacros. 4. Registro de personas evacuadas durante emergencias o simulacros. 5. Evaluación de opinión de docentes con relación al desarrollo de la práctica docente. 6. Reporte de eventos de atención en salud. 7. Consignación, registro y notificación de quejas o reclamos, sugerencias y felicitaciones o recomendaciones derivadas de la prestación de servicios en general. 8. Cumplimiento de obligaciones legales y/o contractuales.

Aspirantes a trabajadores	Datos personales	Nombre, número de identificación, profesión, referencias laborales, referencias personales, experiencia laboral, número de cuenta bancaria, títulos, datos familiares, hobbies, fotografía, edad, estado civil, escolaridad, profesión, género, grupo sanguíneo, fecha de nacimiento, lugar de nacimiento, barrio, dirección, teléfono personal, celular, datos de salud, firma.
	Finalidades	1. Incorporación y actualización de datos en bases de datos institucionales. 2. Evaluación por competencias. 3. Ejecución, verificación y registro de actividades y procedimientos internos propios de la Gestión del Talento Humano de la organización. Obtención de información de los aspirantes 4. Evaluación médica ocupacional de los aspirantes. 5. Registro de lesionados durante emergencias o simulacros. 6. Registro de datos de hojas de vida. 7. Consignación, registro y notificación de quejas o reclamos, sugerencias y felicitaciones o recomendaciones derivadas de la prestación de servicios en general. 8. Cumplimiento de obligaciones legales y/o contractuales.
Referenciadores de aspirantes a trabajadores	Datos personales	Nombre, profesión, teléfono personal, celular.
	Finalidades	1. Incorporación y actualización de datos en bases de datos institucionales. 2. Ejecución, verificación y registro de actividades y procedimientos internos propios de la Gestión del Talento Humano de la organización. 3. Consignación, registro y notificación de quejas o reclamos, sugerencias y felicitaciones o recomendaciones derivadas de la prestación de servicios en general. 4. Cumplimiento de obligaciones legales y/o contractuales.
Donantes de órganos	Datos personales	Nombre, número de identificación, nacionalidad, teléfono personal, fecha de nacimiento, lugar de nacimiento, dirección, género, tipo de sangre, peso, talla, origen racial, datos de historia clínica, edad, EPS, IPS, parentesco, datos de salud, firma.
	Finalidades	1. Incorporación y actualización de datos en bases de datos institucionales. 2. Registro de resultados, procedimientos y actividades relacionados con el servicio de trasplante de órganos. 3. Recolección de consentimiento de donación voluntaria. 4. Control de entrega de historias clínicas. 5. Educación a usuarios. 6. Consignación, registro y notificación de quejas o reclamos, sugerencias y felicitaciones o recomendaciones derivadas de la prestación de servicios en general. 7. Cumplimiento de obligaciones legales y/o contractuales.
Donantes financieros	Datos personales	Nombre, número de identificación.

	Finalidades	1. Incorporación y actualización de datos en bases de datos institucionales. 2. Identificación de donante y monto de aporte. 3. Consignación, registro y notificación de quejas o reclamos, sugerencias y felicitaciones o recomendaciones derivadas de la prestación de servicios en general. 4. Cumplimiento de obligaciones legales y/o contractuales.
Sujetos de investigación	Datos personales	Nombre, número de identificación, iniciales, código, edad, peso, género, datos de historia clínica, teléfono personal, celular, firma.
	Finalidades	1. Incorporación y actualización de datos en bases de datos institucionales. 2. Registro de asistencia a reunión. 3. Registro de entrega de consentimiento informado. 4. Ejecución, registro y control de resultados, procedimientos y actividades de la Unidad de Estudios Clínico y de los sujetos de investigación. 5. Evaluación de emergencia o simulacro. 6. Registro de lesionados durante emergencias o simulacros. 7. Registro de entrega de consentimiento informado. 8. Registro de desviaciones a protocolos clínicos. 9. Consignación, registro y notificación de quejas o reclamos, sugerencias y felicitaciones o recomendaciones derivadas de la prestación de servicios en general. 10. Cumplimiento de obligaciones legales y/o contractuales.
Visitantes	Datos personales	Nombre, número de identificación, edad, EPS, ARL, dirección, correo electrónico personal, género, teléfono personal, celular, cargo, firma.
	Finalidades	1. Incorporación y actualización de datos en bases de datos institucionales. 2. Registro de procesos de Referenciación competitiva solicitados a la organización. 3. Ejecución, verificación, registro y evaluación de actividades y procedimientos propios del Sistema de Seguridad y Salud en el Trabajo de la organización. 4. Registro de proyección de videos institucionales. 5. Registro de asistencia a reunión. 6. Consignación, registro y notificación de quejas o reclamos, sugerencias y felicitaciones o recomendaciones derivadas de la prestación de servicios en general. 7. Registro de apertura y contenido de buzones. 8. Suscripción de Acuerdo de Confidencialidad. 9. Control de visitantes. 10. Reporte de eventos de atención en salud. 11. Registro de requerimientos de información. 12. Cumplimiento de obligaciones legales y/o contractuales.

