ANEXO I

REGLAMENTO DE ESTÁNDARES TÉCNICO-JURÍDICOS PARA LA OPERACIÓN EN EL ECOSISTEMA PREVENCIÓN 4.0.

CAPÍTULO I

PRINCIPIOS TRANSVERSALES SOBRE EL FUNCIONAMIENTO DEL ECOSISTEMA PREVENCIÓN 4.0.

Las pautas técnicas establecidas en el presente Capítulo deberán interpretarse de manera integral y sistémica, en tanto todas ellas responden a principios comunes de confiabilidad, trazabilidad, verificabilidad y gobernanza responsable de la información digital generada en el marco del Ecosistema Prevención 4.0. (EP4.0).

Los estándares relativos a almacenamiento, trazabilidad, disponibilidad, portabilidad, accesibilidad, omnicanalidad, interoperabilidad, auditoría, validación automática, tratamiento de datos biométricos y certificación no constituyen exigencias autónomas, sino componentes interrelacionados de un mismo sistema normativo y tecnológico orientado a asegurar la producción de información jurídicamente válida y administrativamente controlable.

Desde una perspectiva sistémica, el EP4.0 se configura como un conjunto organizado de actores, procesos, datos y tecnologías que interactúan mediante flujos continuos de

información. Cada pauta cumple una función específica -preservar, reconstruir, acceder, contrastar, auditar o validar datos-, pero su eficacia depende de su articulación con las restantes. La debilidad o ausencia de uno de estos componentes puede comprometer la confiabilidad del conjunto.

El funcionamiento del sistema se sustenta en la interdependencia funcional y en mecanismos de retroalimentación continua que permiten detectar desvíos, corregir inconsistencias y sostener la coherencia interna del ecosistema. En tal sentido, la confiabilidad no deriva de una herramienta tecnológica determinada, sino del diseño estructural que integra controles, responsabilidades y mecanismos de verificación.

La concurrencia funcional de los estándares previstos constituye el presupuesto necesario para asegurar el valor probatorio de los registros digitales generados dentro del EP4.0.

CAPÍTULO II

ESTÁNDARES REQUERIDOS PARA LA GESTIÓN DE LA INFORMACIÓN EN EL ECOSISTEMA PREVENCIÓN 4.0.

1. ALMACENAMIENTO

a. Finalidad y valor probatorio

ANEXO I

El almacenamiento de la información generada en el marco del EP4.0 deberá asegurar la preservación íntegra, confidencial y disponible de los datos y registros digitales vinculados al cumplimiento de obligaciones emergentes del Sistema de Riesgos del Trabajo, de modo tal que dichos registros puedan ser utilizados como medio probatorio válido en actuaciones administrativas o en cualquier instancia de control o fiscalización.

b. Políticas de gestión y continuidad operativa

Los prestadores de soluciones tecnológicas deberán implementar políticas formales de gestión de la información que contemplen procedimientos documentados de almacenamiento, respaldo, recuperación y eliminación segura de datos, garantizando que la información relevante pueda ser reconstruida incluso ante contingencias técnicas, fallas operativas o discontinuidad de servicios tecnológicos utilizados.

c. Infraestructura y servicios de terceros

El almacenamiento podrá efectuarse mediante infraestructura tecnológica propia o a través de servicios contratados a terceros, siempre que tales servicios cuenten con respaldo contractual verificable, condiciones adecuadas de continuidad operativa y mecanismos que permitan la recuperación o migración de información ante la finalización o interrupción de dichos servicios.

d. Gobernanza y plazos de conservación

ANEXO I

La gobernanza de datos deberá contemplar la determinación de plazos de conservación acordes a la normativa vigente y la implementación de procedimientos que aseguren la preservación de datos mientras subsistan obligaciones legales o potenciales responsabilidades derivadas de los hechos registrados.

e. Acreditación y auditoría de procesos

Los prestadores deberán poder acreditar ante auditores externos o autoridades competentes la existencia de políticas y procedimientos efectivos de almacenamiento, pudiendo requerirse contratos de servicios tecnológicos, manuales operativos y/o evidencia de pruebas de recuperación de información.

f. Consecuencias de la deficiencia en el almacenamiento

La ausencia de los mecanismos de almacenamiento y recuperación detallados en el presente Anexo podrá afectar la confiabilidad administrativa de los registros digitales generados, pudiendo motivar requerimientos de adecuación por parte de la autoridad competente como condición para continuar operando como prestador en el EP4.0.

