PHYX S.A.S.
NIT. 900939751-9
Bogotá D.C. **protecciondedatos@phyx.co**

PHYX

CONTENIDO

PHYX

INTRODUCCIÓN

PHYX S.A.S. identifica la información como un activo indispensable para el cumplimiento de la estrategia corporativa. Por ello, establece un marco de gobierno que garantice su protección adecuada a lo largo de todo el ciclo de vida, independientemente del medio en que sea generada, procesada, transportada, almacenada o eliminada, asegurando su confidencialidad, integridad, disponibilidad y trazabilidad.

Esta Política describe los requerimientos y normas de seguridad de la información adoptados por PHYX S.A.S., con fundamento en la legislación y regulaciones aplicables, incluyendo, entre otras, la Ley 1581 de 2012, sus decretos reglamentarios y lineamientos de la Superintendencia de Industria y Comercio, así como las disposiciones sectoriales pertinentes (Capítulo 12, Título I de la Circular Básica Jurídica de la SFC, cuando aplique). Igualmente se alinea con los estándares internacionales ISO/IEC 27001:2022 y ISO/IEC 27002:2022, y se integra con el Sistema de Gestión de la Calidad ISO 9001:2015 y el enfoque de sostenibilidad NTS-TS 006-1.

Los requerimientos aquí establecidos constituyen un pilar del Sistema de Gestión de Seguridad de la Información (SGSI) de la compañía y sirven como base para la implantación de controles, procedimientos y estándares que soportan operaciones nacionales e internacionales, proyectos de largo aliento y, cuando corresponda, el tratamiento de datos sensibles de clientes y demás grupos de interés, incluyendo obligaciones de cadena de suministro y acuerdos con terceros.

La seguridad de la información es una prioridad y una responsabilidad de todos. En consecuencia, colaboradores y terceros deben cumplir estos lineamientos, usar la información conforme a su finalidad, aplicar el principio de mínimo privilegio, reportar oportunamente los incidentes y participar en las actividades de formación y mejora continua. Cualquier actuación contraria al espíritu y alcance de esta Política dará lugar a las medidas correctivas y sanciones previstas por la ley y por los acuerdos contractuales vigentes.

PHYX

I. DEFINICIONES

ARCO (Derechos de Acceso, Rectificación, Cancelación y Oposición): Conjunto de derechos de los titulares para acceder a sus datos, rectificarlos, cancelarlos/suprimirlos cuando proceda y oponerse a ciertos tratamientos, sin perjuicio de excepciones legales.

Autorización/Consentimiento: Manifestación previa, expresa e informada del Titular que habilita el tratamiento de sus datos personales por parte de PHYX S.A.S.

Aviso de privacidad: Comunicación verbal o escrita generada por PHYX S.A.S. dirigida al Titular para el tratamiento de sus datos personales, que informa sobre las finalidades, derechos y canales de atención.

Anonimización: Proceso técnico y/o organizacional que transforma datos personales de modo irreversible para que no sea posible identificar a una persona, ni directa ni indirectamente, ni aun combinando con información adicional razonablemente disponible.

Base de datos no automatizada: Conjunto organizado de datos personales creados, tratados y/o almacenados de forma manual (física), sin apoyo de software para su gestión.

Base de datos automatizada: Conjunto organizado de datos personales creados, tratados y/o almacenados mediante sistemas informáticos o software. Su administración recae en el área responsable definida por PHYX S.A.S. (p. ej., Desarrollo Digital y TIC) según el inventario de tratamientos.

Base de datos personales: Conjunto organizado de datos de carácter personal, cualquiera sea la forma o modalidad de creación, recolección, almacenamiento, organización, acceso o eliminación.

Biometría: Tratamiento de datos que resultan de un tratamiento técnico específico relativos a características físicas, fisiológicas o conductuales que permiten o confirman la identificación única (p. ej., huella, rostro, iris, voz). Tienen carácter de dato sensible.

Brecha de datos personales (violación de medidas de seguridad): Incidente de seguridad que ocasiona acceso, pérdida, destrucción, alteración, uso o divulgación no autorizados de datos personales. Debe gestionarse y, cuando corresponda,

notificarse a la SIC y a los Titulares.

Cadena de suministro (seguridad de proveedores): Requisitos y controles aplicados a terceros que tratan información por cuenta propia o de PHYX (due diligence, confidencialidad, DPA, mínimo privilegio, notificación de incidentes, auditoría, subencargados autorizados).

Cesión/Comunicación de datos: Revelación o entrega de datos personales a un tercero distinto del Titular y de los sujetos habilitados, en los términos autorizados por la ley y por el Titular.

CCTV/Videovigilancia: Tratamiento de imágenes y sonidos captados por cámaras con fines de seguridad y control de accesos, con señalización visible, conservación limitada y atención a derechos de los Titulares.

Cookies y tecnologías similares: Mecanismos técnicos de almacenamiento y acceso a información en dispositivos del usuario (cookies, píxeles, SDK), utilizados para fines necesarios, funcionales, analíticos o publicitarios, conforme a la política de cookies y al consentimiento aplicable.

Custodio de la base de datos: Persona que tiene bajo su custodia operativa una base de datos personales al interior de PHYX S.A.S., conforme a los perfiles de acceso y al inventario de tratamientos.

Dato anonimizado: Dato sometido a un proceso irreversible que impide la identificación del Titular. Los datos anónimos dejan de ser datos personales.

Dato personal: Cualquier información vinculada o que pueda asociarse a una persona natural identificada o identificable (p. ej., identificativos, contacto, laborales, financieros para pagos, imágenes, biométricos, registros técnicos, entre otros).

Dato privado: Información de conocimiento restringido, relevante para el ámbito íntimo del Titular (p. ej., hábitos personales, información patrimonial no pública), cuya divulgación está limitada.

Dato público: Información calificada como pública por la ley o la Constitución (p. ej., estado civil, profesión u oficio, calidad de comerciante o servidor público), accesible sin reserva, sin perjuicio de su principio de finalidad.

Dato semiprivado: Información que no es íntima, reservada ni pública, cuyo

conocimiento puede interesar a un grupo o sector (p. ej., información financiera y crediticia en ciertas condiciones).

Dato sensible: Dato que afecta la intimidad del Titular o cuyo uso indebido puede generar discriminación (p. ej., datos de salud, biométricos, orientación sexual, creencias religiosas, origen étnico, filiación política, entre otros). Su tratamiento exige autorización expresa y condiciones reforzadas.

Dato seudonimizado: Dato sometido a tratamiento mediante el cual no puede atribuirse a un Titular sin información adicional separada y protegida (seudonimización).

Delegado de Protección de Datos (DPO): Persona designada por PHYX S.A.S. para coordinar el cumplimiento del régimen de protección de datos y del SGSI, y servir de punto de contacto con Titulares y autoridades.

Derechos de imagen y propiedad intelectual: Autorizaciones, licencias y reglas aplicables al uso de imagen/voz de personas y a obras protegidas (p. ej., gráficos, fotografías, música, software, marcas) en proyectos de PHYX S.A.S., conforme a contrato y a la ley.

Encargado del tratamiento: Persona natural o jurídica, pública o privada, que realiza el tratamiento por cuenta del Responsable, conforme a sus instrucciones.

Evaluación de Impacto en Privacidad (PIA/DPIA): Análisis sistemático de riesgos sobre derechos y libertades de los Titulares para tratamientos que impliquen alto riesgo (p. ej., datos sensibles, perfilamientos, transferencias), con definición de medidas de mitigación.

Finalidad: Propósito legítimo, específico y comunicado al Titular que justifica el tratamiento de sus datos.

Fuentes accesibles al público: Bases de datos cuya consulta puede ser realizada por cualquier persona (p. ej., guías telefónicas, directorios sectoriales, gacetas oficiales, medios de comunicación), siempre que contengan datos de carácter general y conforme a la ley.

Gestión de registros y trazabilidad (logs): Conjunto de evidencias técnicas y administrativas que permiten reconstruir operaciones de tratamiento (accesos, cambios, transmisiones, transferencias), preservando integridad y disponibilidad.
Habeas Data: Derecho del Titular a conocer, actualizar, rectificar, suprimir

información, y a revocar la autorización, así como a ser informado del uso de sus datos personales.

Incidente de seguridad de la información: Evento que compromete o puede comprometer la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información.

Menores de edad: Titulares con interés superior prevalente; su tratamiento exige autorización del representante legal y finalidades específicas, pedagógicas o de seguridad, con mínimos necesarios.

Opt-out (revocatoria/supresión): Mecanismos por los cuales el Titular solicita dejar de recibir comunicaciones o que sus datos sean eliminados cuando proceda.

Perfilamientos/decisiones automatizadas: Tratamientos que evalúan aspectos personales a partir de datos personales (hábitos, intereses, comportamientos) y que pueden producir efectos jurídicos o significativos sobre el Titular. Requieren información clara y salvaguardas.

Principio de mínimo privilegio: Política de acceso que limita permisos a lo estrictamente necesario para cumplir la función asignada.

Propietario/Administrador de la base de datos: Área de PHYX S.A.S. que, dentro del proceso de negocio, tiene la responsabilidad de gestión y cumplimiento del tratamiento asociado a la base de datos.

RNBD (Registro Nacional de Bases de Datos): Registro ante la Superintendencia de Industria y Comercio (SIC) de las bases de datos sujetas a inscripción por parte de los Responsables del tratamiento, incluyendo su actualización y reportes exigidos.
Responsabilidad demostrada (accountability): Deber de evidenciar, mediante políticas, controles y registros, el cumplimiento del régimen de protección de datos y seguridad de la información.

Responsable del tratamiento: Persona natural o jurídica, pública o privada, que decide sobre la finalidad y el tratamiento de los datos personales.

Subencargado: Tercero contratado por un Encargado para apoyar el tratamiento por cuenta del Responsable, con autorización previa y obligaciones equivalentes en protección de datos.
Telemetría y metadatos: Datos técnicos generados por sistemas, dispositivos o

aplicaciones sobre su operación (p. ej., dirección IP, identificadores de dispositivo, eventos), que pueden constituir datos personales cuando identifiquen o hagan identificable al Titular.
Titular del dato personal: Persona natural cuyos datos personales son objeto de tratamiento.

Transmisión de datos: Tratamiento que implica la comunicación interna o externa para su procesamiento por un Encargado en nombre del Responsable, dentro o fuera de Colombia, bajo instrucciones y contrato de transmisión.

Transferencia internacional de datos: Envío de datos personales por un Responsable o Encargado en Colombia a un receptor que es Responsable del tratamiento y se encuentra dentro o fuera del país, sujeto a reglas de país adecuado o mecanismos contractuales y, cuando aplique, autorización de la SIC o consentimiento expreso.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, automatizadas o no (recolección, almacenamiento, uso, circulación, clasificación, actualización, consulta, transmisión, transferencia, supresión.

Usuario autorizado: Persona natural o jurídica con acceso legítimo a datos personales por razón de sus funciones o por habilitación contractual.

Plazo de conservación: Periodo durante el cual los datos se mantienen de forma identificable por razones legales, contractuales o de finalidad; vencido el plazo se aplicará supresión o anonimización segura.

Seudonimización: Tratamiento mediante el cual se reemplazan identificadores directos (p. ej., nombre, cédula) por claves o seudónimos; reduce riesgos pero no impide que, con información separada y controles, pueda re-identificarse al titular.

DPIA/PIA (Evaluación de Impacto en la Privacidad): Análisis estructurado de riesgos para los titulares derivados de un tratamiento (existente o nuevo), que identifica amenazas, valora probabilidad/impacto y define controles y mitigaciones antes o durante el tratamiento.

SDLC seguro (Secure Software Development Life Cycle): integrar controles de seguridad en todas las fases del ciclo de vida del software (requerimientos, diseño, desarrollo, pruebas, despliegue y mantenimiento). Incluye gestión de riesgos, revisiones, pruebas y capacitación.
Requisitos de seguridad: condiciones técnicas y organizacionales que el sistema

debe cumplir (p. ej., cifrado en tránsito/almacenamiento, autenticación multifactor, registro y auditoría, mínimos privilegios, retención de datos, cumplimiento legal).

SAST (Static Application Security Testing): análisis del código fuente o binarios sin ejecutar la aplicación para detectar vulnerabilidades (inyecciones, malas validaciones, fugas de secretos) durante el desarrollo.

DAST (Dynamic Application Security Testing): pruebas de seguridad con la app en ejecución, simulando ataques desde fuera (XSS, inyecciones, errores de configuración) sin acceso al código.

SCA (Software Composition Analysis): inventario y evaluación de componentes de terceros (librerías, frameworks) para encontrar vulnerabilidades, licencias y versiones obsoletas.

SBOM (Software Bill of Materials): "lista de ingredientes" del software: catálogo estructurado de todos los componentes, sus versiones y dependencias, útil para respuesta a incidentes y gestión de vulnerabilidades.

Gestión de secretos: prácticas y herramientas para proteger credenciales (API keys, tokens, contraseñas, certificados): almacenamiento en vaults, rotación, acceso con mínimo privilegio, nunca en código ni repositorios.

Segregación de ambientes: separación estricta de desarrollo, pruebas, staging y producción (redes, cuentas, datos y accesos) para evitar que cambios o datos de prueba afecten producción; datos reales no se usan en dev/test (o se enmascaran).

CI/CD (Integración/Despliegue Continuos): canal automatizado que integra, prueba y despliega cambios con rapidez y control (pipelines). En seguridad: escaneos automáticos (SAST/DAST/SCA), firmas de artefactos, gates de calidad, revisiones obligatorias y rollbacks seguros.

II. OBJETIVO

Definir los objetivos y lineamientos que rigen el tratamiento de datos personales por parte de **PHYX S.A.S.**, en calidad de Responsable y/o Encargado, durante todo su ciclo de vida (recolección, uso, circulación, almacenamiento, transmisión, transferencia, actualización, supresión y/o anonimización) en entornos físicos y digitales y en todas las geografías donde opera la compañía.