Estos datos personales son tratados conforme a lo ordenado en la Ley 1581 de 2012 y según la clasificación establecida por el artículo 2.2.2.25.1.3 del Decreto 1074 de 2015.

Cuando fuere estrictamente necesario, para efectos del cabal cumplimiento de las operaciones propias de FOSCAL, la organización podrá compartir la información de las bases de datos con proveedores y contratistas en general, entre otros, para lo cual, quien autoriza el tratamiento de los datos, da por hecho conocer esta circunstancia y la acepta de forma libre, previa, expresa e inequívoca, toda vez que su autorización ha sido recolectada conforme a lo dispuesto por la Ley 1581 de 2012 y su Decreto reglamentario,

FOSCAL también podrá:

- Realizar, directa o indirectamente, transmisión o transferencia nacional o internacional de datos, cuando resulte imprescindible para el correcto funcionamiento de la organización. Circunstancia que el titular, al autorizar el tratamiento del dato, acepta con dicho acto, tal proceder.
- Utilizar los datos recolectados a través de puntos de seguridad, personal de seguridad y videograbaciones que se realizan dentro o fuera de las instalaciones de la organización, para fines de seguridad y vigilancia de las personas, bienes e instalaciones de FOSCAL y podrán ser utilizados como prueba en cualquier tipo de proceso judicial o administrativo.
- Soportar procedimientos de auditoría externa e interna.
- Enviar y recepcionar mensajes con fines comerciales, publicitarios y/o de atención al cliente, así como todos los relacionados con ocasión de la relación legal o contractual existente con los Titulares.
- Ceder datos personales a terceros para fines legales y/o contractuales.

3. DISPOSICIONES NORMATIVAS

Esta política está desarrollada en el marco jurídico colombiano de protección de datos personales, constituido por las siguientes disposiciones:

- El artículo 15 de la Constitución Política de Colombia protege los derechos a la intimidad, buen nombre y al Hábeas Data. De esta disposición constitucional, se desprenden las demás normas que reglamentan la protección de datos en Colombia.

- La Ley Estatutaria 1581 del 17 de octubre de 2012 establece las condiciones mínimas para realizar tratamiento legítimo de los datos personales de los titulares de la información personal.

- El Decreto 1074 del 2015 define aspectos puntuales frente a la recolección de datos personales, el contenido de la política de tratamiento de la información y el registro nacional de base de datos, entre otros de los puntos tratados.

- La Circular Externa 02 del 4 de noviembre de 2015 de la Superintendencia de Industria y Comercio.

- El Decreto 1759 del 2016 modifica el artículo 2.2.2.26.3.1 del Decreto 1074 de 2015 ampliando los plazos de inscripción de las bases de datos en el Registro Nacional de Bases de Datos.

4. DEFINICIONES

Para efectos de la interpretación y aplicación de esta política deben tenerse en cuenta los siguientes conceptos:

- **AUTORIZACIÓN**. Consentimiento previo, expreso e informado del titular del dato para llevar a cabo el tratamiento de su información personal.

- **CONSULTA.** Solicitud del titular del dato, de las personas autorizadas por este o por la ley, para conocer la información que reposa sobre él, en bases de datos o archivos de la organización.

- **RECLAMO**. Solicitud del titular del dato, de las personas autorizadas por este o por la ley, para corregir, actualizar o suprimir sus datos personales o para revocar la autorización en los casos establecidos en la ley.

- **RESPONSABLE DEL TRATAMIENTO**. Persona natural o jurídica de naturaleza pública o privada, que decide sobre la recolección y fines del tratamiento de los datos personales. Puede ser, a título de ejemplo, la empresa dueña de la base de datos o sistema de información que contiene datos personales.

- **ENCARGADO DEL TRATAMIENTO.** Persona natural o jurídica, pública o privada que, por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del Tratamiento.

- **SUBENCARGADO DEL TRATAMIENTO**. Persona que realiza el tratamiento de datos personales por cuenta de un Encargado del tratamiento.

- **TITULAR DEL DATO**. Es la persona natural cuyos datos personales son objeto del tratamiento.