2. TRAZABILIDAD Y CADENA DE CUSTODIA

a. Garantía de reconstrucción de procesos

ANEXO I

Las soluciones tecnológicas utilizadas deberán garantizar la trazabilidad de los procesos, operaciones y registros generados dentro del EP4.0, permitiendo reconstruir en forma verificable la secuencia de acciones que dieron origen a cada dato, documento o actuación administrativa almacenada.

b. Identificación de origen e intervenciones

La trazabilidad constituye un elemento esencial para conferir valor probatorio a los registros digitales, debiendo los sistemas permitir identificar el origen de la información, las intervenciones humanas o automatizadas realizadas y las modificaciones efectuadas a lo largo del tiempo.

c. Integridad y cadena de custodia

En particular, deberá preservarse una cadena de custodia digital verificable que asegure que los registros no hayan sido alterados desde su generación, permitiendo demostrar su autenticidad e integridad ante requerimientos administrativos o judiciales.

d. Protocolos de acceso y responsabilidad

La gobernanza de datos deberá contemplar la definición de responsables de custodia de la información y establecer protocolos para la generación, modificación y acceso a registros, asignando responsabilidades respecto de las intervenciones permitidas sobre la información y

manteniendo siempre los registros originales inalterados respecto de cualquier operación realizada.

e. Verificación del historial de actuaciones

Los prestadores deberán poder demostrar la existencia de mecanismos que permitan reconstruir el historial de actuaciones realizadas, pudiendo el auditor externo requerir evidencia operativa que permita verificar la continuidad y consistencia de los registros digitales.

f. Medidas correctivas ante falta de trazabilidad

La inexistencia o insuficiencia de mecanismos de trazabilidad podrá afectar la confiabilidad administrativa de la información generada, debiendo adoptarse medidas correctivas cuando tales deficiencias sean detectadas, pudiendo motivar requerimientos de adecuación por parte de la autoridad competente como condición para continuar operando como prestador en el EP4.0.

3. PORTABILIDAD

a. Transferencia de información

Las soluciones tecnológicas implementadas deberán garantizar la portabilidad de los datos generados dentro del EP4.0, permitiendo a los responsables o titulares de la información recuperar y transferir sus datos a otros sistemas sin impedimentos técnicos o contractuales indebidos.

ANEXO I

b. Formatos y reutilización

Los operadores deberán implementar mecanismos que permitan exportar información en formatos estructurados o no estructurados, de modo total o parcial, posibilitando su reutilización inmediata por terceros autorizados.

c. Migración sin alteración de registros

La gobernanza de datos deberá contemplar procedimientos de migración y transferencia de información ante cambios tecnológicos, garantizando que tales procesos no impliquen pérdida, alteración o inaccesibilidad de registros relevantes.

d. Evidencia de capacidad de exportación

El auditor externo podrá requerir evidencia de la existencia de mecanismos efectivos de exportación y recuperación de información, pudiendo verificarse la posibilidad real de migración sin afectar la integridad ni el valor probatorio de los datos.

4. DISPONIBILIDAD

a. Acceso permanente para control y evidencia

La información generada dentro del EP4.0 deberá encontrarse disponible para usuarios autorizados y Organismos de control durante todo el período en que subsistan obligaciones

legales o administrativas vinculadas a su conservación o eventual utilización como evidencia del cumplimiento normativo.

b. Planes de contingencia y recuperación

Los operadores deberán garantizar políticas y procedimientos de continuidad operativa, con gestión de datos que contemplen la existencia de múltiples copias en simultáneo (nube) y/o respaldos periódicos con planes de recuperación ante incidentes. Los mecanismos que permitan restablecer el acceso a la información deberán realizarse en plazos razonables frente a fallas técnicas o contingencias no previstas.

c. Acreditación por medios alternativos

En aquellos supuestos en que la información no pudiera encontrarse disponible de manera inmediata, el responsable deberá poder acreditar el cumplimiento de sus obligaciones mediante medios alternativos verificables, contratos de servicios como respaldo, certificados, registros de actividad o documentación equivalente.

d. Facultades del auditor externo

El auditor externo podrá requerir evidencia de la existencia de políticas de respaldo y pruebas de recuperación de información, verificando la capacidad operativa de restauración de datos relevantes.

e. Impacto de la indisponibilidad

La indisponibilidad recurrente de la información será considerada un factor de merma de confiabilidad administrativa de los registros generados dentro del sistema, pudiendo dar lugar a requerimientos de adecuación y en su caso la adopción de medidas en el marco de las facultades de supervisión y control del organismo.