OBJETIVOS ESPECÍFICOS

i. Garantizar derechos de los Titulares mediante un tratamiento lícito, leal, transparente y seguro, asegurando confidencialidad, integridad, disponibilidad y trazabilidad de la información.

ii. Cumplir la normativa aplicable en Colombia (Ley 1581 de 2012, Ley 1266 de 2008 en lo pertinente, Decreto 1074 de 2015, Decreto 1377 de 2013 y lineamientos de la SIC), los requisitos sectoriales que apliquen (p. ej., Capítulo 12, Título I de la Circular Básica Jurídica de la SFC), y las disposiciones vigentes en los países donde se realicen tratamientos (incluyendo Panamá, México y Estados Unidos – Florida, con potencial expansión a otras regiones de LATAM y fuera de LATAM).

iii. Alinear el tratamiento con estándares internacionales: ISO/IEC 27001:2022 y ISO/IEC 27002:2022 (SGSI), ISO 9001:2015 (calidad) y NTS-TS 006-1 (sostenibilidad), bajo el principio de responsabilidad demostrada (accountability).

iv. Regular proyectos de largo aliento y el manejo de datos sensibles (p. ej., biométricos, salud, CCTV), así como perfilamientos/decisiones automatizadas, cookies y tecnologías similares con consentimiento granular cuando corresponda.

v. Establecer controles de cadena de suministro y acuerdos con terceros (DPA y subencargados autorizados), incluyendo requisitos mínimos de seguridad (cifrado cuando aplique, mínimo privilegio, gestión de vulnerabilidades, registro de eventos, pruebas de resiliencia y notificación de incidentes).

vi. Regular transmisiones y transferencias internacionales de datos, de acuerdo con reglas de país adecuado o mecanismos contractuales y, cuando aplique, autorización de la SIC o consentimiento expreso del Titular.

vii. Gestionar el RNBD: registro, actualización y gobierno de las bases de datos

sujetas a inscripción, y definir plazos de conservación con supresión o anonimización segura una vez cumplidas las finalidades o vencidos los términos legales/contractuales.

viii. Incorporar propiedad intelectual y derechos de imagen: licenciamiento de materiales de terceros, permisos de uso de imagen/voz, manuales de marca y mecanismos de notice & takedown.

ix. Estandarizar la atención de derechos (consulta, actualización, rectificación, supresión, oposición y revocatoria) y el modelo de gestión de incidentes/brechas, incluyendo criterios de reporte a autoridades y comunicación a Titulares cuando corresponda.

III. ÁMBITO DE APLICACIÓN

Esta Política aplica a todo tratamiento de datos personales realizado por PHYX S.A.S., sus filiales, aliados y terceros Encargados/Subencargados que actúen por cuenta de la compañía, dentro y fuera de Colombia.

Cobertura

- **Roles:** Aplica cuando PHYX S.A.S. actúe como Responsable y/o Encargado del tratamiento.
- **Ciclo de vida:** Cubre las fases de recolección, registro, uso, circulación, almacenamiento, transmisión, transferencia, actualización, conservación, supresión y/o anonimización.
- **Medios y entornos:** Tratamientos en canales físicos y digitales, sistemas on-premise y cloud/terceros, dispositivos móviles, CCTV/videovigilancia, biometría, sitios web, apps, cookies y tecnologías similares, CRM, plataformas de analítica y automatización de comunicaciones.
- **Bases de datos:** Incluye bases permanentes y temporales, respaldos, archivos, logs y repositorios documentales, independientemente de su soporte (automatizadas o no automatizadas), y su registro/actualización en

el RNBD cuando aplique.

- **Proyectos:** Aplica a proyectos de corto y largo aliento, especialmente cuando involucren datos sensibles o transferencias internacionales.

- **Sujetos obligados:** Es obligatoria para directivos, colaboradores, contratistas, proveedores y cualquier tercero con acceso a datos personales por relación con **PHYX S.A.S.**, quienes deberán suscribir las obligaciones de confidencialidad y, cuando corresponda, DPA y acuerdos de transmisión/transferencia.

IV. DESTINATARIOS DE LA PRESENTE POLÍTICA.

La presente Política es obligatoria y exigible para toda persona natural o jurídica que, por relación laboral, contractual, estatutaria o de hecho, tenga acceso, conozca, trate o administre datos personales por cuenta de **PHYX S.A.S**.

En particular, aplica a:

- **Órganos societarios y de control:** Representante Legal, Junta/Accionistas, Revisor Fiscal y demás órganos estatutarios cuando accedan a datos personales por el ejercicio de sus funciones.

- **Personal interno:** Directivos, mandos medios y colaboradores (planta, temporales, aprendices), cualquiera sea su modalidad de vinculación.

- **Contratistas y proveedores:** Personas naturales o jurídicas que presten servicios a PHYX S.A.S. (p. ej., logística, tecnología, cloud/hosting, desarrollo de software, BPO, auditoría, seguridad física, mercadeo, analítica, RR. PP.).

- **Encargados y Subencargados del tratamiento:** Terceros que tratan datos por cuenta de PHYX S.A.S., incluidos sus subproveedores autorizados.

- **Aliados y co-contratistas:** Socios comerciales y operativos involucrados en proyectos conjuntos que requieran acceso a datos personales.
- **Auditores externos y aseguradoras:** Únicamente en el marco de sus funciones y bajo obligaciones de confidencialidad.

- **Clientes, cuando corresponda:** En escenarios de acceso legítimo a datos personales administrados por PHYX S.A.S. (p. ej., auditorías o integraciones), conforme a contrato y ley.

PHYX

V. REQUERIMIENTOS APLICABLES AL TRATAMIENTO DE DATOS PERSONALES

La protección de datos personales en **PHYX S.A.S.** se rige por los siguientes principios y reglas. Sirven de criterio obligatorio para diseñar procesos, interpretar conflictos y auditar el cumplimiento en todas las áreas y geografías donde opera la compañía.

i. Legalidad
El tratamiento es una actividad reglada. Toda operación sobre datos personales debe sujetarse a la Constitución, la Ley 1581 de 2012 y normas concordantes, así como a la regulación sectorial y extranjera aplicable.

ii. Finalidad
Cada tratamiento debe obedecer a una finalidad legítima, específica y explícita, informada previamente al Titular. No se admitirán finalidades indeterminadas ni usos incompatibles con el propósito comunicado.

iii. Libertad (consentimiento informado)
El tratamiento requiere autorización previa, expresa e informada del Titular, salvo las excepciones legales. El Titular podrá revocar la autorización y/o solicitar la supresión cuando proceda.

iv. Veracidad o calidad del dato
Los datos deben ser veraces, completos, exactos, comprobables, comprensibles y actualizados. Se prohíbe tratar datos parciales, fraccionados o engañosos.

v. Transparencia
Se garantiza el derecho del Titular a obtener información, en cualquier momento, sobre la existencia y uso de sus datos, y a ejercer consultas y reclamos por los canales definidos.

vi. Acceso y circulación restringida
El acceso a los datos personales es limitado a personas autorizadas y para finalidades previamente definidas. No podrán estar disponibles en Internet u otros medios masivos salvo que el acceso sea técnicamente controlable y justificado, con seguridad adecuada y consentimiento cuando corresponda.

vii. Seguridad

Se aplican medidas técnicas, administrativas y físicas proporcionales al riesgo (control de accesos, cifrado cuando aplique, respaldo, gestión de vulnerabilidades, registros de eventos, continuidad, pruebas de resiliencia), conforme a ISO/IEC 27001:2022 y 27002:2022.

viii. Confidencialidad

Quienes intervengan en el tratamiento deben guardar reserva de la información, incluso después de finalizada la relación, conforme a NDAs, DPAs y cláusulas contractuales.

ix. Pertinencia y minimización

Solo se recolectarán y tratarán datos adecuados, pertinentes y no excesivos respecto de la finalidad. Se desaconseja la recopilación de datos innecesarios o desproporcionados.

x. Proporcionalidad

Las medidas y decisiones de tratamiento deben ser idóneas, necesarias y equilibradas frente a los fines perseguidos y a los derechos de los Titulares.

xi. Temporalidad y conservación

Agotada la finalidad, o vencidos los términos legales/contractuales, se cesará el uso y se procederá a la supresión o anonimización segura, atendiendo, entre otras, la Ley 594 de 2000 y los plazos comerciales/contables aplicables.

Tabla N° 1 (Campos operativos y de retención)

ITEM	NOMBRE DE BASE DE DATOS	PROCESO RESPONSABLE	SOP. Físico	SOP. Digital	RETENCIÓN Archivo de gestión (años)	RETENCIÓN Archivo central (años)	RETENCIÓN Total (años)	ACCESO Confid.	DISPOSICIÓN
1	Historias laborales (contratos, certificaciones, evaluaciones, HV vinculados, docs de identidad, licencias, renuncias, títulos)	Talento Humano	X	X	3	17	**20**	X	Conservación
2	Promoción y selección de personal (candidatos no vinculados, pruebas)	Talento Humano		X	**1**	0	**1**	X	**Eliminación**
3	Prevención de riesgos laborales (SST: reportes, matrices, investigaciones, exámenes ocupacionales)	SG-SST	X	X	3	17	**20**	X	Conservación
4	Seguridad social (afiliaciones, novedades, planillas, certificados PILA)	Nómina / Talento Humano		X	5	15	**20**	X	Conservación
5	**Nómina y pagos** (desprendibles, liquidaciones, retenciones, soportes contables)	Nómina / Finanzas		X	3	7	**10**	X	Conservación
6	Gestión de bienestar (AT, EL, batería psicosocial, programas)	Talento Humano / SG-SST	X	X	3	17	**20**	X	Conservación

ITEM	NOMBRE DE BASE DE DATOS	PROCESO RESPONSABLE	SOP. Físico	SOP. Digital	RETENCIÓN Archivo de gestión (años)	RETENCIÓN Archivo central (años)	RETENCIÓN Total (años)	ACCESO Confid.	DISPOSICIÓN
7	Gestión de operaciones Clientes de largo aliento (comercial, contratos, soportes de servicio)	Comercial		X	3	7	**10**	X	Conservación

Tabla N° 2 (Base legal y mapeo a ISO/IEC 27001:2022)

ITEM	REQUERIMIENTO LEGAL (principal)	REQUERIMIENTO LEGAL (complementario)	ISO/IEC 27001:2022 (controles)
2	Decreto 1072 de 2015, art. 2.2.4.6.13 (SG-SST)	C. de Comercio art. 60 (10 años para soportes), Ley 1581/2012	A.5.31, A.5.34, A.8.10, A.8.11
4	Ley 1581/2012 (minimización y finalidad)	Buenas prácticas SIC: retener HV de no vinculados 6–12 meses	A.5.34, A.8.10
6	Decreto 1072 de 2015, art. 2.2.4.6.13 (20 años)	Resoluciones MinTrabajo aplicables; Ley 1581/2012	A.5.34, A.8.10, A.7.4
8	Decreto 1072 de 2015, art. 2.2.4.6.13 (SG-SST)	Normatividad de seguridad social; C. Comercio art. 60	A.5.34, A.8.10, A.8.11
10	Decreto 1072 de 2015, art. 2.2.4.6.13; Res. 2404/2019 (Batería Psicosocial)	Ley 1581/2012	A.5.34, A.6.1, A.8.10
12	Código e Comercio art. 60 (10 años) y normas tributarias	Ley 1581/2012	A.5.31, A.5.34, A.8.10

xii. Responsabilidad demostrada (accountability)
PHYX S.A.S. debe evidenciar el cumplimiento mediante políticas, inventarios, evaluaciones de riesgo (PIA cuando aplique), contratos, registros de tratamiento, controles y reportes a autoridades.

xiii. Lealtad y expectativa razonable
El tratamiento debe respetar la expectativa legítima del Titular sobre el uso de sus datos y evitar prácticas engañosas o invasivas.

xiv. Datos sensibles y menores
El tratamiento de datos sensibles (p. ej., salud, biométricos) exige autorización expresa y medidas reforzadas. El tratamiento de menores prioriza su interés superior y requiere autorización del representante legal, con fines específicos y mínimos necesarios.

xv. Transmisiones y transferencias internacionales
Las transmisiones a Encargados y las transferencias internacionales a Responsables se sujetan a contrato, reglas de país adecuado o mecanismos contractuales, y cuando corresponda, autorización de la SIC o consentimiento expreso.

xvi. Perfilamientos y decisiones automatizadas
Cuando se realicen, se informarán criterios, finalidades y consecuencias al Titular, habilitando mecanismos de oposición cuando proceda y aplicando salvaguardas técnicas y organizativas.

xvii. Cookies y tecnologías similares
Su uso se regirá por la política de cookies, con consentimiento granular para fines no estrictamente necesarios.

xviii. **Cadena de suministro (terceros)**
Proveedores, Encargados y Subencargados estarán sujetos a debida diligencia, acuerdos de confidencialidad/DPA, principio de mínimo privilegio, controles de seguridad, notificación de incidentes sin demora indebida y derechos de auditoría.

xix. **Gobernanza y trazabilidad**
Se mantendrán inventarios de tratamientos, RNBD cuando aplique, y logs que permitan reconstruir operaciones relevantes de tratamiento.