- **TRATAMIENTO.** Cualquier operación o conjunto de operaciones sobre datos personales tales como: la recolección, el almacenamiento, el uso, la circulación o supresión de esa clase de información.

- **BASE DE DATOS**. Conjunto organizado, sea físico o digital, de datos personales que sea objeto de Tratamiento.

- **CESIÓN DE LA BASE DE DATOS**. Transferencia de la calidad de responsable de una Base de Datos a otro responsable a título gratuito u oneroso. Se le considerará al nuevo responsable del Tratamiento de la base de datos cedida tal condición a partir del momento en que sea perfeccionada la cesión.

- **TRANSMISIÓN NACIONAL DE DATOS**. Envío de datos personales que realiza el Responsable o el Encargado dentro del territorio nacional a un destinatario que será un responsable o Encargado y cuya operación está cobijada por un negocio jurídico.

- **TRANSFERENCIA INTERNACIONAL DE DATOS**. Envío de datos personales que realiza el Responsable o Encargado desde Colombia a un destinatario que será un responsable que se encuentra fuera del país y cuya operación está cobijada por una declaración de conformidad emitida por la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio o por una causal de excepción en los términos señalados en el artículo 26 de la Ley 1581 de 2012.

- **TRANSMISIÓN INTERNACIONAL DE DATOS**. Envío de datos personales que realiza el responsable desde Colombia a un destinatario que será un Encargado que se encuentra fuera del país y cuya operación está cobijada por un contrato de transmisión de datos en los términos señalados en el artículo 2.2.2.25.5.2 del Decreto 1074 de 2015 o una declaración de conformidad emitida por la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio.

- **NNA**. Hace referencia a los menores de 18 años, y corresponde a la sigla de Niños, Niñas y Adolescentes.

- **DATO PERSONAL**. Cualquier información que directa o indirectamente se refiere a una persona natural y que permite identificarla, estos datos se clasifican en:

- **DATO PERSONAL SENSIBLE.** Información que afecta la intimidad de la persona o cuyo uso indebido puede generar su discriminación, tales como datos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos (huellas dactilares, fotos).

- **DATO PERSONAL PRIVADO**. Es el dato que por su naturaleza íntima o reservada sólo es relevante para la persona Titular del dato. Ejemplos: información extraída a partir de la inspección del domicilio, número telefónico siempre y cuando no se encuentre en bases públicas o el salario. También lo son los datos que reposen en los archivos de la Registraduría, referentes a la identidad de las personas, cómo son sus datos biográficos, su filiación y fórmula dactiloscópica.

- **DATO PERSONAL SEMIPRIVADO**. Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como, entre otros, el dato referente al cumplimiento o incumplimiento de las obligaciones financieras o los datos relativos a las relaciones con las entidades de la seguridad social.

- **DATO PERSONAL PÚBLICO.** Es el dato calificado como tal por ley o la Constitución Política o el que no sea privado, semiprivado o sensible. Son públicos, entre otros, el nombre, el número de identificación, fecha y lugar de expedición del documento de identificación, profesión, calidad de comerciante o de servidor público, datos contenidos en el registro público mercantil de las Cámaras de Comercio, entre otros.

5. OBLIGACIONES

Esta política es de obligatorio y estricto cumplimiento para todos y cada uno de los miembros de FOSCAL, al igual que para todos los terceros que obran en nombre de la misma o que tratan o se relacionan con datos personales por disposición de la organización, como encargados o subencargados. Todos ellos deberán observar y respetar esta política en el cumplimiento de sus funciones, actividades y ejecuciones contractuales, aún después de terminados los vínculos legales, funcionales, comerciales, laborales o de cualquier índole que con la organización hubieren establecido. De igual manera, se comprometen a guardar estricta confidencialidad en relación con los datos en su momento tratados.

Es importante señalar que FOSCAL realiza tratamiento de datos personales de sus respectivos titulares, contando con un equipo de trabajo capacitado y actualizado en protección de datos personales y que cuenta con acuerdos de confidencialidad suscritos con sus trabajadores, proveedores y demás miembros de la organización, pensando siempre en preservar la privacidad de la información a la cual pudieren llegar a tener acceso en desarrollo de sus obligaciones y responsabilidades.

No obstante, agradecemos que cualquier incumplimiento de las obligaciones y en general, de la política contenida en este documento, que se entiende como un incumplimiento gravísimo de las obligaciones contractuales de los obligados, sea reportada mediante mensaje enviado a través:

- Página web *www.foscal.com.co* icono *contáctenos*
- Correos electrónicos: *atencion.paciente1@foscal.com.co*
- Personalmente mediante contacto con el personal de atención al Paciente y su Familia en las instalaciones de la organización ubicada en la Calle 155A 23 09, Floridablanca, Santander

sin perjuicio de las acciones contractuales o legales que de ello se generen.