5. ACCESIBILIDAD

a. Estándares de accesibilidad técnica

Las plataformas y servicios digitales utilizados deberán cumplir estándares reconocidos de accesibilidad, permitiendo que los distintos actores autorizados del EP4.0 puedan acceder a la información necesaria para verificar el cumplimiento de obligaciones legales y operativas.

b. Acceso remoto

En el marco del EP4.0. la accesibilidad supone la existencia de medios de acceso remoto a la información, asegurando que empleadores, trabajadores y organismos de control puedan realizar consultas sin obstáculos técnicos indebidos. Los accesos presenciales podrán sustituir a los accesos remotos solamente en casos de dificultad técnica insalvable.

c. Protección de datos

ANEXO I

Los mecanismos de acceso a información deberán garantizar la protección de datos personales y sensibles.

d. Perfiles de usuario y autenticación

La gobernanza de datos deberá definir políticas de acceso que contemplen perfiles autorizados y mecanismos de autenticación adecuados, resguardando la confidencialidad de la información.

e. Funcionalidad

Los proveedores de soluciones 4.0. deben garantizar que la información sea siempre accesible. Para ello, ofrecerán herramientas que funcionen de manera independiente o integrada en sus plataformas, eligiendo siempre la opción técnica que mejor facilite el uso y la consulta de los datos.

f. Obstrucción de la capacidad de control

La falta de accesibilidad por parte del órgano de control afectará la capacidad de supervisión y verificación administrativa del sistema implementado, pudiendo ser causal de exclusión del prestador de soluciones 4.0. como integrante del Ecosistema.

6. OMNICANALIDAD

a. Diversidad de canales de interacción

ANEXO I

Los operadores del EP4.0 deberán prever múltiples canales de interacción entre usuarios, prestadores y Organismos de control, permitiendo realizar trámites, consultas e intercambios de información por diversas vías tecnológicas o presenciales.

b. Coherencia e integridad de la información multicanal

La estrategia omnicanal deberá asegurar que la información gestionada por cada canal no posea inconsistencias o contradicciones que puedan afectar el valor probatorio de los registros generados.

c. Documentación de canales e integración

Los prestadores deberán documentar los canales disponibles y los procedimientos de integración de información, pudiendo el auditor externo verificar la consistencia de registros gestionados por distintos medios de interacción.

7. INTEROPERABILIDAD

a. Objetivo

Las herramientas y soluciones tecnológicas implementadas deberán prever la capacidad de interoperar con otros sistemas, en especial los sistemas públicos exigibles derivados del cumplimiento de obligaciones e imposiciones normativas.

ANEXO I

b. Eficiencia en la gestión de datos

La interoperabilidad deberá entenderse como la posibilidad efectiva de interactuar de manera segura y verificable entre sistemas distintos, evitando la duplicación innecesaria de registros o la generación de inconsistencias.

c. Fortalecimiento de la confiabilidad probatoria

Desde la perspectiva probatoria, la interoperabilidad constituye un elemento que fortalece la confiabilidad de los registros digitales, en tanto permite corroborar la consistencia de la información mediante la integración entre registros con bases propias, externas y/o registros oficiales.

d. Escalabilidad

Los prestadores deberán prever que las herramientas implementadas puedan incorporar nuevas integraciones sin necesidad de rediseños estructurales que impidan la continuidad operativa del servicio.

e. Verificación de la interoperabilidad

El auditor externo o certificador 4.0. podrá verificar la existencia de procesos y mecanismos que permitan la interoperabilidad efectiva de datos e información, requiriendo evidencia práctica de integraciones activas o protocolos documentados, sin exigir estándares tecnológicos específicos.

