

AVISO DE PRIVACIDAD INTEGRAL

MONITOREO DE SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS DEL INSTITUTO REGISTRAL Y CATASTRAL DEL ESTADO DE NUEVO LEÓN

En atención a lo dispuesto por los artículos 3 fracción II, 27, 28 y demás relativos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, se pone a su disposición el siguiente aviso de privacidad en los siguientes términos:

I.- Denominación y domicilio del responsable.

La Dirección de Información del Instituto Registral y Catastral del Estado de Nuevo León, en adelante LA DIRECCIÓN, es la responsable del tratamiento de los datos personales que se generen y requieran para el monitoreo de seguridad de los sistemas informáticos del Instituto. LA DIRECCIÓN es responsable de resguardarlos y mantenerlos en estricta confidencialidad, con las salvedades previstas en el artículo 23 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León (en adelante, LPDPPSO-NL). Tiene su domicilio en el Pabellón Ciudadano, Washington 2000 Oriente, colonia Obrera, Monterrey, Nuevo León, C.P. 64010.

II.- A quién aplica.

Este aviso aplica a dos grupos de personas titulares:

- a) **Personal con acceso:** servidores públicos, prestadores de servicios y proveedores que acceden con una cuenta a los servidores, bases de datos, aplicaciones y equipos de red del Instituto.
- b) **Personas usuarias de los portales:** ciudadanos y cualquier persona que visite o utilice los sitios y servicios web del Instituto.

III.- Datos personales que se tratan.

Los datos se registran de forma automática por los sistemas del Instituto. No se recaban datos personales sensibles.

a) *Del personal con acceso:*

- **Identificación:** nombre de la cuenta de usuario y, a través del inventario de cuentas, el nombre de la persona a la que está asignada; nombre del equipo desde el que se conecta. El nombre de un servidor público, en lo que se refiere al ejercicio de sus funciones, se rige por el principio de máxima publicidad; los registros de actividad asociados a su cuenta no son públicos y se tratan conforme a este aviso.



- **Laborales:** área y puesto asociados a la cuenta. Por tratarse de designaciones que el propio Instituto establece para el desempeño del empleo, cargo o comisión, son información de libre acceso.
- **Actividad en sistemas:** dirección IP de origen; fecha y hora de inicio y fin de sesión; intentos de acceso fallidos; uso de privilegios administrativos; altas, bajas y cambios de cuentas y grupos; servicios y tareas programadas creados o modificados; cambios de configuración; huella de las llaves de acceso utilizadas; conexiones a bases de datos (cuenta, base, IP y aplicación) y cambios de roles o de estructura de las bases; conexión de memorias USB y discos externos a los servidores. La dirección IP permite identificar de manera indirecta el dispositivo y a la persona que lo utiliza en un momento determinado, aunque provenga de la red del Instituto; por ello se trata como dato personal y no se difunde, ya que su difusión desagregada podría comprometer la seguridad de los sistemas o la privacidad de la ubicación del personal.
- **Comandos y procesos:** nombre del programa ejecutado y del programa que lo inició. **Los comandos con sus argumentos** (sistemas Linux) y **la línea de comandos de los procesos** (sistemas Windows) **solo se registrarán a partir de la publicación de este aviso**, enmascarados en el propio servidor antes de salir de él y truncados a una longitud máxima. Los comandos y programas son herramientas y activos tecnológicos del Instituto, no atributos de la persona que los utiliza; sin embargo, al quedar registrados junto con la cuenta de una persona, forman parte de sus datos personales y se tratan conforme a este aviso.

b) De las personas usuarias de los portales:

- **Dirección IP** desde la que se visita el portal, fecha y hora, método, ruta de la página **sin los valores que se capturan en formularios o en la dirección**, código de respuesta, tamaño y tiempo de respuesta, y tipo de navegador de forma abreviada. Una dirección IP aislada corresponde a un dispositivo y no directamente a una persona; se trata como dato personal porque puede vincularse con una persona determinada.
- Si la ruta contiene una CURP, un RFC, un folio o un correo electrónico, se enmascara antes de guardarse.

Lo que no se recaba: contenido de pantallas, pulsaciones de teclado, comunicaciones personales, navegación en internet del personal, **texto de las consultas a las bases de datos, valores de parámetros o formularios, cookies, página de procedencia (Referer)**, ni contraseñas. Si un nombre de usuario inexistente se escribe al intentar entrar, se guarda transformado de forma irreversible mediante una función criptográfica con clave, porque con frecuencia es una contraseña o un nombre escrito por error.

IV.- Fundamento.