6. ESTRUCTURA ADMINISTRATIVA SOBRE PROTECCIÓN Y TRATAMIENTO DE DATOS

FOSCAL ha establecido para efectos del Sistema de Gestión de Seguridad de Datos Personales- SGSDP la siguiente estructura orgánica o de gobierno:

- **Director General:** funcionario estratégico del Sistema, encargado de definir y aprobar la Política de Tratamiento de la Información – PTI de la organización y de la toma de decisiones fundamentales para la implementación del SGSDP.

  De igual forma será el encargado de aprobar las modificaciones y actualizaciones de la Política de Tratamiento de la Información – PTI y de hacer seguimiento del funcionamiento del Sistema de Gestión de Seguridad de Datos Personales, para lo cual se apoyará en el Comité del Sistema de Gestión de Seguridad de Datos Personales – SGSDP, al cual dará su estructura y cuya creación aprobará.

  El Director General sostendrá comunicación directa con el Comité del SGSDP.

- **Presidente del comité:** responsable del apoyo técnico del Comité del SGSDP, encargado de velar por el cumplimiento de las funciones de aquel y supervisar la implementación de la PTI, además de servir de canal de comunicación entre los demás órganos y miembros del SGSDP.

- **Comité Sistema de Gestión de Seguridad de Datos Personales - SGSDP**: órgano encargado de la aprobación de normas y procedimientos diferentes de la PTI y la implementación y mantenimiento del SGSDP.

- **Responsable de Base Documental:** aquel funcionario a quien el presidente del Comité asigne la responsabilidad de velar por la implementación, cumplimiento y actualización de normas y procedimientos relacionados con el ámbito Bases Documentales, que forman parte del SGSDP, aplicados por la Organización en materia de Protección de Datos Personales.

- **Responsable de Procesos:** aquel funcionario a quien el presidente del Comité asigne la responsabilidad de velar por la implementación, cumplimiento y actualización de normas y procedimientos relacionados con el ámbito Procesos, que forman parte del SGSDP, aplicados por la Organización en materia de Protección de Datos Personales.

- **Responsable de TIC:** aquel funcionario a quien el presidente del Comité asigne la responsabilidad de velar por la implementación, cumplimiento y actualización de normas y procedimientos relacionados con el ámbito TIC que forman parte del SGSDP, que aplica la Organización en materia de Protección de Datos Personales.

- **Responsable de Locaciones Físicas:** aquel funcionario a quien el presidente del Comité asigne la responsabilidad de velar por la implementación, cumplimiento y actualización de normas y procedimientos relacionados con el ámbito Locaciones Físicas, que forman parte del SGSDP, aplicadas por la Organización en materia de Protección de Datos Personales.

- **Responsable de PQR:** aquel funcionario a quien el presidente del Comité asigne la responsabilidad de la atención de las peticiones, quejas o reclamos que surjan con ocasión al Tratamiento de Datos Personales realizado por la Organización.

- **Responsable de Cultura organizacional**: Aquel funcionario a quien el presidente del Comité asigne la responsabilidad de la coordinar los espacios de socialización y sensibilización a los trabajadores sobre sistema de gestión de seguridad de datos personales, aplicadas por la Organización en materia de Protección de Datos Personales.

7. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES

En el desarrollo, interpretación y aplicación de la presente política, se aplicarán, de manera armónica e integral, los siguientes principios:

7.1. PRINCIPIOS RELACIONADOS CON LA RECOLECCIÓN DE DATOS PERSONALES

- La recolección y tratamiento de datos personales debe realizarse para fines lícitos respetando las normas generales, especiales y la autorización dada por el titular sobre los mismos.

- Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. Dichos datos serán tratados de forma leal y lícita.

- Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

- Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste.

- Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos por los correspondientes datos rectificados o completados, siempre y cuando el titular de la información así lo solicite. Desde el momento en el que el titular pone en conocimiento esta situación a la Organización se dará aplicación al correspondiente procedimiento.

- Sólo deben recolectarse los datos personales que sean estrictamente necesarios para el cumplimiento de las finalidades del tratamiento, de tal forma que se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objetivo del tratamiento. En consecuencia, debe hacerse todo lo razonablemente posible para limitar el procesamiento de datos personales al mínimo necesario. Es decir, los datos deberán ser: adecuados, pertinentes y acordes con las finalidades para las cuales fueron previstas.