ANEXO I

8. AUDITORÍA Y VERIFICABILIDAD

a. Acceso para órganos de control

Las herramientas tecnológicas deberán permitir la auditoría integral de la información y de los procesos digitales, garantizando a los órganos de control y auditores externos el acceso seguro y verificable a los registros necesarios.

b. Registros de actividad, marcas temporales y gestión de capas

A tales efectos, los sistemas deberán conservar registros de actividad (*logs*) que permitan identificar acciones, marcas temporales, intervinientes y resultados obtenidos en cada actuación relevante. También se deberán contar con capas de información según se trate de la información en fuente o los diversos usos o accesos a la misma.

c. Gestión de perfiles de auditoría

La gobernanza de datos deberá contemplar políticas claras de conservación y acceso a registros de auditoría, definiendo perfiles autorizados y mecanismos que preserven la confidencialidad sin impedir la verificación.

d. Protección contra alteraciones posteriores

La posibilidad de auditar los sistemas es requisito esencial para el valor probatorio. Los registros auditables deben estar protegidos contra alteraciones y ser verificables en cualquier

instancia. La gestión de información por capas deberá blindar la inalterabilidad de los datos en la fuente.

e. Documentación de control interno

Los prestadores deberán documentar procedimientos internos que aseguren la disponibilidad de información auditada, incluyendo manuales operativos y registros de auditorías previas, según las prácticas más económicas y eficaces en el uso del tiempo.

f. Acceso a entornos de prueba y mejora continua

El auditor externo podrá requerir acceso a entornos de prueba o evidencia operativa para verificar la consistencia, pudiendo recomendar mejoras para fortalecer la transparencia.

9. AUTOCONTROL

a. Mecanismos de detección de errores

Las soluciones tecnológicas deberán incorporar mecanismos de validación automática y control interno que permitan detectar inconsistencias o desvíos respecto de las obligaciones legales y las mejores prácticas.

b. Monitoreo continuo y alertas tempranas

Tales mecanismos deberán permitir el monitoreo de indicadores de cumplimiento, generando alertas que posibiliten medidas correctivas antes de que los incumplimientos produzcan efectos jurídicos.

c. Supervisión de validaciones y alertas

La gobernanza de datos deberá contemplar la supervisión periódica de estos mecanismos, asignando responsables para la revisión de alertas y adopción de acciones correctivas.

d. Documentación de procesos de autocontrol

Los prestadores deberán documentar los procesos de autocontrol, pudiendo el auditor externo requerir evidencia del funcionamiento de alertas y medidas adoptadas.

10. TRATAMIENTO DE DATOS BIOMÉTRICOS

a. Sujeción a normativa de protección de datos

El uso de datos biométricos deberá ajustarse estrictamente a la normativa de protección de datos personales.

b. Principio de proporcionalidad y necesidad

La utilización de tales datos deberá estar justificada en relación con la finalidad, evitando su recolección cuando existan medios menos invasivos para cumplir la misma función.

c. Consentimiento informado

En cada caso, deberá contarse con consentimiento informado, garantizando los derechos de acceso, rectificación, cancelación y oposición, conforme a las normas aplicables.

d. Protocolos de recolección y eliminación

La gobernanza de datos establecerá protocolos específicos para la recolección y eliminación segura, definiendo responsables internos para minimizar riesgos de acceso no autorizado.

e. Sanción por uso desproporcionado

El uso indebido de datos biométricos afectará la confiabilidad administrativa de los sistemas y se considerará una violación a los principios de protección de datos, pudiendo dar lugar a requerimientos de adecuación y en caso de incumplimiento, a la adopción de medidas en el marco de las facultades de supervisión y control del organismo.

11. CERTIFICACIONES DE CUMPLIMIENTO TÉCNICO Y ORGANIZATIVO

Conforme las previsiones de la Resolución de esta SUPERINTENDENCIA DE RIESGOS DEL TRABAJO (S.R.T.) N° 48 de fecha 31 de octubre de 2025, el cumplimiento por parte de los prestadores de soluciones 4.0. de los estándares establecidos en dicho cuerpo normativo y en el presente Anexo, será acreditado mediante la obtención de certificaciones de cumplimiento técnico y organizativo.

ANEXO I

La certificación no sustituye las facultades de control estatal ni exime de responsabilidad por incumplimientos detectados con posterioridad.

CAPÍTULO III

PRESTADORES DE SOLUCIONES 4.0.

En esta sección se reglamentan aspectos operativos asociados al proceder de los Prestadores de Soluciones 4.0. consignados en la Resolución S.R.T. N° 48/25 como sujetos del EP4.0.