El tratamiento se realiza en cumplimiento de las atribuciones y facultades conferidas por la Ley del Instituto Registral y Catastral del Estado de Nuevo León, artículo 23, fracciones V y XXIV, y demás relativos, y está justificado por finalidades concretas, lícitas, explícitas y legítimas, de conformidad con los artículos 16 y 17 de la LPDPPSO-NL. Se realiza además en cumplimiento del deber de establecer y mantener medidas de seguridad administrativas, físicas y técnicas para proteger los datos personales que el Instituto trata en sus sistemas registrales y catastrales, previsto en el artículo 36 de la LPDPPSO-NL.

V.- Finalidades.

Los datos personales se utilizarán **únicamente** para las siguientes finalidades, todas necesarias para cumplir las atribuciones del Instituto:

Finalidades primarias:

- Proteger la confidencialidad, integridad y disponibilidad de la información registral y catastral que resguardan los sistemas del Instituto.
- Detectar, investigar, contener y documentar incidentes de seguridad, ataques y accesos no autorizados, incluso correlacionando eventos de distintos servidores.
- Bloquear de forma automática y temporal, en el portal web, las direcciones IP que realizan intentos repetidos de acceso por fuerza bruta.
- Identificar qué cuenta realizó un cambio en un sistema, para atribuir responsabilidades técnicas y restaurar el servicio.
- Vigilar la disponibilidad y el funcionamiento de servidores, aplicaciones y bases de datos.
- Integrar y conservar la evidencia de un incidente, con cadena de custodia.
- Acreditar ante órganos de control y auditores el cumplimiento de las medidas de seguridad.

*Finalidades secundarias: * **ninguna.**

Negación expresa. Los registros **no se usan para evaluar el desempeño, ni para medir productividad, jornada, asistencia, puntualidad o conducta** ajena a la seguridad de los sistemas. No se elaboran perfiles individuales ni tableros de actividad por persona. La consulta de la actividad de una cuenta de persona solo procede para atender un hallazgo o incidente concreto, con justificación registrada.

Uso como prueba. Cuando un incidente de seguridad lo amerite, los registros podrán aportarse como prueba ante el órgano interno de control, en procedimientos de responsabilidad

administrativa o ante el Ministerio Público, en los términos de la legislación aplicable y conforme al artículo 23, fracciones I y III, de la LPDPPSO-NL.

Datos de terceros. EL PERSONAL CON ACCESO **no debe escribir datos personales de ciudadanos** (CURP, RFC, nombres, folios, expedientes) **ni contraseñas** como argumento de un comando. Para eso se usan archivos o variables que no quedan registrados. Los datos que aun así lleguen a registrarse se enmascaran en el servidor de origen.

VI.- Transferencias y remisiones.

Los datos personales podrán transmitirse, sin requerir el consentimiento del titular, a las autoridades competentes que los requieran en el ejercicio de sus atribuciones (órgano interno de control, fiscalía, autoridad jurisdiccional), en los supuestos de excepción que prevé el artículo 23 de la LPDPPSO-NL y conforme a lo previsto en su Título Quinto, Capítulo Único, «De las Transferencias y Remisiones de Datos Personales», así como en el artículo 145 fracción V de la Ley de Transparencia y Acceso a la Información Pública del Estado de Nuevo León.

Avisos de alerta. Para avisar al personal de seguridad fuera de horario, el Instituto envía alertas mediante un servicio de mensajería instantánea cuyo proveedor está fuera del país. Esas alertas **no contienen datos personales**: solo número de hallazgo, severidad, regla, servidor afectado, conteo y un enlace a la consola interna, que exige autenticación. **No contienen cuentas de personas, direcciones IP de ciudadanos, comandos, rutas ni texto de errores**, y un filtro institucional rechaza cualquier mensaje que no se ajuste a esa plantilla. Por su contenido, estas alertas no constituyen tratamiento de datos personales.

Toda otra transferencia, nacional o internacional, se sujetará al consentimiento del titular.

VII.- Consecuencias de la negativa.

El registro de actividad es una condición técnica de seguridad para operar los sistemas del Instituto y no puede desactivarse para una persona en particular. Para el personal con acceso, la negativa tendrá como consecuencia la imposibilidad de otorgar una cuenta en esos sistemas. Para las personas usuarias de los portales, el registro técnico es inherente a la conexión; quien no desee que se registre su visita puede realizar sus trámites en las ventanillas del Instituto.

VIII.- Mecanismos, medios y procedimientos para ejercer los derechos ARCO.

El titular, por sí o mediante representante legal debidamente acreditado, podrá ejercer los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) ante la Unidad de Transparencia del Instituto o a través de <https://www.plataformadetransparencia.org.mx/>, conforme al artículo 61 de la LPDPPSO-NL y sin mayores requisitos que los del artículo 63.