- **Autorización para tratamiento de datos sensibles:** para efectos de la recolección de datos sensibles se deben cumplir los siguientes requisitos:

  - La autorización debe ser explícita y previa a la recolección del dato o a más tardar, concomitante con ella.
  - Se debe informar al titular expresamente que no está obligado a autorizar el tratamiento de dicha información, salvo deber legal o contractual, de lo cual se dejará registro.
  - Para su transmisión y/o transferencia, lo mismo que para su almacenamiento, se utilizarán mecanismos de seguridad especial tales como cifrado de bases de datos, registro de control de accesos a estas, copias de seguridad alojadas en lugar físico diferente a donde están alojadas las bases de datos, conexiones seguras, etc. según el caso.

- **Autorización de tratamiento de datos de niños, niñas y adolescentes (NNA):** para efectos de la recolección y tratamiento de datos de niños, niñas y adolescentes se deben cumplir los siguientes requisitos:

  - La autorización debe ser otorgada por personas que estén facultadas para representarlos. El representante de los NNA deberá garantizarles el derecho a ser escuchados y valorar su opinión del tratamiento teniendo en cuenta la madurez, autonomía y capacidad de los NNA para entender el asunto.
  - Se debe informar que es facultativo responder preguntas sobre datos de los NNA.
  - El tratamiento debe respetar el interés superior de los NNA y asegurar el respeto de sus derechos fundamentales.
  - Se debe informar de forma explícita y previa al titular cuáles de los datos que serán objeto de tratamiento son sensibles y la finalidad del mismo.

De igual manera, en general para la recolección de datos, la organización tendrá presentes los siguientes principios:

- **PRINCIPIO DE DIGNIDAD:** toda acción u omisión asociada al tratamiento de datos personales debe ejecutarse siempre salvaguardando la dignidad del titular y amparándolos demás derechos constitucionales, en especial el derecho al buen nombre, a la honra, a la intimidad y el derecho a la información.

- **PRINCIPIO DE LEGALIDAD:** el tratamiento de datos *"es una actividad reglada, debiéndose por tanto estar sometida a todas las disposiciones que le regulan"* y a los principios que lo enmarcan. (Ley 1581 de 2012).

- **PRINCIPIO DE LIBERTAD:** el tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

- **PRINCIPIO DE INTEGRIDAD:** en el tratamiento debe garantizarse el derecho del titular a obtener del responsable o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

7.2. PRINCIPIOS RELACIONADOS CON EL USO DE DATOS PERSONALES

- **PRINCIPIO DE FINALIDAD**: los datos personales deben ser procesados con un propósito específico y explícito, el cual debe ser autorizado por el titular o permitido por la ley. Se deberá informar al titular del dato de manera clara, suficiente y previa acerca de la finalidad de la información suministrada y, por tanto, no podrán recopilarse datos sin una finalidad específica.

- **PRINCIPIO DE TEMPORALIDAD:** los datos personales se conservarán únicamente por el tiempo razonable y necesario para cumplir la finalidad del tratamiento y las exigencias legales o instrucciones de las autoridades de vigilancia y control u otras autoridades competentes. Los datos serán conservados cuando ello sea necesario para el cumplimiento de una obligación legal o contractual. Para determinar el término del tratamiento se considerarán las normas aplicables a cada finalidad y los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.

- **PRINCIPIO DE NO DISCRIMINACIÓN:** queda prohibido realizar cualquier acto de discriminación por las informaciones recaudadas en las bases de datos o archivos.

7.3. PRINCIPIO RELACIONADO CON LA CALIDAD DE LA INFORMACIÓN

- **PRINCIPIO DE VERACIDAD O CALIDAD**: La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error. Se deberán adoptar medidas razonables para asegurar que los datos sean precisos y suficientes y, cuando así lo solicite el titular o cuando la Organización así lo determine, sean actualizados, rectificados o suprimidos cuando sea procedente.

7.4. PRINCIPIOS RELACIONADOS CON LA PROTECCIÓN, EL ACCESO Y CIRCULACIÓN DE DATOS PERSONALES

- **PRINCIPIO DE SEGURIDAD:** cada miembro de la Organización deberá cumplir las medidas técnicas, humanas y administrativas que establezca la misma para otorgar seguridad a los datos personales evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- **PRINCIPIO DE TRANSPARENCIA:** en el tratamiento de datos personales debe garantizarse el derecho del Titular a obtener en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

- **PRINCIPIO DE ACCESO RESTRINGIDO:** sólo se permitirá acceso a los datos personales a las siguientes personas:

  - ❖ Al titular del dato.
  - ❖ A las personas autorizadas por el titular del dato.
  - ❖ A las personas que por mandato legal u orden judicial sean autorizadas para conocer la información del titular del dato.
  - ❖ Los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares de los datos personales o terceros autorizados conforme a la presente política o a la ley.