VI. DERECHOS DE LOS TITULARES DE LOS DATOS

Los Titulares de datos personales tratados por **PHYX S.A.S.** gozan, de manera gratuita, de los derechos consagrados en la Constitución Política y en la Ley 1581 de 2012 y demás normas aplicables. El ejercicio de estos derechos es personalísimo y se realiza por el Titular o su representante/facultado conforme a la ley.

a. Derecho de acceso
Conocer y obtener información sobre: (i) los datos personales que reposan en nuestras bases; (ii) el tratamiento aplicado; (iii) las finalidades; (iv) el origen de los datos; (v) las transferencias/transmisiones realizadas; y (vi) la identificación de los Responsables/Encargados.

b. Derecho de actualización
Solicitar la actualización de sus datos cuando hayan cambiado o existan novedades.

c. Derecho de rectificación
Solicitar la corrección de datos inexactos, incompletos o fraccionados para mantener su veracidad y calidad.

d. Derecho de supresión (cancelación)
Solicitar la eliminación de los datos cuando: (i) no se respeten los principios, derechos y garantías constitucionales y legales; (ii) hayan dejado de ser necesarios o pertinentes para la finalidad; o (iii) haya vencido el plazo de conservación. Este derecho no procede cuando exista un deber legal o contractual de conservación.

e. Derecho a la revocatoria del consentimiento
Revocar la autorización otorgada para una o varias finalidades. La revocatoria procede cuando no subsista un deber legal/contractual que impida su eliminación o cuando la ley permita mantenerlos por razones legítimas.

f. Derecho de oposición
Oponerse a tratamientos para finalidades específicas, salvo que exista mandato legal o intereses superiores prevalentes. PHYX S.A.S. realizará un juicio de proporcionalidad cuando haya tensión entre derechos (p. ej., información/expresión vs. intimidad/datos).

g. Derecho a presentar quejas y reclamos
Presentar consultas y reclamos ante PHYX S.A.S. por los canales definidos y, de no ser resueltos conforme a la ley, acudir a la Superintendencia de Industria y Comercio (SIC) para la protección de sus derechos.

h. Derecho a ser informado sobre el uso de sus datos
Ser informado, previa solicitud, del uso que se ha dado a sus datos personales.

i. Derecho a otorgar autorización
Otorgar su autorización previa, expresa e informada para el tratamiento, por cualquier medio que permita consulta posterior. Excepciones a la autorización: (i) requerimiento de entidad pública o judicial; (ii) datos de naturaleza pública; (iii) emergencia médica o sanitaria; (iv) tratamientos con fines históricos, estadísticos o científicos autorizados por la ley; (v) datos del Registro Civil. En estos casos, siguen rigiendo los principios de protección de datos.

Los canales y plazos de atención de consultas y reclamos se detallan en el Procedimiento de Habeas Data (Sección 8).

VII. DEBERES DE LOS DESTINATARIOS DE ESTA POLÍTICA RESPECTO DE LAS BASES DE DATOS DE CARÁCTER PERSONAL CUANDO OSTENTEN LA CALIDAD DE RESPONSABLES Y ENCARGADOS

Deberes del Responsable del tratamiento

- **a.** Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del hábeas data y de los derechos previstos en la ley y en esta Política.
- **b.** Solicitar, documentar y conservar la autorización del Titular, o dejar constancia de las excepciones legales, manteniendo evidencia verificable.
- **c.** Informar al Titular, de forma clara y previa, las finalidades, canales de atención, derechos y mecanismos de revocatoria/opt-out.
- **d.** Conservar la información bajo medidas de seguridad administrativas, técnicas y físicas para impedir su adulteración, pérdida, uso, acceso o divulgación no autorizada.

e. Suministrar al Encargado únicamente datos veraces, completos, exactos, actualizados, comprobables y comprensibles, y actualizarlos oportunamente.
f. Rectificar la información cuando sea incorrecta y comunicar lo pertinente a Encargados/Subencargados.
g. Exigir a Encargados/Subencargados el respeto de las condiciones de seguridad y privacidad, mediante DPA y cláusulas de transmisión/transferencia, con derecho de auditoría.
h. Tramitar consultas y reclamos dentro de los términos legales; registrar las marcas “reclamo en trámite” e “información en discusión judicial” cuando corresponda.
i. Adoptar y mantener un Manual interno de políticas y procedimientos (gestión de derechos, incidentes, conservación/eliminación, cookies, CCTV, biometría).
j. Informar al Encargado cuando determinada información esté en discusión por parte del Titular y restringir su circulación.
k. Informar al Titular el uso dado a sus datos cuando lo solicite.
l. Notificar incidentes o brechas de seguridad a la autoridad competente y a los Titulares conforme a la regulación vigente y a los procedimientos internos.
m. Registrar, actualizar y reportar las bases de datos en el RNBD cuando aplique, y llevar el inventario de tratamientos.
n. Evaluar y gestionar riesgos del tratamiento (incluida PIA/DPIA cuando proceda) y aplicar privacidad desde el diseño y por defecto.
o. Cumplir las instrucciones y requerimientos de la SIC y de otras autoridades competentes, en Colombia y en los países donde se traten datos.
p. Gestionar transferencias internacionales con base en reglas de país adecuado o mecanismos contractuales, y obtener autorizaciones cuando sea necesario.
q. Asegurar formación periódica y concienciación al personal y terceros involucrados.

Deberes del Encargado del tratamiento

a. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del hábeas data.
b. Conservar la información bajo condiciones de seguridad idóneas para impedir adulteración, pérdida, consulta, uso o acceso no autorizado.
c. Realizar actualización, rectificación o supresión de los datos a solicitud del Responsable, dentro de los plazos legales/contractuales.
d. Actualizar la información reportada por el Responsable dentro de los cinco (5) días hábiles siguientes a su recibo, cuando aplique.
e. Tramitar consultas y reclamos que reciba y remitirlos al Responsable cuando así se haya pactado, dejando trazabilidad.

f. Registrar en sus sistemas la leyenda “reclamo en trámite” y “información en discusión judicial” en los términos de la ley.
g. Abstenerse de circular información controvertida por el Titular cuyo bloqueo haya sido ordenado por la SIC.
h. Permitir el acceso restringido únicamente a personas autorizadas, bajo principio de mínimo privilegio y segregación de funciones.
i. Notificar sin demora indebida los incidentes o brechas al Responsable y colaborar en la atención y mitigación.
j. No subcontratar (Subencargados) el tratamiento sin autorización previa del Responsable y sin imponerles obligaciones equivalentes.
k. Eliminar, devolver o anonimizar los datos al finalizar la relación, según instrucción del Responsable y plazos de conservación aplicables.
l. Cumplir las instrucciones del Responsable y las de la SIC y demás autoridades competentes.

Deberes del Oficial de seguridad de la información, continuidad del negocio y protección de datos personales

a. Estructurar, mantener y mejorar el Programa de Privacidad y Protección de Datos y su SGSI asociado.
b. Mantener el inventario de bases de datos y registro RNBD, incluyendo actualizaciones y reportes.
c. Revisar y aprobar contratos de transmisión/transferencia (incluidos internacionales) y sus anexos de seguridad.
d. Integrar la política y controles en los procesos organizacionales; liderar capacitaciones y campañas de cultura de datos.
e. Atender visitas y requerimientos de la SIC y coordinar respuestas.
f. Controlar y actualizar continuamente el inventario de recolecciones, usos y divulgaciones; promover minimización y finalidad.
g. Dirigir evaluaciones de impacto (PIA/DPIA) y mantener el archivo histórico de evaluaciones y análisis de amenazas.
h. Mantener y actualizar protocolos de incidentes, coordinar la respuesta y los reportes a autoridades/Titulares según proceda.
i. Revisar y, de ser el caso, modificar condiciones contractuales con Encargados/Subencargados según resultados de evaluaciones y auditorías.
j. Actualizar comunicaciones externas (política, avisos de privacidad, banner de cookies, señalización CCTV).
k. Reportar periódicamente a la Alta Dirección sobre riesgos, controles, monitoreo, incidentes y planes de mejora.

VIII. PROCEDIMIENTO DE HABEAS DATA PARA EL EJERCICIO DE LOS DERECHOS DE INFORMACIÓN, ACCESO, ACTUALIZACIÓN, RECTIFICACIÓN, CANCELACIÓN (SUPRESIÓN), OPOSICIÓN Y REVOCATORIA

PHYX S.A.S., Establece el flujo, plazos y requisitos para que los Titulares (o sus legitimados) ejerzan sus derechos frente a la compañía, en los términos de la Constitución y la Ley 1581 de 2012.

a. Canales de atención

- Correo electrónico: protecciondedatos@phyx.co
- Formulario web: www.phyx.com (PQRS de datos personales).

Las respuestas se emitirán por el mismo canal de la solicitud, salvo indicación distinta del Titular.

b. Legitimación e identificación

Pueden presentar solicitudes: el Titular; sus causahabientes; el representante legal en caso de menores o incapaces; o apoderado con poder auténtico.
Para validar identidad/representación se debe adjuntar:

- Copia del documento de identidad del Titular (o del representante).
- Poder con reconocimiento de contenido ante notario (si aplica).
- Documentos que sustenten la petición (p. ej., correcciones solicitadas).

Protección de terceros: PHYX S.A.S. verificará la identidad antes de entregar información y anonimizará o tachará datos de terceros cuando sea necesario.

c. Contenido mínimo de la solicitud

- Nombres y apellidos del Titular (y representante, si aplica).
- Tipo y número de identificación.
- Derecho que se ejerce: acceso, actualización, rectificación, supresión, oposición o revocatoria (parcial o total) e información sobre el uso.
- Descripción clara y precisa de la petición y bases/soportes.
- Dirección física o electrónica de notificación.

- Firma (electrónica o manuscrita, según el canal).

Si la solicitud está incompleta, dentro de los cinco (5) días hábiles siguientes a su recepción se requerirá subsanar. Si el solicitante no aporta lo requerido dentro de los dos (2) meses siguientes, se entenderá desistida.

d. Clasificación y acuse de recibo

PHYX S.A.S. clasificará la petición como consulta o reclamo y enviará acuse de recibo dentro de los dos (2) días hábiles siguientes a la recepción completa.
Además, cuando corresponda, se registrará en la base de datos la leyenda:

- "Reclamo en trámite" (dentro de los 2 días hábiles posteriores a la recepción completa).
- "Reclamo resuelto" al finalizar el trámite.

e. Plazos de respuesta

Consultas (p. ej., acceso o información sobre el uso):

- Hasta diez (10) días hábiles desde la recepción completa.
- Si no fuere posible, antes de vencer el término se informará la causa y se ampliará por cinco (5) días hábiles adicionales.

Reclamos (p. ej., actualización, rectificación, supresión, oposición, revocatoria):

- Hasta quince (15) días hábiles desde la recepción completa.
- Si no fuere posible, se informarán los motivos y se ampliará por ocho (8) días hábiles adicionales.

Si PHYX S.A.S. no es Responsable de la base de datos involucrada (actúa como Encargado), informará tal situación al solicitante y remitirá el reclamo/consulta al Responsable pertinente, dejando constancia, y copiará dicha comunicación al Titular.

f. Criterios de decisión por tipo de derecho

- **Acceso:** Se entregará copia o consulta de los datos del Titular, finalidades, origen, transmisiones/transferencias y Responsable/Encargado, resguardando datos de terceros.

- **Actualización/Rectificación:** El Titular deberá indicar los datos a corregir/actualizar y aportar soporte; PHYX S.A.S. actualizará y notificará a Encargados / Subencargados pertinentes.

- **Supresión (cancelación):** Procede cuando los datos no sean necesarios o pertinentes para la finalidad, haya vencido el plazo de conservación o no se respeten principios/ derechos. No procede cuando exista deber legal o contractual de conservación o razones legítimas para su mantenimiento.

- **Oposición:** Se analizará la finalidad (p. ej., marketing directo) y se realizará juicio de proporcionalidad frente a derechos prevalentes o mandatos legales.

- **Revocatoria del consentimiento:** Parcial o total, cuando no subsista deber legal/contractual de conservar los datos.

- **Información sobre el uso:** Se informará el uso dado a los datos a petición del Titular.

g. Gratuidad, formatos y seguridad

- El trámite es gratuito. PHYX S.A.S. podrá cobrar costos de reproducción/envío cuando el Titular solicite copias físicas adicionales.

- Se dispondrán formatos (digitales y físicos) para facilitar el ejercicio de derechos.

- Las respuestas contendrán medidas de seguridad adecuadas (p. ej., cifrado de anexos, entrega presencial verificada, o canal autenticado).

h. Registro, trazabilidad y conservación

PHYX S.A.S. documentará y almacenará todas las solicitudes y respuestas, así como los marcadores de estado en las bases de datos (“reclamo en trámite/resuelto”) y conservará la trazabilidad conforme a las políticas internas de correspondencia y archivo.

i. Recurso ante la autoridad

Para acudir ante la Superintendencia de Industria y Comercio (SIC) se debe agotar previamente el trámite de consulta y/o reclamo descrito en esta sección. PHYX S.A.S. atenderá oportunamente los requerimientos que eleven las autoridades

competentes.

Nota especial - Datos sensibles y menores: cuando el reclamo o solicitud involucre datos sensibles (salud, biometría, orientación, etc.) o datos de menores de edad, PHYX S.A.S. aplicará verificación reforzada de identidad, limitación estricta del acceso, mecanismos de entrega segura y criterios de conservación mínima, privilegiando el interés superior del menor.

IX. REGISTRÓ CENTRAL DE BASES DE DATOS PERSONALES.

PHYX S.A.S. mantendrá un Registro Central de Bases de Datos Personales (RC-BD) que consolide y gobierne todas las bases de datos tratadas por la organización, tanto cuando actúe como Responsable como cuando actúe como Encargado. Este registro es obligatorio, auditable y se articula con el Registro Nacional de Bases de Datos (RNBD) administrado por la SIC cuando aplique.

a. Finalidad del RC-BD

- Identificar y controlar el ciclo de vida de cada base de datos (creación, uso, transmisión/transferencia, conservación y disposición final).
- Documentar finalidades, responsables, encargados, medidas de seguridad, retención y bases legales del tratamiento.
- Mantener la trazabilidad de cambios, incidentes y auditorías.
- Servir como insumo para RNBD, evaluaciones de impacto (PIA/DPIA), inventario de activos de información y matriz de riesgos.

b. Contenido mínimo por base de datos

Cada registro incluirá, como mínimo:

- **Identificación:** nombre único, código/ID, fecha de creación, estado (activa/suspendida/cancelada).
- **Propiedad y roles:** área propietaria; Responsable y Encargado/Subencargados (con datos de contacto); Custodio operativo.
- **Descripción y colectivo:** descripción funcional; colectivos de Titulares (empleados, ex empleados, candidatos, clientes, proveedores, visitantes, usuarios de plataformas, etc.).
- **Tipos y categorías de datos:** personales, sensibles, niños, niñas y adolescentes (si aplica), datos públicos/semiprivados/privados.
- **Finalidades del tratamiento:** específicas y explícitas, por proceso.