En virtud de dicha norma, los prestadores de soluciones 4.0. pueden ser entidades, empresas o áreas de empresas, especializadas en el desarrollo y/o implementación de soluciones tecnológicas avanzadas, caracterizados según el alcance de sus servicios, pudiendo brindarlos dentro de sus organizaciones y/o a para terceros, conforme las siguientes pautas:

I. Prestadores Integrales de Soluciones 4.0.: Empresas o entidades especializadas en la comercialización e implementación de soluciones tecnológicas 4.0. para terceros que se acrediten e inscriban como tales en el EP4.0.
II. Prestadores de Autogestión 4.0.: Empresas que diseñan e implementan soluciones 4.0. exclusivamente para su uso interno, debiendo acreditar e inscribir sus circuitos en el EP4.0.

ANEXO I

III. Prestadores 4.0. eventuales - Aseguradoras de Riesgos del Trabajo (A.R.T.): Las A.R.T. podrán actuar como prestadores eventuales de soluciones 4.0. para los empleadores alcanzados por su cobertura, como parte de sus planes de gestión, debiendo para ello acreditarse e inscribirse en el EP4.0.

CAPÍTULO IV

REGISTRO DE PRESTADORES DE SOLUCIONES 4.0.

I. Objetivo

La inscripción en el REGISTRO DE PRESTADORES DE SOLUCIONES 4.0. (RPS) tendrá por finalidad la organización, identificación y supervisión de los actores del Ecosistema Prevención 4.0. en el marco de la Resolución S.R.T. Nº 48/25.

II. Solicitud y clasificación

Los prestadores solicitarán su incorporación al Registro de Prestadores de Soluciones 4.0., en adelante "RPS", indicando su categoría operativa: Prestador Integral, Prestador de Autogestión 4.0. o Prestador 4.0. eventual-ART.

En dicha solicitud deberán declarar el alcance de sus servicios, especificando si se trata de soluciones genéricas o especializadas.

ANEXO I

III. Acreditación de idoneidad

Los prestadores de soluciones 4.0. acreditarán su capacidad técnica mediante la demostración de un marco de gestión de riesgos tecnológicos y seguridad de la información acorde a la complejidad de la tecnología empleada. En el caso de los Prestadores de Autogestión, la acreditación se enfocará en la interoperabilidad de sus sistemas internos con el EP4.0, asegurando que la información sea accesible para los órganos de control.

IV. Presentación de documentación y responsables

Los prestadores de soluciones 4.0. presentarán la designación formal de un Responsable de Estándares, en los términos del artículo 5° de la Resolución S.R.T. N° 48/25 o la norma que la complemente o modifique en el futuro.

V. Control y auditoría

Los prestadores de soluciones 4.0. se someterán a los mecanismos de auditoría integral, facilitando el acceso a registros de eventos, marcas de tiempo e historiales de actividad inalterables. Asimismo, deberán permitir auditorías externas cuando la autoridad lo considere necesario para verificar la integridad de la cadena de custodia digital.

VI. Registro y vigencia

Los prestadores de soluciones 4.0. obtendrán registros temporarios, provisorios y/o definitivos en el “RPS” para su operación en el EP4.0, conforme a las certificaciones técnicas acreditadas.

ANEXO I

a. Registro temporario: Se otorgará a los prestadores que ingresen al EP4.0.

Este registro permitirá el inicio de operaciones por un plazo máximo de UN (1) año calendario desde su inscripción.

A tal efecto, deberán presentar una Declaración Jurada que contenga:

- El detalle de las soluciones tecnológicas a implementar y
- El compromiso formal de adecuación a los estándares técnicos establecidos en la normativa vigente.

b. Registro provisorio: Se otorgará a los prestadores que cumplan con el núcleo mínimo de estándares exigidos, a saber: almacenamiento, trazabilidad y portabilidad. Tendrá una duración de UN (1) año calendario desde el momento de la inscripción, prorrogable mediante la presentación de una declaración jurada de mantenimiento de condiciones hasta TREINTA (30) días previos al vencimiento del plazo.

c. Registro definitivo: Se otorgará a los prestadores que demuestren la plena satisfacción de los estándares establecidos en la Resolución S.R.T. N° 48/25 y en la presente disposición, o en las normas que eventualmente establezca la autoridad competente, mediante la acreditación de las certificaciones que correspondan a la prestación brindada.