- **PRINCIPIO CIRCULACIÓN RESTRINGIDA:** sólo se puede enviar o suministrar los datos personales a las siguientes personas:

  - ❖ Al titular del dato, sus causahabientes o sus representantes legales.
  - ❖ A las personas autorizadas por el titular del dato o por la ley.
  - ❖ A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial. En este último caso, de conformidad con la Corte Constitucional, se procederá de la siguiente manera:

    - ✓ En primer lugar, la entidad pública o administrativa debe justificar su solicitud indicando el vínculo entre la necesidad de obtener el dato y el cumplimiento de sus funciones constitucionales o legales.

- ✓ En segundo lugar, con la entrega de la información se le informará a la entidad pública o administrativa que debe cumplir los deberes y obligaciones que le impone la ley 1581 de 2012 como responsable del tratamiento. La entidad administrativa receptora debe cumplir con las obligaciones de protección y garantía que se derivan de la citada ley, en especial la observancia de los principios de finalidad, uso legítimo, circulación restringida, confidencialidad y seguridad.

- **PRINCIPIO DE CONFIDENCIALIDAD:** todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley o por el titular del dato.

8. DERECHOS APLICABLES A LOS TITULARES DE DATOS PERSONALES

FOSCAL está comprometida en respetar y garantizar los siguientes derechos de los titulares de los datos:

- Permitir, una vez cada mes calendario, el acceso en forma gratuita a los datos personales por parte del titular, si así lo requiere, o cuando existan modificaciones sustanciales de la PTI que lo ameriten.
- Conocer, actualizar y rectificar los datos personales. Para el efecto es necesario establecer previamente la identificación de la persona para evitar que terceros no autorizado accedan a los datos del titular del dato.
- Informar sobre el uso que FOSCAL ha dado a los datos personales del titular.
- Dar trámite a las consultas y reclamos siguiendo las pautas establecidas en la ley y en la presente política.
- Acceder a la solicitud de revocatoria de la autorización y/o supresión del dato personal cuando la Superintendencia de Industria y Comercio haya determinado que en el tratamiento realizado por los directivos, trabajadores y miembros de FOSCAL se ha incurrido en conductas contrarias a la Ley 1581 de 2012 o a la Constitución.
- El titular también podrá revocar la autorización y solicitar la supresión del dato, cuando no exista un deber legal o contractual que le imponga el deber de permanecer en la base de datos o archivo del responsable o encargado.

Los derechos de los titulares, podrán ejercerse por las siguientes personas:

- Por el titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que ponga a disposición FOSCAL
- Por sus causahabientes, quienes deberán acreditar tal calidad.
- Por el representante y/o apoderado del titular, previa acreditación de la representación o apoderamiento.
- Por estipulación a favor de otro o para otro.
- Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

9. PROCEDIMIENTO PARA EJERCER SUS DERECHOS COMO TITULAR DE LOS DATOS

CANALES DE COMUNICACIÓN

A efectos de que los titulares de datos personales, sus representantes legales, apoderados o herederos, todos estos debidamente acreditados, ejerzan los derechos a los que se refiere la Ley 1581 de 2012 y demás normas concordantes, y en general para la atención de PQR asociadas a los datos personales, hemos establecido UNICAMENTE los siguientes canales de comunicación:

- Página web www.foscal.com.co icono *contáctenos*,
- Correos electrónicos: *atencion.paciente1@foscal.com.co,*
- Personalmente mediante contacto con el personal de atención al Paciente y su Familia en las instalaciones de la organización ubicadas en la Calle 155A No. 23-09, Floridablanca, Santander.

FUENTES DE PQR E INFORMES ADMINISTRATIVOS Y JUDICIALES

Según la circunstancia en que se genere la PQR tenga en cuenta lo siguiente:

- **Cuando el Titular Realiza Consulta o Reclamos Verbales:** Cuando la PQR se quiera formular a través del canal físico, en sede, de manera verbal, se deberá tener en cuenta los siguientes aspectos:

  a. Al Titular se le proveerá el formulario correspondiente al formato "*Consulta – Reclamo Verbal",* que para el efecto tiene establecido la organización para cada caso.

  b. Adicionalmente deberá anexar:

  - ❖ Copia del documento idóneo que permita su identificación o de la calidad en que actúa (titular, causahabiente o apoderado).
  - ❖ Poder si se actúa a través de representante.

- ❖ Si se tratase de una persona jurídica, debe el representante legal, presentar el documento idóneo que acredite la existencia y representación legal de la misma, junto con la exhibición de un documento idóneo que permita su identificación.
- ❖ Los anexos o soportes que considere necesarios para su consulta o reclamo.