- **Base jurídica:** consentimiento, mandato legal/contractual u otra habilitación aplicable.
- **Origen/procedencia** y mecanismo de autorización (formato, casilla web, contrato, audio, etc.).
- **Sistema de tratamiento:** automatizada/no automatizada; repositorios (aplicación, CRM/ERP, DMS, nube, on-premise).
- **Localización y custodio técnico:** ubicación lógica/física; proveedor cloud y región si aplica.
- **Transferencias y transmisiones:** terceros receptores, país de destino, fundamento (país adecuado/cláusulas/consentimiento), canales y periodicidad.
- **Medidas de seguridad**: clasificación (alta/media/baja), controles relevantes (acceso/MFA, cifrado en tránsito/reposo cuando aplique, DLP, respaldo, registros y monitoreo, continuidad, seguridad física).
- **Retención y disposición:** plazos (archivo de gestión/central/total), evento de cierre, criterios de supresión/anonimización y saneamiento de medios.
- **Gobernanza:** RNBD (sí/no; fecha de registro/actualización), evaluaciones PIA/DPIA (fecha/estado), resultado de auditorías y última revisión.
- **Riesgos y controles:** nivel de riesgo inherente/residual, amenazas clave, controles ISO/IEC 27001:2022 asociados.
- **Incidentes y acciones:** historial de incidentes/brechas relacionados, decisiones y planes de mejora.
- **Notas legales:** restricciones contractuales con clientes/aliados, avisos de privacidad, señalización (CCTV), banner de cookies, bases sectoriales (p. ej., SFC cuando aplique).

c. Creación, actualización y cierre

- **Alta/creación:** toda nueva base de datos debe registrarse en el RC-BD antes de iniciar el tratamiento, acompañada de su finalidad, evaluación de riesgos y, cuando corresponda, PIA/DPIA y evidencia de autorización.
- **Actualizaciones:** cambios en finalidad, categorías de datos, roles, transferencias internacionales, medidas de seguridad, retención o estado deberán registrarse en el RC-BD en el menor tiempo posible y dentro de los plazos definidos por la SIC para el RNBD.
- **Revisión periódica:** el custodio actualizará el RC-BD con periodicidad mensual respecto de cambios operativos y, como mínimo, realizará una revisión integral anual (o ante cambios sustanciales).
- **Cierre/cancelación:** el cierre se registrará indicando motivos, evidencia de supresión/anonimización, retiro de respaldos y borrado seguro de medios, así como comunicación a terceros/Encargados.

d. **Integraciones con otros procesos**

- **Gestión de incidentes:** todo incidente relacionado con una base de datos se documentará en el RC-BD con su clasificación, causa raíz, impacto y acciones correctivas (ver Sección 19).
- **Control de cambios:** todo cambio tecnológico/organizacional que afecte el tratamiento (nuevos campos, nuevas integraciones, migraciones, nube, etc.) debe referenciar el ID de la base y dejar traza en el RC-BD.
- **Auditoría y cumplimiento:** el RC-BD será insumo de auditorías internas/externas (ISO 27001, ISO 9001, NTS-TS 006-1) y de requerimientos de autoridad.

Nota: El RC-BD es un documento controlado. Su acceso está restringido al personal autorizado y se gestiona conforme a los niveles de clasificación de la información y a los principios de necesidad de conocer.

X. TRATAMIENTO DE DATOS PERSONALES.

Las operaciones de tratamiento realizadas por PHYX S.A.S., en calidad de Responsable y/o Encargado, se ejecutan con sujeción a la Ley 1581 de 2012, normas reglamentarias y estándares internos de seguridad de la información. Todo tratamiento se limita a finalidades determinadas, explícitas y legítimas, con minimización de datos, medidas de seguridad proporcionales al riesgo y plazos de conservación definidos en el Anexo de Retención Documental y en el Registro Central de Bases de Datos (RC-BD).

i.Gestión del Recurso Humano

a. **Antes de la relación (selección y contratación)**

- **Finalidad:** evaluar idoneidad, validar referencias, aplicar pruebas, gestionar convocatorias y cumplimiento precontractual.

- **Información previa:** a los candidatos se les informan finalidades, derechos y canales; se documenta la autorización (p. ej., Formato F11-P28 u otros medios).

- **Conservación:**

- ✓ **No seleccionados:** eliminación segura (HV, pruebas, entrevistas) en máx. 3 meses, salvo autorización expresa para conservar en bolsa de talento por un plazo definido.
- ✓ **Seleccionados:** incorporación al legajo personal.

- ➢ **Terceros de reclutamiento:** contratos con encargo de tratamiento (DPA), finalidades y medidas de seguridad; eliminación/devolución de datos al cierre del proceso.

b. Durante la relación laboral/contractual

- ➢ **Legajo personal:** físico y/o digital, custodiado por Talento Humano; acceso por necesidad de conocer y mínimo privilegio.
- ➢ **Usos permitidos:** administración del vínculo (nómina, beneficios, evaluación, SST, formación, disciplinario), cumplimiento legal y contractual.
- ➢ **Requerimientos de autoridad:** validación jurídica de competencia y pertinencia; trazabilidad de entregas.

c. Después de la relación

- ➢ **Archivo central:** traslado del legajo con medidas altas de seguridad.
- ➢ **Conservación:** documentos del SG-SST por 20 años desde la terminación (Decreto 1072/2015) y demás soportes conforme al Anexo de Retención.
- ➢ **Cesión a terceros:** prohibida salvo autorización del Titular o habilitación legal expresa.

i. Accionistas

a. Carácter reservado conforme a libros societarios y normativa mercantil.
b. Finalidad: gestión estatutaria, convocatorias, dividendos y obligaciones legales.
c. Acceso: según Código de Comercio y reglas internas.

ii. Proveedores y personal del proveedor

a. Finalidad: selección, debida diligencia, ejecución y seguimiento contractual, seguridad de la cadena de suministro.
b. Datos tratados: identificación, contacto, idoneidad/certificaciones y, cuando proceda, validaciones para acceso a instalaciones/sistemas.
c. Minimización: solo lo necesario, pertinente y no excesivo.

d. **Personal del proveedor:** verificación de idoneidad y cumplimiento de requisitos del servicio; eliminación/devolución cuando cese la necesidad.
e. **Confidencialidad en órdenes de compra:** uso exclusivo para el objeto contratado, no divulgación, protección, y devolución/eliminación a solicitud o al cierre; obligación post-contractual y derecho de auditoría.

iii. Clientes y contactos (B2B)

a. **Finalidades:** prospección y gestión comercial, ejecución de servicios, atención de PQRS, satisfacción, facturación y cobranza, cumplimiento normativo.
b. **Datos de contacto profesionales:** tratados en su calidad de uso profesional sin perjuicio de los derechos del Titular; opt-out para comunicaciones de marketing.
c. **Intercambio de datos con clientes:** cuando se comparta información del personal de PHYX para la ejecución del servicio, se hará bajo contrato con obligaciones de seguridad equivalentes, control de acceso y derecho de auditoría.

iv. Proyectos de largo aliento con clientes (duración ≥ 4 meses)

a. **Identificación y clasificación**: definición de bases de datos por proyecto, categorías (personales/sensibles) y rol de PHYX (Responsable/Encargado).
b. **Consentimiento y contratos:** obtención de autorización cuando aplique; acuerdos de encargo (y de subencargo si corresponde) con medidas, fines y obligaciones equivalentes.
c. **Registro y gobernanza:** inscripción/actualización en RNBD cuando aplique; inclusión en RC-BD con finalidades, retención, controles e incidentes.
d. **Controles reforzados:** acceso por rol, autenticación robusta, registros de acceso, cifrado cuando aplique, respaldo y pruebas de restauración, monitoreo, planes de continuidad y gestión de incidentes con notificación conforme a ley/contrato.
e. **Transferencias internacionales:** (p. ej., Panamá, México, EE. UU. u otros LATAM) conforme a régimen de país adecuado o mecanismos contractuales vigentes; información al Titular cuando corresponda.

v. Plataformas web, dominios y aplicaciones

a. **Cobertura:** sitios web, formularios, aplicaciones y servicios digitales de PHYX.
b. **Bases jurídicas:** consentimiento; ejecución de contrato/medidas

precontractuales; cumplimiento legal; interés legítimo (seguridad, prevención de fraude, analítica con salvaguardas, marketing con opt-out).

c. **Cookies y tecnologías afines:** banner y Centro de Preferencias con categorías y finalidades; registro de consentimiento y gestión de caducidad.
d. **Derechos del Titular:** canales de la Sección VIII para acceso, rectificación, supresión, oposición y revocatoria.
e. **Política de Privacidad vigente:** detalla finalidades específicas y terceros receptores cuando aplique.

vi. Contratación, alianzas y cooperación con terceros

a. **Acceso por terceros:** sujetos a esta Política y a Acuerdo de Encargo (DPA) con medidas de seguridad acordes al tipo de dato.
b. **Proporcionalidad:** verificación de que el dato solicitado es indispensable para la finalidad.
c. **Subencargados:** requieren autorización previa del Responsable y deberes equivalentes.
d. **Incidentes:** notificación sin demora indebida al Responsable y cooperación en la mitigación.
e. **Auditoría:** PHYX se reserva derecho de auditoría y puede exigir evidencia de cumplimiento.

vii. Comunidad y actividades de RSE

a. **Finalidades:** convocatorias, participación, comunicación institucional y medición de impacto.
b. **Autorización previa e informada** en los instrumentos de recolección; tratamiento de datos sensibles solo cuando sea estrictamente necesario, con medidas reforzadas y conservación mínima.

viii. Reglas comunes a todo tratamiento

a. **Minimización y calidad**: solo datos adecuados, pertinentes y exactos; actualización oportuna.
b. **Acceso restringido:** necesidad de conocer y mínimo privilegio; segregación de funciones; revisiones periódicas de permisos.
c. **Retención y disposición:** plazos definidos en Anexo de Retención; supresión/anonimización y saneamiento de medios al cumplir la finalidad o vencer el plazo.
d. **Transferencias y transmisiones:** documentadas en RC-BD con base jurídica y salvaguardas; subencargados con autorización y obligaciones

equivalentes.

e. **Datos sensibles y de menores:** tratamiento excepcional y proporcional; evaluación de impacto cuando proceda; acceso estrictamente limitado; conservación mínima.
f. **Seguridad e incidentes:** controles administrativos, físicos y técnicos proporcionales al riesgo; gestión de incidentes conforme a los procedimientos internos y notificación a titulares y/o autoridades cuando aplique.
g. **Transparencia**: información clara en avisos de privacidad y canales efectivos para ejercer derechos (Sección VIII).

Contacto: Para consultas sobre el fundamento jurídico o ejercicio de derechos, escribir a protecciondedatos@phyx.co

XI. USUARIOS DE PLATAFORMAS

PHYX S.A.S. desarrolla parte de su actividad a través de sitios web, formularios, aplicaciones y servicios digitales ("las Plataformas"). Quien registre datos en las Plataformas declara que ha leído y acepta esta Política de Tratamiento de Datos Personales y los términos y condiciones aplicables. Si no está de acuerdo, no deberá registrarse ni suministrar datos.

i. Finalidades del tratamiento en Plataformas

Los datos personales se tratarán para:

- **Gestión de cuenta y soporte:** crear y administrar el registro, autenticar acceso, atender incidentes y PQRS.
- **Comunicaciones de servicio:** confirmaciones, notificaciones operativas, recordatorios y solicitudes de información.
- **Estadística y mejora:** métricas de uso, analítica y experiencia de usuario (datos agregados/seudonimizados cuando sea posible).
- **Seguridad y prevención de fraude:** monitoreo de accesos, detección de usos indebidos y protección de la infraestructura.
- **Relación comercial B2B:** coordinación de servicios y proyectos con clientes y prospectos.
- **Marketing con opción de exclusión:** envío de contenidos, novedades y promociones con opt-out en cada mensaje o en los centros de preferencia.
- **Eventos y logística:** inscripción, gestión de asistencia y comunicaciones relacionadas.

- **Cumplimiento legal** y requerimientos de autoridad.

En contextos B2B, los datos de contacto profesionales se usan para fines operativos y comerciales legítimos, sin perjuicio del derecho a oponerse al marketing.

ii. Base jurídica

- Consentimiento (formularios, newsletters, cookies no esenciales).
- Ejecución de contrato o medidas precontractuales (cuenta, soporte, prestación del servicio).
- Cumplimiento legal (retenciones, reportes).
- Interés legítimo (seguridad, prevención de fraude, analítica básica, comunicaciones B2B), con salvaguardas y opt-out para marketing.

iii. Cookies y tecnologías similares

- Uso de banner y Centro de Preferencias con categorías (esenciales, medición, funcionales, publicidad).
- Registro y gestión del consentimiento; el usuario puede retirar o modificar su elección en cualquier momento.

iv. Derechos de los titulares en Plataformas

- Acceso, actualización, rectificación, supresión, oposición y revocatoria del consentimiento, conforme a la Sección VIII.

- Canales: protecciondedatos@phyx.co y mecanismos habilitados en las Plataformas.
- Todas las comunicaciones de marketing incluyen desuscripción inmediata.

v. Contenido generado por el usuario (UGC) e identidad

- El usuario puede publicar o cargar materiales (texto, imagen, audio, video) según los términos de uso.
- Podrán emplearse nombres o seudónimos para identificar autoría en la Plataforma.
- El usuario declara contar con derechos y permisos necesarios (incluye permisos de imagen de terceros y licencias/copyright del material).
- PHYX podrá solicitar acreditación de derechos, moderar o retirar contenidos que infrinjan la ley, derechos de terceros o esta Política.

PHYX

vi. Uso de imagen y material de terceros para difusión

- Para fines promocionales (p. ej., eventos, casos de éxito), PHYX solicitará autorizaciones de uso de imagen y, cuando aplique, licencias o permisos de materiales de terceros (fotografías, logotipos, obras protegidas), con alcance, duración y territorio definidos.
- El titular puede revocar el permiso salvo que exista otra base legal o obligación contractual que lo impida.

vii. Niños, niñas y adolescentes

- Las Plataformas no están dirigidas a menores. Si excepcionalmente se tratan datos de NNA, se exigirá autorización del representante legal y se aplicarán medidas reforzadas.

viii. Conservación y seguridad

- Conservación por los plazos necesarios para las finalidades o los exigidos por ley y luego supresión/anonimización.
- Medidas de seguridad administrativas, físicas y técnicas proporcionales al riesgo (acceso por rol, registros, cifrado cuando aplique, respaldos, monitoreo, continuidad y gestión de incidentes).

ix. Transferencias y encargados

- Podrán realizarse transmisiones a proveedores (encargados) para operar las Plataformas, sujetos a DPA y controles equivalentes.
- Transferencias internacionales (p. ej., centros de datos o soporte en otros países) se realizarán con salvaguardas contractuales y conforme a la regulación vigente; se actualizará el RC-BD/RNBD cuando aplique.

x. Información transparente

- La Política de Privacidad específica de las Plataformas detalla las categorías de datos, finalidades concretas, terceros receptores, mecanismos de opt-out y cookies.
- Cualquier cambio material será comunicado por medios visibles en las Plataformas.