ANEXO I

VII. Alcances

En función de lo consignado en el artículo 2° de la presente disposición, la información generada a partir del empleo de soluciones tecnológicas ofrecidas por prestadores 4.0. con registro provisorio y definitivo tendrán valor probatorio *per se*, en atención a las certificaciones oportunamente acreditadas.

VIII. Supervisión y cancelación

La inscripción en el Registro no limita las facultades de supervisión de la S.R.T., la que podrá requerir información, formular observaciones y, en caso de incumplimientos graves o reiterados que afecten la confiabilidad del sistema, disponer la suspensión o cancelación de la inscripción conforme los procedimientos aplicables.

CAPÍTULO V

CERTIFICADORES 4.0.

En esta sección se reglamentan aspectos operativos asociados al proceder de los Certificadores 4.0. consignados en la Resolución S.R.T. N° 48/25 como actores del EP4.0.

a. Demostración de calidad y seguridad

La certificación es el medio idóneo para demostrar que los sistemas cumplen estándares de calidad y seguridad, facilitando la incorporación ordenada al EP4.0.

ANEXO I

b. Actualización periódica de certificados

La gobernanza de datos debe contemplar la actualización periódica de las certificaciones para asegurar que las condiciones verificadas se mantengan vigentes.

c. Evaluación de correspondencia operativa

Auditores externos podrán verificar la autenticidad de las certificaciones y evaluar si la operación real del sistema se corresponde con lo certificado.

d. Pérdida de vigencia y requerimientos de adecuación

La pérdida o vencimiento de certificaciones relevantes podrá motivar revisiones por parte de la autoridad competente y motivar requerimientos de adecuación a la normativa vigente.

CAPÍTULO VI

REGISTRO DE CERTIFICADORES 4.0.

I. Naturaleza del registro

El Registro de Certificadores 4.0. (RC) es de carácter público y declarativo, destinado a identificar a las entidades que deseen emitir las certificaciones relativas al cumplimiento de los estándares técnicos establecidos para el EP4.0.

ANEXO I

La inscripción en el RC no tendrá carácter constitutivo de la actividad certificadora, en tanto se trata de entidades preexistentes que desarrollan su actividad conforme su propio marco jurídico y técnico, limitándose la S.R.T. a su anotación y publicidad administrativa en el marco del Sistema de Riesgos del Trabajo.

II. Inscripción

Las entidades que deseen inscribirse como Certificadores 4.0. en el EP4.0 deberán solicitar su inscripción ante la Superintendencia de Riesgos del Trabajo (S.R.T.) acompañando:

a) Documentación que acredite su personería jurídica y vigencia;
b) Declaración del alcance de las certificaciones que emitirán en el marco del EP4.0.
c) Antecedentes o experiencia de la entidad y/o de los equipos de trabajo asignados para llevar adelante las tareas de certificación técnica o evaluación de estándares de gestión o tecnológicos.
d) Declaración jurada de independencia respecto de los prestadores a los que certifiquen y compromiso de facilitar a la S.R.T., cuando ésta lo requiera, la información necesaria para verificar la autenticidad y alcance de las certificaciones expedidas.

La responsabilidad por el contenido técnico de las certificaciones emitidas recaerá exclusivamente en el certificador.

ANEXO I

La inscripción en el RC no implicará validación técnica previa ni posterior de sus procedimientos internos.

República Argentina - Poder Ejecutivo Nacional
Año de la Grandeza Argentina

Hoja Adicional de Firmas
Anexo Disposición

Número: DI-2026-45957783-APN-GG#SRT

CIUDAD DE BUENOS AIRES
Jueves 7 de Mayo de 2026

Referencia: ANEXO I - REGLAMENTO DE ESTÁNDERES TÉCNICO-JURÍDICOS PARA LA OPERACIÓN EN EL ECOSISTEMA PREVENCIÓN 4.0. - Expediente EX-2025-115601290-APN-SITAP#SRT

El documento fue importado por el sistema GEDO con un total de 24 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2026.05.07 16:09:22 -03:00

Fernando Gabriel Perez
Gerente General
Gerencia General
Superintendencia de Riesgos del Trabajo

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2026.05.07 16:09:23 -03:00