- **Cuando el Titular Realiza la Petición o Consulta por Medio de Correo Electrónico:** Cuando la PQR se quiera formular a través del canal virtual del correo electrónico, se deberá tener en cuenta los siguientes aspectos:

a. Para verificar la condición de titular, éste al momento de enviar el correo electrónico, deberá adjuntar:

- ❖ Copia ampliada al 150% de su documento de identificación.
- ❖ En tratándose de un causahabiente o apoderado del titular, documento que acredite la calidad de causahabiente o poder debidamente otorgado
- ❖ Si se tratase de una persona jurídica, debe el representante legal, presentar el documento idóneo que acredite la existencia y representación legal de la misma, junto con la exhibición de un documento idóneo que permita su identificación.
- ❖ Los anexos o soportes que considere necesarios para su consulta o reclamo.

- **Cuando la Consulta Proviene de Organismos de Control:** Cuando el asunto tenga como origen en una entidad administrativa o de control se deberá tener en cuenta los siguientes aspectos:

a. Deberán indicar la correspondiente solicitud de manera expresa e inequívoca.

b. La finalidad concreta para la cual requieran la información solicitada (salvo que sea autoridad judicial).

c. Indicar las funciones específicas que le han sido conferidas por la ley relacionadas con dicha finalidad mencionando la correspondiente norma (esta exigencia no aplica cuando se trate de autoridad judicial).

10. ACCIONES PREVIAS A QUEJAS ANTE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

En el evento en que se desee elevar una queja ante la Superintendencia de Industria y Comercio referido a datos personales, recuerde que previamente debe haber agotado el trámite de consulta o reclamo ante FOSCAL, de acuerdo a las indicaciones anteriormente referidas, advirtiendo nuestra total disposición a atender sus inquietudes.

11. DEBERES DE FOSCAL COMO RESPONSABLE DEL TRATAMIENTO

A los titulares de datos y terceros interesados, les informamos que FOSCAL, en desarrollo del tratamiento de los datos personales cumple y exige que se cumplan los deberes que impone la ley así:

11.1. DEBERES RESPECTO DEL TITULAR DEL DATO

- Solicitar y conservar, en las condiciones previstas en esta política, copia de la respectiva autorización otorgada por el titular.
- Informar de manera clara y suficiente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data, es decir, conocer, actualizar o rectificar sus datos personales.
- Informar a solicitud del titular sobre el uso dado a sus datos personales.
- Tramitar las consultas y reclamos formulados en los términos señalados en la presente política.

11.2. DEBERES RESPECTO DE LA CALIDAD, SEGURIDAD Y CONFIDENCIALIDAD DE LOS DATOS PERSONALES

- Observar los principios de veracidad, calidad, seguridad y confidencialidad en los términos establecidos en la siguiente política.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- Implementar las normas y procedimientos de seguridad necesarios para asegurar la confidencialidad, integridad y disponibilidad de la información y bases de datos de la Organización, también asegurar la estabilidad, disponibilidad de la infraestructura tecnológica y la operación.
- Actualizar la información cuando sea necesario.
- Rectificar los datos personales cuando ello sea procedente.

11.3. DEBERES CUANDO REALIZA EL TRATAMIENTO A TRAVÉS DE UN ENCARGADO O SUBENCARGADO

- Poner en conocimiento del encargado o subencargado la presente Política de Tratamiento de la Información, para advertir de la obligación que les asiste de operar el tratamiento de datos que se le encomiende en el marco de la misma.
- Suministrar al encargado o subencargado del tratamiento, únicamente datos cuyo tratamiento esté previamente autorizado conforme a la ley.
- Garantizar que la información que se suministre al encargado o subencargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- Comunicar de forma oportuna al encargado o subencargado del tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.
- Informar de manera oportuna al encargado o subencargado del tratamiento, las rectificaciones realizadas sobre los datos personales para que éste proceda a realizar los ajustes pertinentes.
- Exigir al encargado o subencargado del tratamiento, en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular.
- Informar al encargado o subencargado del tratamiento, cuando determinada información se encuentre en condición de "*reclamo en trámite*" por parte del titular o en se trate de "*información en discusión judicial*", una vez se haya presentado la reclamación o recibido la información. Así mismo deberá reportar los eventos en que el reclamo se atienda o la discusión judicial sea superada.