PHYX

XII. PROHIBICIONES

En PHYX S.A.S. queda terminantemente prohibido realizar las siguientes conductas en relación con datos personales y activos de información. Su incumplimiento acarrea sanciones disciplinarias y contractuales, sin perjuicio de responsabilidades civiles, administrativas y penales.

i. Tratamiento sin legitimación

a. Tratar datos personales sin autorización válida del titular o sin base jurídica aplicable.
b. Ampliar finalidades más allá de las informadas ("función diferente") o realizar perfilamientos incompatibles.
c. Reidentificar información anonimizada o intentar revertir procesos de seudonimización.
d. Recabar datos excesivos o no pertinentes frente a la finalidad.

ii. Datos sensibles y de menores

a. Tratar datos sensibles (salud, biometría, orientación, etc.) sin autorización expresa y salvaguardas reforzadas.
b. Tratar datos de niños, niñas y adolescentes sin autorización del representante legal y sin asegurar el interés superior del menor.
c. Capturar biometría, CCTV o control de accesos sin aviso, señalización y medidas de minimización.

iii. Acceso, uso y divulgación no autorizados

a. Acceder, usar, consultar, copiar, extraer, ceder, circular o divulgar datos personales sin necesidad y sin permiso ("curiosidad" o "fishing interno").
b. Compartir información por canales inseguros (apps de mensajería no autorizadas, correos personales, dispositivos no gestionados).
c. Publicar datos en internet/intranets sin control de acceso, sin cifrado cuando aplique o sin autorización del custodio.
d. Transferir al exterior sin salvaguardas contractuales o hacia países sin nivel adecuado.
e. Entregar información a autoridades sin validar competencia, alcance y proporcionalidad.

iv. Seguridad de la información

a. Compartir credenciales, desactivar MFA, eludir controles, usar contraseñas débiles o reutilizadas.
b. Introducir shadow IT (uso no autorizado o no gestionado por TI), (servicios en la nube, apps, extensiones) sin evaluación y aprobación de TI/Seguridad.
c. Extraer datos a dispositivos personales o medios removibles no cifrados; almacenar datos en ubicaciones no aprobadas.
d. Usar datos reales de producción en ambientes de prueba/desarrollo sin enmascaramiento o base jurídica.
e. Alterar, borrar o manipular registros, logs o evidencias de seguridad.
f. Omitir el reporte inmediato de incidentes o debilidades conocidas.

Para el SGSI se tienen en cuenta, las políticas descritas en el **Manual de Políticas específicas de seguridad de la información y cbs.**

v. Conservación y disposición

a. Conservar datos más allá de los plazos definidos o eliminar antes de tiempo sin causa legal.
b. Disponer de información sin borrado seguro o sin saneamiento de medios.

vi. Marketing y canales digitales

a. Enviar comunicaciones comerciales sin consentimiento cuando sea exigible o sin opción de opt-out visible y funcional.
b. Implementar cookies no esenciales sin consentimiento o sin centro de preferencias.
c. Usar material de terceros (imágenes, logos, obras) o imagen de personas sin permisos/licencias y sin respetar derechos de autor.

vii. Proveedores y subencargados

a. Entregar datos a terceros sin contrato de encargo (DPA) o sin cláusulas de transmisión/transferencia.
b. Subcontratar (subencargados) sin autorización previa ni obligaciones equivalentes.
c. Negarse a permitir auditorías o a notificar incidentes sin demora indebida.

viii. Derechos de los titulares

a. Obstaculizar o demorar injustificadamente el ejercicio de derechos (acceso, rectificación, supresión, oposición, revocatoria).

b. Usar patrones oscuros (dark patterns) para obtener o mantener consentimientos.

ix. Sanciones y consecuencias

a. Empleados: llamadas de atención, suspensión y/o terminación con justa causa conforme al reglamento interno, además de acciones civiles o penales cuando aplique.
b. Contratistas/proveedores: terminación anticipada del contrato, multas, indemnizaciones por daños, reporte a listas de desempeño y ejercicio de acciones legales.
c. Organizacionales: reporte a autoridad competente, medidas correctivas y preventivas, y fortalecimiento de controles.

x. Excepciones y canal de aprobación

Cualquier excepción estrictamente necesaria (p. ej., entrega a autoridad competente, uso de datos sensibles por obligación legal) debe:

a. Contar con análisis de base jurídica y proporcionalidad,
b. Aprobación previa y escrita de Jurídica/Protección de Datos y Seguridad de la Información, y
c. Quedar documentada en el Registro Central de Bases de Datos (RC-BD).

Reporte y consultas: incidentes o dudas deben notificarse de inmediato a gestiondelriesgo@phyx.co y protecciondedatos@phyx.co

XIII. TRANSFERENCIA INTERNACIONAL DE DATOS.

PHYX S.A.S. podrá realizar transferencias (entrega de datos a un Responsable ubicado en otro país) y transmisiones (encargo de tratamiento a un Encargado ubicado en otro país) únicamente cuando exista base jurídica válida y salvaguardas adecuadas, garantizando un nivel de protección equivalente al exigido por la normativa colombiana.

i. Principios y alcance

- **Necesidad y proporcionalidad:** solo datos pertinentes para la finalidad transferida; minimización por defecto.
- **Equivalencia de protección:** el país de destino debe ofrecer nivel adecuado de protección o, en su defecto, aplicarse salvaguardas contractuales y

técnicas que garanticen derechos y seguridad.

- **Trazabilidad:** toda transferencia/transmisión se registra en el Registro Central de Bases de Datos (RC-BD) y, cuando aplique, en el RNBD.
- **Transparencia:** las finalidades, destinatarios y países se informan en la Política/Aviso de Privacidad y, cuando corresponda, al Titular.

ii. Regímenes de destino y países de operación

- **Operación prevista:** Potencialmente otras jurisdicciones de LATAM.
- **Evaluación por país y proveedor:** previo a transferir, PHYX clasifica el destino como adecuado o no adecuado según lineamientos de la SIC y evalúa al receptor (Responsable/Encargado) en seguridad, privacidad y legalidad.

iii. Bases y escenarios que habilitan la transferencia

Se podrán realizar excepcionalmente cuando concurra al menos una de las siguientes bases:

- Ejecución de contrato con el Titular o medidas precontractuales adoptadas a solicitud del Titular.
- Transacciones bancarias y bursátiles conforme a la legislación aplicable.
- Tratados internacionales incorporados al ordenamiento jurídico colombiano.
- Interés público o requerimiento legal/administrativo/judicial debidamente motivado y proporcional.
- Consentimiento expreso, previo e informado del Titular, cuando resulte aplicable.

Cuando el país no sea considerado “seguro/adecuado”, el consentimiento por sí solo no exime de implementar salvaguardas contractuales y técnicas.

iv. Salvaguardas obligatorias (si el destino no es adecuado)

Antes del envío/recepción, se deberán implementar y documentar, como mínimo:

- **Contrato de transferencia o transmisión (DPA/CCT):** finalidades, categorías de datos, roles, subencargados, medidas técnicas y organizativas, confidencialidad, asistencia en derechos, auditoría, onward transfers (transferencias ulteriores) con obligaciones equivalentes, retorno/eliminación al cierre y notificación de incidentes sin demora indebida.

- **Evaluación de impacto y de transferencias (PIA/TIA):** análisis de riesgos legales, regulatorios y técnicos del país receptor; medidas de mitigación.
- **Controles técnicos reforzados:** cifrado en tránsito y, cuando corresponda, en reposo; gestión de claves; control de acceso por rol y mínimo privilegio; registro y monitoreo de accesos; segregación de ambientes; pruebas de restauración de copias de seguridad.
- **Limitación de finalidad y retención:** tiempos definidos, eliminación / anonimización al vencimiento.
- **Derechos del Titular:** cooperación del receptor para atender acceso, rectificación, supresión, oposición y revocatoria en plazos legales.
- **Auditoría y verificación:** derecho de auditoría de PHYX y entrega de evidencias de cumplimiento por el receptor.

v. Flujo de aprobación y documentación

Toda transferencia/transmisión internacional debe:

- **Ser solicitada por el área dueña del proceso con:** finalidad, categorías de datos, volumen, país(es), receptor(es), base jurídica y plazo.
- Contar con revisión y aprobación previa y escrita del Oficial de Protección de Datos y del área Jurídica (contratos, CCT/DPA, TIA/PIA).
- Quedar inscrita/actualizada en el RC-BD (y RNBD cuando aplique), incluyendo destino, base, salvaguardas y plazo de conservación.

vi. Receptores y subencargados

- El receptor (Responsable/Encargado) no podrá subcontratar (subencargados) sin autorización previa y por escrito de PHYX, imponiéndoles obligaciones equivalentes (flujo descendente).
- En proyectos con múltiples jurisdicciones, cada eslabón de la cadena debe operar con salvaguardas equivalentes y reportar incidentes al punto único definido por PHYX.

vii. Derechos, incidentes y cooperación regulatoria

- PHYX y el receptor garantizarán el ejercicio de derechos de los Titulares sin discriminación por el lugar de tratamiento.
- Incidentes/brechas: el receptor notificará a PHYX sin demora indebida; PHYX procederá conforme a los procedimientos internos y obligaciones frente a SIC y Titulares.

- Requerimientos de autoridad extranjera: el receptor deberá informar y canalizar a través de PHYX y Jurídica; solo se revelará lo estrictamente necesario, dejando trazabilidad.

viii. Prohibiciones y restricciones

- Está prohibida la transferencia a países sin garantías adecuadas sin salvaguardas contractuales y técnicas previas.
- Se prohíbe la reidentificación de datos anonimizados, la ampliación de finalidades, y el uso para perfilamiento no compatible.
- Se prohíbe cualquier onward transfer que no replique las obligaciones pactadas con PHYX.

ix. Actualización y revisión

- Las transferencias internacionales serán revisadas al menos anualmente o ante cambios de proveedor, país, legislación o arquitectura.
- Cualquier modificación de destino, finalidad o receptor exige nueva evaluación y adenda contractual antes de continuar el flujo.

Canal de consultas/aprobaciones: protecciondedatos@phyx.co (con copia a Jurídica).
Registro: toda transferencia/transmisión debe estar reflejada en el RC-BD y, cuando corresponda, en el RNBD.

XIV. ROLES Y RESPONSABILIDADES EN EL CUMPLIMIENTO DE LA PROTECCION DE DATOS PERSONALES.

La protección de datos en PHYX S.A.S. es una responsabilidad transversal basada en el principio de responsabilidad demostrada. Toda área y persona que trate datos personales debe cumplir esta Política, las normas aplicables y los procedimientos internos.

i. Alta Dirección

- Aprobar la Política, sus revisiones y el Programa de Privacidad.
- Asignar recursos, priorizar riesgos y patrocinar la cultura de protección de datos.
- Recibir y evaluar reportes periódicos de riesgos, incidentes y cumplimiento.

ii. Oficial de Protección de Datos (OPD)

- Diseñar, mantener y mejorar el Programa de Privacidad y el RC-BD (Registro Central de Bases de Datos).
- Registrar/actualizar, cuando aplique, las bases en el RNBD y atender requerimientos de la SIC.
- Definir y actualizar procedimientos (gestión de derechos, incidentes, retención, cookies, CCTV, biometría).
- Coordinar DPIA/PIA y TIAs (evaluaciones de impacto y de transferencias).
- Revisar y aprobar cláusulas y contratos de transmisión/transferencia (incl. subencargados).
- Liderar formación y campañas de concienciación.

iii. Seguridad de la Información / TI

- Implementar y operar controles administrativos, físicos y técnicos (acceso por rol, mínimo privilegio, MFA, cifrado cuando aplique, respaldo y restauración, monitoreo y registros).
- Gestionar vulnerabilidades, continuidad y respuesta a incidentes; mantener evidencias (logs).
- Validar nuevas soluciones (on-prem/cloud) y prevenir shadow IT.

iv. Jurídica/Compliance

- Asegurar la base jurídica de cada tratamiento y la conformidad contractual (DPA/CCT, NDA, licencias y permisos de imagen/copyright).
- Atender y canalizar requerimientos de autoridades; definir criterios de proporcionalidad.
- Apoyar en investigaciones de incidentes y en medidas correctivas.

v. Propietarios de Proceso / Dueños de Base de Datos

- Definir finalidades, categorías y plazos de conservación de “su” base; mantenerla actualizada en el RC-BD.
- Garantizar minimización de datos y calidad (exactitud/actualización).
- Autorizar accesos bajo necesidad de conocer; realizar revisiones periódicas de permisos.

vi. Custodios de la Base de Datos

- Operar controles de acceso y uso legítimo; ejecutar retención y disposición segura.
- Registrar cambios, incidentes y transferencias; asegurar la trazabilidad.

vii. Encargados y Subencargados (terceros)

- Tratar datos solo conforme instrucciones de PHYX y contrato de encargo.
- Notificar incidentes sin demora indebida y permitir auditorías.
- No subcontratar sin autorización previa y obligaciones equivalentes.

viii. Talento Humano

- Gestionar tratamientos de RR. HH. (selección, nómina, SST, disciplina) según esta Política.
- Custodiar legajos; ejecutar plazos (p. ej., 3 meses no seleccionados; 20 años SG-SST).
- Incluir cláusulas de confidencialidad y cumplimiento en contratos laborales/servicios.

ix. Comercial/Marketing/UX

- Gestionar consentimiento, opt-out y preferencias (newsletters, campañas).
- Respetar listas de exclusión y límites de perfilamiento; gobernanza de cookies/martech.
- Verificar permisos de imagen y derechos de autor en piezas y casos de éxito.

x. Gestión de Proyectos/PMO (incluye proyectos de largo aliento)

- Identificar el rol (Responsable/Encargado), las bases de datos del proyecto y su registro.
- Asegurar contratos de encargo/transferencia, controles reforzados y reporting.
- Coordinar con OPD y Seguridad la gestión de riesgos y los planes de respuesta.

xi. Auditoría Interna/Calidad

- Verificar cumplimiento legal y de esta Política/ISO; emitir hallazgos y seguimiento.
- Evaluar eficacia de controles y mejora continua.

xii. Todos los usuarios (empleados y contratistas)

- Usar la información conforme finalidad, mantener confidencialidad y reportar

incidentes de inmediato.

- No compartir credenciales, no extraer datos a medios no autorizados ni usar canales inseguros.

xiii. Matriz RACI resumida (actividades clave)

Actividad	Responsable (R)	Aprobador (A)	Consultado (C)	Informado (I)
Actualizar Política y Programa de Privacidad	OPD	Alta Dirección	Jurídica, Seguridad, Calidad	Todas las áreas
Registro/actualización RC-BD/RNBD	OPD / Prop. Proceso	OPD	Jurídica, Seguridad, TI	Alta Dirección
Gestión de derechos (ARCO/Revocatoria)	OPD	Jurídica	Prop. Proceso	Solicitante, Alta Dirección
Incidentes de seguridad (detección-respuesta)	Seguridad/TI	OPD/Jurídica	Prop. Proceso, PMO	Alta Dirección, Usuarios afectados
DPIA/PIA y TIA	OPD	Jurídica	Seguridad, Prop. Proceso, PMO	Alta Dirección
Contratos DPA/Transferencias	Jurídica	OPD	PMO, Prop. Proceso, Seguridad	Compras, Alta Dirección
Revisión de accesos y mínimos privilegios	Prop. Proceso	Seguridad	TI, OPD	Auditoría/Calidad
Retención y disposición segura	Custodio	Prop. Proceso	OPD, Seguridad	Auditoría/Calidad
Formación y concienciación	OPD	Alta Dirección	Seguridad, Talento Humano	Todas las áreas

XV. TEMPORALIDAD DEL DATO PERSONAL.

La conservación de los datos personales en PHYX S.A.S. se rige por el principio de finalidad y necesidad: solo se mantendrán por el tiempo estrictamente necesario para cumplir la finalidad informada, atender obligaciones legales/contractuales y soportar la defensa de derechos. Cumplidos estos propósitos, los datos serán suprimidos o anonimizados de forma segura.

i. Reglas generales de conservación

a. **Vinculación a la finalidad:** cada base de datos tendrá un plazo de retención

definido en el Registro Central de Bases de Datos (RC-BD), alineado con su finalidad.

b. **Minimización y revisión periódica:** los plazos serán revisados al menos una vez al año o cuando cambie la finalidad, el marco legal o el riesgo.
c. **Legal/contractual prevalente**: si existe un término legal o contractual específico, éste prevalece sobre la finalidad.
d. **Bloqueo y legal hold:** cuando haya litigios, auditorías o requerimientos de autoridad, los datos serán bloqueados (suspendida su eliminación) hasta el cierre formal del proceso (legal hold).
e. **Eliminación/anonimización segura:** agotada la finalidad o vencido el plazo, se aplicará borrado seguro o anonimización irreversible; se dejará evidencia (acta/log) de la disposición.
f. **Backups:** los respaldos mantienen los mismos plazos; al vencimiento, se asegura su depuración o cifrado con destrucción de claves que imposibilite la recuperación.
g. **Trazabilidad:** todo ciclo de retención y disposición se documenta en el RC-BD (fecha de alta, cambios de plazo, eventos de legal hold, fecha y método de eliminación).

ii. Plazos de referencia por categoría (ejemplos típicos)

Los siguientes son plazos guía; el RC-BD definirá el plazo exacto para cada base:

CATEGORÍA / PROCESO	PLAZO DE CONSERVACIÓN TÍPICO	OBSERVACIONES CLAVE
Candidatos no seleccionados	3 meses	Eliminación de HV/pruebas; conservación mayor solo con consentimiento o obligación legal.
Historia laboral / Nómina / SST	20 años desde la terminación	Conforme a exigencias de SG-SST y archivo laboral.
Contratos (clientes/proveedores) y expedientes contractuales	5 a 10 años	Según prescripción civil/mercantil; puede ampliarse por defensa de derechos.
Contable y fiscal (facturas, soportes)	10 años	Según régimen de comercio y archivo.
PQRS y servicio	2 a 5 años	Según riesgos, garantías y trazabilidad de atención.
Marketing y newsletters	Vigencia del consentimiento o hasta oposición/opt-out	Minimizar y depurar contactos inactivos; registrar opt-out.

CATEGORÍA / PROCESO	PLAZO DE CONSERVACIÓN TÍPICO	OBSERVACIONES CLAVE
CCTV / control de accesos	30 a 90 días	Extensible si hay incidentes o requerimientos. Señalización y acceso restringido.
Seguridad/monitoreo (logs, telemetría)	6 a 24 meses	Según análisis de riesgo, continuidad y forense; minimizar datos personales.
Proyectos de largo aliento (≥4 meses)	Durante el proyecto + plazo contractual	Al cierre: devolución/eliminación o anonimización; actualizar RNBD/RC-BD.
Atenciones legales (reclamaciones, litigios)	Mientras dure el proceso + prescripción	Legal hold con bloqueo de eliminación hasta cierre definitivo.

iii. Criterios para definir/eliminar

- **Base jurídica:** contrato, obligación legal, consentimiento o interés legítimo con salvaguardas.
- **Riesgo y sensibilidad:** a mayor criticidad (p. ej., datos sensibles), menor plazo operativo y controles reforzados.
- **Necesidad operacional:** concluir servicios, auditorías y garantías.
- **Defensa de derechos:** extensión razonable para atender controversias (documentar razón y nueva fecha).

iv. Procedimiento de disposición final

- **Verificación previa:** validar ausencia de legal hold y que se cumplieron finalidades/obligaciones.
- **Selección del método:**
  - ✓ **Digital:** borrado seguro (sobre-escritura; eliminación criptográfica) o anonimización.
  - ✓ **Físico:** triturado/pulverizado o proveedor certificado.
- **Evidencia:** generar acta/log (qué, cuándo, cómo, quién).
- **Backups:** programar depuración en la siguiente ventana de retención o revocar claves si se usa cifrado por compartimiento.
- **Actualización del RC-BD:** registrar la disposición y ajustar el inventario si procede.

v. Derechos del titular y retención

- Las solicitudes de supresión y revocatoria se atienden cuando no exista una obligación legal/contractual de conservar.
- Si la supresión no procede, el dato quedará en bloqueo (uso restringido) hasta el vencimiento legal.

Nota: Los plazos definitivos y responsables constan en el Registro Central de Bases de Datos y en los procedimientos de retención y disposición asociados a cada proceso. Cualquier excepción debe contar con aprobación previa y escrita de Jurídica y del Oficial/Líder de Protección de Datos y quedar documentada.

XVI. MEDIDAS DE SEGURIDAD

PHYX S.A.S. adopta controles administrativos, físicos y tecnológicos acordes con el riesgo y la criticidad de los datos personales tratados, en línea con buenas prácticas del SGSI y la ISO/IEC 27001:2022. Todos los destinatarios de esta Política deben cumplir estas medidas y reportar de inmediato cualquier sospecha de vulneración o tratamiento inadecuado.

i. Principios y gobierno de la seguridad

- **Enfoque basado en riesgos:** identificación, valoración y tratamiento de riesgos por proceso y base de datos; revisión periódica.
- **Clasificación y manejo de la información:** pública, interna, confidencial y sensible; etiquetado y controles por nivel.
- **Privacidad desde el diseño y por defecto:** minimización de datos, separación de funciones y configuración segura.
- **Cadena de suministro:** evaluación y obligaciones contractuales a proveedores/encargados (DPA, cláusulas de seguridad, derecho de auditoría, notificación de incidentes, subencargos controlados).
- **Continuidad y resiliencia:** BIA, RTO/RPO definidos, respaldo y recuperación probados, sitios alternos cuando aplique.

ii. Controles administrativos

- **Políticas y procedimientos vigentes** (accesos, uso aceptable, BYOD/teletrabajo, retención y disposición, control de cambios, respaldo/recuperación, respuesta a incidentes, uso de imagen y derechos de autor).
- **Gestión de identidades y accesos (IAM):** alta/baja/cambio de usuarios, revisiones periódicas de permisos, mínimo privilegio y segregación de

funciones.

- **Concienciación y capacitación anual y por rol** (incluye phishing, manejo de sensibles, reporte de incidentes).
- **Gestión de terceros:** due diligence de seguridad, matrices de cumplimiento, TIAs/DPIAs cuando apliquen.
- **Gestión de proyectos de largo aliento:** registro y control de bases del proyecto, contratos de encargo/transferencia, controles reforzados.

iii. Controles físicos

- **Perímetro y acceso físico:** credenciales, registros de visitantes, CCTV con retención limitada, zonas restringidas para salas de servidores/archivos.
- **Protección de medios:** gabinetes cerrados, transporte seguro de medios, borrado y destrucción certificados de papel y soportes al final de su vida útil.
- **Ambiente y energía**: controles contra incendio, UPS, climatización y detección de agua donde aplique.

iv. Controles tecnológicos

- **Autenticación y MFA:** MFA obligatorio para accesos remotos, cuentas privilegiadas, VPN y sistemas críticos.
- **Cifrado:** en tránsito (TLS) y en reposo cuando aplique; gestión segura de llaves (HSM/servicios KMS).
- **End-point y servidores:** EDR/antimalware, hardening, parches y gestión de vulnerabilidades con escaneos regulares y corrección priorizada.
- **Red y perímetro:** segmentación, firewalls, WAF para apps expuestas, listas de control de acceso, VPN con cifrado fuerte.
- **Monitoreo y registros:** centralización de logs, correlación de eventos, alertas y conservación proporcional al riesgo.
- **Desarrollo y pruebas:** control de cambios, revisiones de código y prohibido usar datos reales en pruebas sin enmascaramiento/apropiada base legal.
- **Datos y DLP:** controles de fuga (DLP), bloqueo de copias no autorizadas, control de cargas/descargas en nube.
- **SaaS/Nube:** configuración segura (CSPM), principio de responsabilidad compartida, segregación de ambientes, backups verificados.

v. Medidas mínimas por nivel de seguridad de la base de datos

NIVEL	EJEMPLOS DE DATOS	MEDIDAS MÍNIMAS OBLIGATORIAS
Bajo	Contacto B2B no sensible, contenidos públicos	Políticas y capacitación; control de accesos por rol; cifrado en tránsito; respaldo periódico; hardening básico y parches regulares.
Medio	Clientes y proveedores (datos personales no sensibles), PQRS	Todo lo anterior + MFA para accesos administrativos; cifrado en reposo donde aplique; registros centralizados; revisión trimestral de permisos; DPA con terceros; pruebas de recuperación.
Alto	Datos sensibles (salud, biometría), RR.HH./nómina, menores, credenciales	Todo lo anterior + segregación de redes; tokenización/enmascaramiento; control reforzado de cuentas privilegiadas (PAM); escaneo continuo de vulnerabilidades; DLP; monitoreo 24/7 de eventos críticos; pruebas de intrusión periódicas; borrado seguro certificado.

El nivel se define en el Registro Central de Bases de Datos (RC-BD) y se revisa ante cambios de riesgo, tecnología o normativa.

vi. Gestión y reporte de incidentes

- **Detección y reporte inmediato:** cualquier colaborador o proveedor debe reportar de inmediato sospechas a gestiondelriesgo@phyx.co y protecciondedatos@phyx.co por los canales definidos.
- **Respuesta estructurada:** contención, análisis, erradicación, recuperación y lecciones aprendidas, con trazabilidad completa.
- **Notificaciones externas:** PHYX evaluará y realizará las notificaciones a autoridades y titulares en los plazos legales aplicables, de acuerdo con la naturaleza y severidad del incidente.
- **Post-mortem y mejora:** registro del incidente en el RC-BD, acciones correctivas/preventivas y actualización de controles.

vii. Obligaciones del personal y de terceros

- Cumplimiento estricto de esta Política y de los procedimientos asociados.
- Uso legítimo según finalidad; prohibido compartir credenciales, almacenar datos en medios no autorizados o usar canales inseguros.
- Colaboración en auditorías, pruebas y actividades de mejora continua del SGSI.

Nota: Cualquier excepción a estas medidas debe estar justificada por riesgo, aprobada por escrito por Seguridad de la Información y el Oficial/Líder de Protección de Datos, y registrada en el RC-BD.

PHYX

XVII. PROCEDIMIENTOS Y SANCIONES.

PHYX S.A.S. adopta un régimen interno de cumplimiento, investigación y consecuencias para prevenir, detectar, corregir y sancionar el tratamiento indebido de datos personales. Este régimen se articula con las facultades sancionatorias de la Superintendencia de Industria y Comercio (SIC) previstas en la Ley 1581 de 2012 (multas; suspensión de actividades de tratamiento; cierre temporal; y, tratándose de datos sensibles, cierre definitivo de la operación involucrada).

i. Activación del procedimiento (cómo se inicia)

Se activa por cualquiera de estos gatillos:

- Reporte de un incidente o sospecha de incumplimiento.
- Hallazgo de auditoría interna/externa.
- Requerimiento de autoridad (p. ej., SIC).
- Queja de un Titular o tercero.

Quien tenga conocimiento debe reportar de inmediato por los canales oficiales (gestiondelriesgo@phyx.co y protecciondedatos@phyx.co), sin filtrar información fuera de los mecanismos definidos.

ii. Gestión del caso (paso a paso)

a. **Contención inicial y preservación de evidencias:** Seguridad/TI ejecuta contención; Jurídica y el Oficial de Protección de Datos (OPD) activan legal hold y preservan trazabilidad (logs, correos, respaldos, medios).
b. **Apertura de investigación interna:** OPD lidera; participan Seguridad/TI, Jurídica y el dueño del proceso afectado. Se designa un responsable del caso y un número de expediente.
c. **Análisis de causa raíz y alcance:** identificación de datos comprometidos, categorías (sensibles o no), sistemas, terceros involucrados, impacto y obligaciones de notificación.
d. **Plan de acción correctivo/preventivo:** medidas inmediatas y estructurales con plazos, responsables y criterios de verificación.
e. **Notificaciones externas (si aplican):** a Titulares y/o SIC, conforme tiempos y requisitos legales.
f. **Cierre y lecciones aprendidas:** acta de cierre, actualización de controles/procedimientos y capacitación focalizada.