11.4. DEBERES RESPECTO DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

FOSCAL deberá cumplir con los siguientes deberes:

- Informarle las eventuales violaciones a los códigos de seguridad y la existencia de novedades en la administración de la información de los Titulares.
- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

11.5. DEBERES CUANDO OBRA COMO ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES

Cuando FOSCAL realiza el tratamiento de datos en nombre de otra entidad u Organización responsable del tratamiento, adquiere la calidad de encargado y por tanto se obliga a cumplir los siguientes deberes:

- Establecer que el responsable del tratamiento esté autorizado para suministrar a FOSCAL los datos personales que tratará como encargado.
- Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Realizar oportunamente la actualización, rectificación o supresión de los datos.
- Actualizar la información reportada por los responsables del tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.
- Tramitar las consultas y los reclamos formulados por los titulares en los términos señalados en la presente política.
- Registrar en la base de datos la leyenda "*reclamo en trámite*" en la forma en que se establece en la presente política.

- Insertar en la base de datos la leyenda "*información en discusión judicial*" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
- Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
- Permitir el acceso a la información únicamente a las personas autorizadas por el titular o facultadas por la ley para dicho efecto.
- Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan novedades en la administración de la información de los titulares.
- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

12. VIDEOVIGILANCIA

FOSCAL utiliza medios de video vigilancia instalados en diferentes sitios internos y externos de sus sedes. Por ello se informa a los titulares y terceros, la existencia de estos mecanismos mediante la difusión en sitios visibles de anuncios con alertas de videovigilancia. No obstante, ningún dispositivo de videovigilancia se sitúa en lugares que puedan afectar la intimidad de los titulares.

La información recolectada por estos mecanismos se utilizará para fines de seguridad de los bienes, instalaciones y personas que se encuentren en éstas, o como prueba en cualquier tipo de procedimiento interno, judicial o administrativo, siempre con sujeción y cumplimiento de las normas legales.

Las imágenes solo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explicitas y que hayan justificado la instalación de las cámaras o videocámaras.

13. AVISO DE PRIVACIDAD

Para todos los efectos legales, FOSCAL manifiesta cumplir con el ***Aviso de Privacidad*** de que trata el artículo 2.2.2.25.3.2 del Decreto 1074 de 2015. Los titulares de datos personales que deseen consultarlo, podrán hacerlo enviando su solicitud a los siguientes correos electrónicos atencion.paciente1@foscal.com.co.

14. VIGENCIA DE BASES DE DATOS

FOSCAL, cuando actúe como responsable, conservará en su base de datos, los datos personales que hayan sido recolectados, mientras siga desarrollando las actividades que constituyen su objeto social.

Cuando FOSCAL actúe en la calidad de encargado, la vigencia de los datos personales bajo su tratamiento estará determinada por las indicaciones que al efecto le señale el correspondiente responsable.

Lo expresado en los párrafos anteriores, se tendrá siempre en cuenta sin perjuicio del ejercicio de los derechos de supresión que le asisten al titular o de orden legal, administrativa o judicial que ordene la supresión de los mismos.

En tratándose de las historias clínicas, la retención estará conforme a las disposiciones legales y reglamentarias que sobre el tema se aprueben y conforme a los procedimientos que al efecto se aprueban por parte de la organización.

15. MODIFICACIÓN Y/O ACTUALIZACIÓN DE LA POLÍTICA DE TRATAMIENTO DE LA INFORMACIÓN

En el evento de cualquier cambio sustancial en la Política de Tratamiento de la Información, se procurará la comunicación de forma oportuna a los titulares de los datos a través de los medios de comunicación establecidos por la institución.

Las comunicaciones se enviarán como mínimo diez (10) días antes de implementar la nueva política y/o actualización sustancial de la misma. Cuando el cambio se refiera a la finalidad del tratamiento, se deberá solicitar del titular una nueva autorización.

Esta Política de Tratamiento de la Información – PTI fue aprobada por el Director General de FOSCAL, el día 4 de octubre del año 2017. Reemplaza cualquier otro documento que con anterioridad se hubiere elaborado. Se ha dado a conocer mediante aviso de privacidad elaborado conforme a la ley. La presente PTI inicia su vigencia pasados diez (10) días del correspondiente Aviso de Privacidad. Para conocimiento de los titulares y terceros interesados puede ser consultada en la página www.foscal.com.co.

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Tatiana Angarita Rodríguez Yolanda Ballesteros Rueda.	Consultoría FERSACO. Integrantes Comité Sistema Gestión Seguridad de Datos Personales – SGSDP. Coordinadora SMG - Ing. Yolanda Ballesteros Rueda.	Director General – Dr. Jorge Ricardo León Franco.
FECHA DE ELABORACIÓN:	**FECHA DE REVISIÓN:**	**FECHA DE APROBACIÓN:**
30 abril de 2015	6 al 27 septiembre de 2017	4 octubre de 2017