Todo el proceso se documenta en el Registro Central de Bases de Datos (RC-BD) y en el repositorio de incidentes.

iii. Criterios de severidad

La clasificación orienta las medidas y sanciones internas:

- **Leve:** incumplimiento formal sin exposición de datos ni reiteración.
- **Moderado:** exposición limitada, sin datos sensibles, con rápida contención.
- **Grave:** exposición amplia o de datos sensibles, o incumplimiento de obligaciones de notificación/atención de derechos.
- **Crítico:** afectación masiva, reidentificación/venta/divulgación dolosa, reincidencia o desatender instrucciones de autoridad.

iv. Medidas internas (además de las legales)

Según la severidad y la relación con PHYX, podrán imponerse una o varias de las siguientes acciones:

a. Para empleados y contratistas individuales

- Amonestación escrita y plan de mejora.
- Capacitación obligatoria y evaluación.
- Suspensión temporal de accesos o funciones, rotación de tareas.
- Sanción disciplinaria conforme reglamento interno (hasta terminación del contrato con justa causa).
- Responsabilidad civil/penal, si procede.

b. Para proveedores/encargados/subencargados

- Plan correctivo con plazos y evidencia de cierre.
- Penalidades contractuales y retención de pagos según DPA/orden de compra.
- Auditoría extraordinaria o incremento de controles.
- Suspensión o terminación del contrato, e inhabilidad temporal para nuevas contrataciones.
- Exigencia de notificación a sus propios subencargados y flujo descendente de obligaciones.

c. Para áreas/procesos internos

- Revisión de diseño del proceso, DPIA/TIA, ajustes de controles.
- Reconfiguración de roles y accesos; segregación de funciones.
- Endurecimiento de políticas (p. ej., DLP, cifrado, backups, retenciones).
- Incremento de monitoreo y reportes a la Alta Dirección.

v. Garantías del debido proceso

a. Notificación al presunto infractor y oportunidad de descargos.
b. Imparcialidad del equipo investigador.
c. Decisión motivada por escrito y derecho de recurso conforme a los reglamentos aplicables.

vi. Cooperación con autoridades y terceros

a. Todas las actuaciones con la SIC u otra autoridad serán coordinadas por Jurídica y el OPD.
b. Las respuestas serán íntegras, oportunas y con evidencias verificables.
c. Cuando aplique, se realizarán notificaciones a Titulares con lenguaje claro, medidas adoptadas y canales de atención.

vii. Reincidencia y agravantes/atenuantes

a. **Agravantes:** dolo, ocultamiento, reincidencia, afectación de datos sensibles o de niños/adolescentes, desobedecer instrucciones de autoridad.
b. **Atenuantes:** autorreporte temprano, colaboración plena, contención eficaz, evidencia de controles previos y capacitación vigente.

viii. Cierre y mejora continua

a. Cada caso cerrará con acta, evidencias de ejecución del plan y lecciones aprendidas.
b. Las políticas y procedimientos se actualizarán según hallazgos; se programará capacitación focalizada.
c. La Alta Dirección recibirá reportes periódicos con tendencias, KPIs (tiempos de contención, notificación, cierre) y acciones de mejora.

Nota: Este régimen no sustituye las sanciones de ley. La SIC puede imponer, entre otras, multas, suspensión de actividades de tratamiento y cierres temporales o definitivos de operaciones, especialmente cuando involucran datos sensibles. PHYX S.A.S. hará todo lo necesario para evitar estas consecuencias mediante prevención, respuesta efectiva y cumplimiento demostrable.

PHYX

XVIII. ENTREGA DE DATOS PERSONALES A AUTORIDADES.

PHYX S.A.S. atenderá requerimientos de autoridades únicamente por los canales formales y bajo criterios de legalidad, necesidad, proporcionalidad y trazabilidad. El objetivo es garantizar el cumplimiento del mandato público sin vulnerar derechos de los titulares ni la seguridad de la información.

i. Alcance y canal oficial

- Aplica a solicitudes de autoridades judiciales, administrativas o de control con competencia legal.
- Todas las solicitudes se gestionan exclusivamente a través de Jurídica y el Oficial/Líder de Protección de Datos (OPD). Queda prohibida la entrega directa por cualquier otra área o persona.

ii. Verificación de la solicitud

Antes de entregar información, se debe confirmar y documentar:

- Competencia y legitimidad del solicitante (autoridad, número de proceso/actuación, firma digital o sello).
- Fundamento jurídico (norma, orden, oficio, providencia, medida cautelar; en penal, orden de juez o fiscal según aplique).
- Finalidad declarada y alcance de los datos requeridos (fechas, sistemas, personas, periodos).
- Plazo de respuesta y confidencialidad/reserva del expediente.
- Si el requerimiento es internacional, verificar canal MLAT o cooperación válida; de lo contrario, no se entrega de forma directa.
- Si la solicitud es vaga, desproporcionada o carece de soporte, se pedirá aclaración o limitación (principio de mínima revelación).

iii. Principio de mínima revelación

- Se entrega solo lo estrictamente necesario y pertinente a la finalidad informada.
- Se excluyen datos de terceros no involucrados y datos sensibles no indispensables.
- Cuando sea posible, se privilegia la consulta en sitio/ventana de lectura o extracción parcial frente a copias masivas.

iv. Preparación y validación del paquete de información

- Extracción controlada por TI/Seguridad y el custodio de la base, siguiendo listas de verificación.
- Integridad y autenticidad: hash/huella digital, firmas y/o sellado de tiempo.
- Seudonimización/anonimización cuando la autoridad lo acepte y cumpla la finalidad.
- Revisión jurídica-OPD previa a la entrega para validar alcance y riesgos.

v. Entrega segura y cadena de custodia

- Medio de transferencia: canal cifrado (SFTP/VPN/Plataforma segura) o dispositivo cifrado (con contraseña aparte y por canal distinto).
- Registro de cadena de custodia: quién solicita, quién autoriza, qué se entrega, cuándo, cómo y a quién; hash de archivos y recibo.
- Rotulado de confidencialidad y restricciones de uso (p. ej., “Uso exclusivo del expediente X; prohibida su divulgación a terceros”).

vi. Notificación a titulares

- Solo cuando sea legalmente procedente y no comprometa la investigación/actuación.
- Si existe prohibición de informar (p. ej., reserva), se difiere la notificación hasta el levantamiento de la reserva.

vii. Plazos, conservación y bloqueo

- Se cumple el plazo legal indicado por la autoridad; si es insuficiente, se solicita prórroga razonada.
- Se conserva un expediente interno con copia de lo entregado, hashes y constancias.
- Si hay legal hold, la información queda bloqueada de eliminación hasta orden en contrario.

viii. Excepciones, negativas y objeciones

PHYX S.A.S. podrá negar u objetar total o parcialmente la entrega cuando:

- La autoridad no es competente o la solicitud carece de base legal.
- La solicitud es desproporcionada o irrelevante frente a la finalidad.
- Existen límites constitucionales (p. ej., secreto profesional, defensa) o reservas legales superiores.
- Se trate de transferencia internacional directa sin canal válido (MLAT/autoridad colombiana competente).

En estos casos, Jurídica comunicará la decisión motivada y, de ser necesario, propondrá mecanismos alternos (revisión en sitio, datos agregados, disociación).

ix. Roles y responsabilidades

- Jurídica: valida competencia y base legal, define alcance, objeciones y comunicaciones con la autoridad.
- OPD: asegura cumplimiento de principios de protección de datos, minimización y trazabilidad; registra en RC-BD.
- Seguridad/TI: extrae, protege, cifra, verifica integridad y gestiona la cadena de custodia.
- Custodio/Propietario de la base: delimita conjuntos de datos y verifica pertinencia.
- Alta Dirección: conoce requerimientos críticos y aprueba medidas excepcionales si corresponde.

x. Documentación y mejora continua

- Todo requerimiento y su atención se documenta (checklist legal, técnico y de privacidad; actas; logs; hashes).
- Los casos relevantes alimentan lecciones aprendidas y actualizaciones de procedimientos, controles y capacitación.

Cláusula de seguridad: La autoridad receptora es informada de las obligaciones de protección sobre los datos entregados y de los riesgos de uso indebido. PHYX S.A.S. se reserva el derecho de exigir constancia de recibo y de solicitar devolución/destrucción certificada cuando legalmente proceda.

XIX. GESTIÓN DE INCIDENTES DE SEGURIDAD DE INFORMACIÓN

PHYX

PERSONAL

PHYX S.A.S. mantiene un proceso único, coherente y eficaz para gestionar eventos e incidentes que afecten (o puedan afectar) la confidencialidad, integridad, disponibilidad y trazabilidad de los datos personales. Este proceso articula el SGSI, la Continuidad del Negocio, el Programa de Privacidad y los requisitos legales aplicables.

i. Alcance y definiciones

- Evento de seguridad: suceso que puede indicar una falla de control o una condición no deseada (p. ej., alerta de antivirus, intento de acceso no autorizado).
- Incidente de seguridad de información personal: evento o serie de eventos que comprometen o podrían comprometer datos personales (p. ej., acceso no autorizado, pérdida, divulgación indebida, ransomware, envío a destinatario equivocado).
- Aplica a todas las sedes, usuarios, proveedores/encargados y todas las geografías donde PHYX trate datos.

ii. Principios

- Prioridad por riesgo: tratamiento proporcional a la criticidad de la información y al impacto potencial en titulares y negocio.
- Minimización de exposición y evidencia preservada.
- Notificación y transparencia: comunicación oportuna dentro de los plazos legales aplicables y según acuerdos contractuales.
-
- Mejora continua: cada incidente genera lecciones aprendidas y ajustes de control.

iii. Roles y responsabilidades

- Comité de Continuidad del Negocio (CCN): dirección estratégica, priorización y decisión de escalamiento.
- Oficial/Líder de Protección de Datos (OPD): califica incidente de datos personales, verifica obligaciones legales, coordina notificaciones a titulares/autoridad y registro en RC-BD.

- Seguridad de la Información/TI: contención técnica, análisis forense, restauración y hardening posterior.

- Jurídica: base legal, relación con autoridades, objeciones o reservas, redacción de comunicaciones externas.
- Propietario/Custodio de la Base: determina alcance de datos afectados y apoya la remediación.
- Comunicaciones/Relaciones Públicas: mensajes a partes interesadas, cuando corresponda.
- Proveedores/Encargados: reportan sin demora indebida y cooperan según DPA/contrato.

iv. Canales de reporte (obligatorio)

- Correo: gestiondelriesgo@phyx.co y protecciondedatos@phyx.co
- Mesa de servicio/ticketing: categoría “Incidente de datos personales”
- Línea de contingencia: definida en el PCN para fuera de horario
- Todo colaborador/tercero debe reportar de inmediato sospechas o debilidades.

v. Ciclo de vida del incidente (flujo)

a. Detección y registro: creación de ticket con fecha/hora, reportante, sistemas afectados, tipo de datos potencialmente comprometidos.
b. Triagem y clasificación: Leve / Moderado / Grave / Crítico, con base en alcance, tipo de dato (sensible o no), volumen, exposición y probabilidad de afectación a los titulares.
c. Contención inicial: aislamiento de equipos/cuentas, revocación de accesos, bloqueo de exfiltraciones, deshabilitar integraciones comprometidas.
d. Análisis técnico-forense: causa raíz, vector, ventana de exposición, evidencias (logs, imágenes, hashes), datos y titulares impactados.
e. Notificaciones y comunicaciones (si aplican): a titulares y/o autoridades y clientes conforme la ley y los contratos; mensajes claros sobre hechos, riesgos, medidas y canales de soporte.
f. Erradicación y remediación: eliminación de malware/backdoors, parcheo, rotación de credenciales, reconfiguración, corrección de procesos.
g. Recuperación: restauración desde respaldos confiables, validaciones de integridad, pruebas funcionales y de seguridad.
h. Cierre y lecciones aprendidas: acta de cierre, acciones correctivas / preventivas con responsables y fechas, actualización de políticas / controles y capacitación focalizada.

Todos los pasos se documentan y se mantienen evidencias con cadena de custodia.

vi. Criterios de severidad (resumen)

- Leve: sin exposición confirmada; control falló pero no hay impacto en titulares.
- Moderado: exposición limitada, sin datos sensibles; contención rápida.
- Grave: exposición de volumen relevante o datos sensibles, o incumplimiento de plazos procesales.
- Crítico: filtración pública, ransomware con exfiltración, afectación masiva, reincidencia o desatender instrucciones de autoridad.

Las categorías determinan SLA internos para contención, análisis y comunicación, así como la activación del CCN y de ejecutivos de continuidad.

vii. Evidencias y cadena de custodia

- Preservación forense: imágenes, volcados de memoria, registros, correos, configuraciones y artefactos con hashes y sellos de tiempo.
- Acceso restringido y almacenamiento seguro de evidencias.
- Trazabilidad completa de quién accede, cuándo y para qué.

viii. Interacción con autoridades y terceros

- Coordinada por Jurídica y el OPD.
- Notificaciones dentro de los plazos legales aplicables y con contenido requerido.
- Atención de requerimientos (SIC u otras) con información mínima necesaria y controles de transferencia segura.

ix. Integración con Continuidad y proveedores

- PCN/DRP: restauración priorizada según BIA, RTO/RPO; pruebas periódicas.
- Cadena de suministro: cláusulas de reporte de incidentes, derecho de auditoría, subencargos controlados, y evidencias de cierre de acciones correctivas.

x. Métricas y mejora continua

- KPIs/KRIs: tiempo a detección (MTTD), tiempo a contención (MTTC), tiempo a notificación, reincidencias, causas raíz más frecuentes.
- Pruebas y simulacros: ejercicios de mesa y técnicos (al menos anuales) con escenarios de fuga, ransomware, error humano y fallo de tercero.

- Actualizaciones de controles, capacitación y contratos según lecciones aprendidas.

Cláusula final: todo incidente de seguridad de información personal será registrado en el Registro Central de Bases de Datos (RC-BD) y su tratamiento seguirá este procedimiento. La falta de reporte oportuno o el incumplimiento de estas directrices pueden acarrear medidas disciplinarias y acciones contractuales adicionales a las sanciones legales aplicables.

Nota: Para la gestión de incidentes se tienen en cuenta además, las disposiciones descritas en el **Manual de Administración de incidentes.**

XX. CONSIDERACIONES DE LAS AUDITORÍAS DE LOS SISTEMAS DE INFORMACIÓN

PHYX S.A.S. ejecuta auditorías de sistemas de información con enfoque basado en riesgos, buscando evidencia objetiva de cumplimiento, eficacia y mejora continua, minimizando el impacto en la operación.

i. Objetivo y alcance

- Verificar cumplimiento de: normas ISO aplicables (p. ej., ISO/IEC 27001:2022 e ISO 9001:2015), requisitos legales y regulatorios vigentes, contratos con clientes/proveedores, políticas internas y controles del SGSI/SGC.
- Evaluar diseño, implementación y eficacia de controles técnicos, organizacionales y físicos (incluyendo Anexo A de ISO 27001:2022), así como controles de privacidad sobre datos personales.
- Aplica a todas las sedes, procesos, activos, aplicaciones, infraestructuras, terceros/encargados y regiones donde PHYX opere o trate datos.

ii. Tipos de auditoría

- Internas (primera parte): realizadas por auditores competentes e independientes del proceso auditado, conforme al programa anual basado en riesgos.
- Externas (segunda/tercera parte): clientes, organismos de certificación, o entes reguladores.
- Temáticas/técnicas: ciberseguridad, continuidad, desarrollo seguro, gestión de accesos, datos personales, cadena de suministro, cloud/SaaS, OT, etc.

iii. Planificación y coordinación (minimizar impacto)

- Plan anual de auditoría aprobado por la Alta Dirección, con criterios, alcance, métodos y ventanas de auditoría acordadas para evitar periodos críticos.
- Notificación previa de agenda, requerimientos de acceso y evidencias esperadas.
- Uso de ambientes espejo/lectura cuando sea posible; acceso solo-lectura a logs, respaldos o exportaciones controladas para no alterar sistemas productivos.
- Identificación de puntos de contacto (dueños de proceso, custodios de activos) y establecimiento de canales de comunicación.

iv. Ejecución

- Métodos: entrevistas, revisión documental, pruebas de diseño y de efectividad, muestreo estadístico/dirigido, observación directa y, si procede, pruebas técnicas controladas (p. ej., revisión de configuraciones, hardening, escaneos autorizados).
- Evidencias: suficientes, pertinentes y confiables; preservadas con trazabilidad y cadena de custodia cuando sea necesario (no se almacenan datos personales salvo necesidad demostrable y con minimización).
- Reglas de acceso: principio de mínimo privilegio, cuentas de auditoría temporales, registro de accesos y revocación inmediata al cierre.

v. Criterios y clasificación de hallazgos

- Conformidad / Observación / No conformidad menor / No conformidad mayor (afecta cumplimiento legal/contractual o control clave; riesgo alto).
- Cada hallazgo incluye: criterio, condición (evidencia), causa, consecuencia (riesgo) y corrección/correctiva propuesta.

vi. Tratamiento de hallazgos y seguimiento

- Emisión de informe con conclusiones sobre eficacia y eficiencia de los sistemas y controles.
- Planes de acción con responsables, plazos y métricas de cierre; verificación de implementación y eficacia.
- Re-auditorías o verificaciones puntuales cuando se trate de no conformidades mayores o reiteradas.

vii. Auditorías a terceros y cadena de suministro

- PHYX puede auditar o exigir evidencias a encargados/subencargados críticos (p. ej., reportes SOC 2/ISO 27001, pruebas de penetración, resultados de BCP/DRP, evidencia de gestión de incidentes y notificaciones).
- Cláusulas contractuales incluyen derecho de auditoría, tiempos de respuesta y obligaciones de remediación.

viii. Confidencialidad, seguridad y ética

- Los auditores firmarán acuerdos de confidencialidad y cumplirán las políticas de seguridad, privacidad y Conflicto de Interés.
- La información recogida se usa exclusivamente para fines de auditoría; se anonimiza o minimiza cuando incluya datos personales.

ix. Registros y trazabilidad

- Conservación de: programa anual, planes de auditoría, listas de verificación, evidencias, informes, planes de acción y constancias de cierre.
- Los registros se protegen con controles de integridad, acceso y retención definidos.

x. Métricas y mejora continua

- Indicadores: cumplimiento del plan (%), tiempo de cierre de no conformidades, reincidencia, tendencia de causas raíz, y efectividad de acciones.
- Resultados alimentan la Revisión por la Dirección, el plan de mejora del SGSI/SGC y la capacitación focalizada.

Cláusula final: Ninguna actividad de auditoría debe interrumpir injustificadamente los procesos de negocio ni degradar la seguridad. Cualquier prueba intrusiva requerirá autorización formal, plan de contención y supervisión técnica para proteger la operación y los datos.

PHYX

XXI. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN PERSONAL

PHYX S.A.S. integra la seguridad y la protección de datos personales a lo largo de todo el ciclo de vida de sus sistemas de información (planear–construir–probar–desplegar–operar–retirar), incluidos los servicios prestados sobre redes públicas y nubes/híbridos.

i. Gobernanza del ciclo de vida (SDLC) seguro

- Requisitos desde el origen: toda iniciativa tecnológica debe documentar requisitos funcionales y de seguridad/privacidad (confidencialidad, integridad, disponibilidad, trazabilidad, minimización, retención, residencia de datos, transferencias y base legal).
- Evaluación de riesgos y diseño: amenaza y riesgo (threat modeling), clasificación de información, controles por defecto (privacidad desde el diseño y por defecto), cripto, segregación de funciones y principio de mínimo privilegio.
- Gestión de cambios: todo cambio sigue Control de Cambios (plan, evaluación de impacto, ventana, aprobación, reversibilidad/rollback, verificación post-cambio). Cambios urgentes quedan justificados y auditados.
- Configuración y versiones: líneas base seguras (hardening), gestión de configuración (CMDB), versionamiento, Infraestructura como Código (IaC) y revisiones antes de promover ambientes.

ii. Seguridad en adquisición y proveedores

- Debida diligencia: exigencia de certificaciones/evidencias (p. ej., ISO/IEC 27001, reportes SOC, pruebas de contingencia, políticas de privacidad).
- Contratos: anexos de seguridad y acuerdos de tratamiento / transmisión / transferencia con derecho de auditoría, tiempos de notificación de incidentes y obligaciones de remediación.
- Integraciones y APIs: autenticación fuerte, autorización granular, cifrado en tránsito, limitación de tasa, validación de entrada y registros auditables.

iii. Desarrollo seguro de software

- Normas de codificación segura y libros de estilo; revisiones de código por

pares.
- Análisis automático y continuo: SCA/SBOM (componentes y licencias), SAST/DAST/IAST, chequeos de secretos/credenciales y de IaC.
- Gestión de dependencias: origen confiable, control de versiones, parches de seguridad oportunos.
- Gestión de secretos: bóvedas, rotación, nunca embebidos en código.
- Entornos segregados: desarrollo, pruebas, pre-producción y producción separados; accesos diferenciados; datos reales prohibidos en dev/test salvo excepción justificada y aprobada.
- Datos de prueba: preferentemente ficticios o enmascarados/anonimizados; si excepcionalmente se usan reales, se aplican controles equivalentes a producción y registro de autorización.

iv. Pruebas, aceptación y despliegue

- Plan de pruebas: funcionalidad, seguridad, rendimiento, regresión y pruebas específicas de controles de datos personales (consentimiento, derechos ARCO, retención/borrado).
- Validación de plataforma: cuando cambie SO, DB, middleware o nube, se revalida compatibilidad y postura de seguridad.
- Criterios de aceptación: incluyen resultados de seguridad sin hallazgos críticos/altos pendientes y plan de remediación para medios/bajos.
- Despliegues controlados: CI/CD con aprobaciones, firmas de artefactos, segregación de llaves y rollback probado.

v. Protección de transacciones y comunicaciones

- Cifrado en tránsito: TLS vigente (y mTLS cuando aplique), deshabilitar algoritmos inseguros.
- Integridad y no repudio: firmas digitales y sellado de tiempo donde sea requerido.
- Controles de aplicación: validación de entradas/salidas, protección anti-CSRF/XSS/SQLi, cabeceras seguras, gestión de sesión y caducidad.

vi. Operación, mantenimiento y vulnerabilidades

- Parcheo: inventario, priorización por criticidad, ventanas de mantenimiento y verificación post-parche.
- Endurecimiento continuo: escaneo de configuración, cierre de puertos/servicios innecesarios.
- Monitoreo y logging: registros de seguridad con inmutabilidad/retención

definida; correlación de eventos; alertas ante accesos anómalos y exfiltración.
- Gestión de vulnerabilidades: escaneos programados y bajo demanda; pruebas de penetración periódicas para activos críticos; remediación según SLA.
- Backups y recuperación: copias cifradas, pruebas de restauración, RTO/RPO alineados al BIA; segregación lógica/física de respaldos.

vii. Datos personales: salvaguardas específicas

- Cifrado en reposo para datos personales y claves gestionadas (HSM/KMS) con rotación.
- Retención y eliminación: reglas por tipo de dato y finalidad; borrado seguro y evidencias de destrucción.
- Acceso: controles RBAC/ABAC, registros de acceso a datos personales y revisiones periódicas de permisos.
- Residencia y transferencias: cumplimiento de país adecuado o mecanismos contractuales; registro en RNBD cuando corresponda.

viii. Desarrollo tercerizado y SaaS/PaaS/IaaS

- Autorización previa para subencargos; obligaciones equivalentes de seguridad / privacidad.
- Seguridad compartida en nube: configuración responsable por PHYX (identidades, redes, cifrado, copias, llaves) y verificación de controles del proveedor.

ix. Retiro y disposición de sistemas

- Plan de descomisionamiento: inventario de datos/activos, exportación cuando aplique, borrado/anonimización verificada, revocación de accesos, revocación de certificados/claves y actualización de CMDB/RNBD.

x. Documentación y evidencia

- Requisitos, diseños, evaluaciones de riesgo, resultados de pruebas, aprobaciones de cambios, manuales de operación, bitácoras de despliegue, evidencias de controles y matrices de trazabilidad se conservan conforme política de retención y están disponibles para auditoría.

Cláusula de cumplimiento: Ningún sistema que trate datos personales será

promovido a producción sin validación de seguridad y sin cumplir los requisitos aquí descritos. El incumplimiento puede acarrear bloqueo del despliegue, acciones disciplinarias/contractuales y demás medidas previstas en la Política.

XXII. VIGENCIA

i. **Vigencia de las bases de datos**. Cada base de datos tendrá una vigencia igual al período en que subsista la finalidad que justificó su tratamiento o al plazo que determine una causa legal, contractual o jurisprudencial específica. Al extinguirse la finalidad o cumplirse el plazo, se aplicarán las reglas de conservación, bloqueo y eliminación segura definidas por PHYX S.A.S. y la normatividad aplicable.

ii. **Vigencia de la Política.** Esta Política entra en vigor a partir de su aprobación y deroga todas las versiones anteriores. Será revisada al menos una vez al año o cuando se presenten cambios sustanciales (p. ej., modificaciones regulatorias, nuevas regiones de operación, incorporación de tecnologías / plataformas, variaciones en el modelo de tratamiento o en el nivel de riesgo).

iii. **Aprobación y control documental.**

- Órgano aprobador: Gerencia General de PHYX S.A.S.
- Propietario del documento: Líder de Protección de Datos / Responsable del SGI.
- Fecha de aprobación de la versión vigente: febrero de 2025.
- Próxima revisión programada: febrero de 2026 (o antes si ocurren cambios relevantes).

iv. **Publicación y comunicación.** La versión vigente será publicada en los canales internos y, cuando corresponda, en los canales externos (p. ej., sitio web/avisos de privacidad), garantizando su accesibilidad para titulares, clientes, proveedores, aliados y autoridades.

v. **Alcance territorial.** La Política es aplicable a todas las operaciones y regiones donde PHYX S.A.S. trate datos personales (incluidas filiales, sucursales y encargados/subencargados), y sus traducciones deberán mantener equivalencia jurídica con esta versión en español.

vi. **Registro y actualización ante autoridades.** Las altas, modificaciones o cancelaciones de bases de datos y de sus finalidades serán registradas/actualizadas oportunamente en el RNBD u otros registros

exigidos por las autoridades competentes, según corresponda.

vii. **Trazabilidad de cambios.** Toda modificación de esta Política se incorporará en la "Referencia de Cambios" con número de versión, fecha, secciones afectadas y motivo del ajuste. La compañía conservará el histórico de versiones conforme a su procedimiento de control documental.

XXIII. REFERENCIA DE CAMBIOS:

Cuando se realicen cambios a esta Política, los últimos cinco cambios o modificaciones se deben referenciar por el encargado de calidad utilizando la tabla de referencia de cambios; los cambios o modificaciones deben estar aprobados por la Gerencia General.

Tabla: Referencia de Cambios

MODIFICACIÓN NO.	DÍA	MES	AÑO	SECCIÓN(ES)	OBSERVACIONES
1	24	06	2026	Todas	Emisión del documento.

ETIQUETA SEGURIDAD DE LA INFORMACIÓN	
ELEMENTO	**DETALLE**
Clasificación	CONFIDENCIAL
Proceso	SGI – Protección de Datos Personales
Responsable del documento	Oficial de seguridad de la información, continuidad del negocio y PDP
Uso Autorizado	Uso interno y externo controlado. Documento marco divulgado a Titulares y Autoridades. Uso interno obligatorio para Alta Dirección, Jurídica, Talento Humano, TI, Seguridad de la Información y otros procesos.
Dimensión CID	C – I – D (Confidencialidad Alta / Integridad Alta / Disponibilidad Media-Alta)
Responsable del etiquetado	Líder SGI / Oficial de Seguridad de la Información, continuidad y PDP

APROBÓ
PHYX S.A.S.
NIT. 900939751-9