Si el ejercicio es electrónico, el titular deberá presentarse dentro de los 3 días siguientes en la Unidad de Transparencia para acreditar su identidad. La respuesta se dará en un plazo no mayor a 20 días hábiles, ampliable hasta por 10 días hábiles más cuando se justifique y se notifique dentro del plazo de respuesta.

Para ejercer el acceso sobre visitas a los portales, conviene indicar la dirección IP, la fecha y el horario aproximado, porque el Instituto no asocia esas direcciones con nombres.

Límites durante una investigación. Los derechos de acceso, cancelación y oposición podrán limitarse **temporalmente** mientras los registros sean necesarios para atender un incidente de seguridad, un procedimiento administrativo o judicial en curso, o una obligación legal, en los supuestos de improcedencia que prevé el artículo 66 de la LPDPPSO-NL. La limitación se notificará al titular de forma fundada y motivada y concluirá cuando cese la causa. La rectificación de registros técnicos procede para corregir la asignación de una cuenta a una persona, no para alterar el contenido de un evento, que se conserva íntegro como evidencia.

Bloqueo automático. Si una dirección IP fue bloqueada por error en el portal web, puede solicitarse su revisión ante LA DIRECCIÓN, en el domicilio señalado en la sección I. El bloqueo es una medida de control de acceso adoptada conforme al artículo 36 de la LPDPPSO-NL y no constituye un tratamiento indebido de datos personales.

IX.- Domicilio de la Unidad de Transparencia.

Tercer piso del Pabellón Ciudadano, Washington 2000 Oriente, colonia Obrera, Monterrey, Nuevo León, C.P. 64010, de 8:00 a 17:00 horas. Teléfono 81-2033-0075, extensión 41629.

X.- Plazos de conservación.

- **En cada servidor:** el tiempo que permita el espacio asignado al registro local (norma técnica mínima: 14 días en Windows; en Linux, 40 archivos de 100 MB); al llenarse, los registros más antiguos se eliminan automáticamente.
- **En el sistema central de monitoreo del Instituto:** 90 días contados desde la fecha del evento, sin prórroga ordinaria. La base de datos los elimina automáticamente por día.
- **Respallos del sistema central:** con un plazo que no exceda el de la información respaldada más el ciclo de rotación del respaldo.
- **Hallazgos:** cada hallazgo conserva hasta 50 eventos relacionados como evidencia, hasta la conclusión formal del expediente o asunto, conforme al Catálogo de Disposición Documental del Instituto.
- **Conservación legal por incidente:** los registros vinculados a un incidente de seguridad o a un procedimiento en curso se separan en un almacén de acceso restringido, con huella digital

y manifiesto, y se conservan hasta que el caso concluya; después se suprimen o se transfieren según el Catálogo de Disposición Documental.

- **Bitácora de consultas al sistema central:** al menos un año.

Al vencer los plazos, los datos se suprimen de forma segura, conforme al Catálogo de Disposición Documental del Instituto. Cuando el catálogo fija un plazo condicionado, este concluye con el cierre o la conclusión formal del expediente o asunto.

XI.- Encargados y servicios en la nube.

Los registros se reciben, almacenan y analizan en infraestructura propia del Instituto, sin servicios de cómputo en la nube. Las alertas descritas en la sección VI salen por un único servidor institucional que filtra su contenido. Si en el futuro interviniera un encargado o un servicio en la nube que reciba datos personales, se formalizarán las condiciones que exige la LPDPPSO-NL en su Título Cuarto, «Relación del Responsable y Encargado», y en su Título Quinto, «De las Transferencias y Remisiones de Datos Personales», y se actualizará este aviso antes de hacerlo.

XII.- Medidas de seguridad.

El acceso al sistema central es exclusivo del personal de seguridad de la información y de los administradores designados, con cuentas propias, contraseña y segundo factor de autenticación, y por roles. Cada consulta de detalle queda registrada con usuario, fecha, hora y criterio de búsqueda en una bitácora que no puede modificarse y que revisa un área ajena a la operación de seguridad. La lista de personas con acceso se revisa trimestralmente. Las exportaciones solo proceden con justificación registrada y nunca hacia servicios externos. La evidencia de incidentes se resguarda con huella digital (SHA-256) y cadena de custodia. Este tratamiento forma parte del inventario de tratamientos y del documento de seguridad del Instituto, conforme a los artículos 36, 41 y 45 de la LPDPPSO-NL.

XIII.- Medio para comunicar cambios al aviso.

Los cambios se darán a conocer en <https://ircnl.gob.mx/> y, para el personal con acceso, por correo institucional, antes de que entren en vigor.

XIV.- Dónde consultar este aviso.

En <https://ircnl.gob.mx/sobre-el-tratamiento-de-los-datos-personales>, en la TABLA DE AVISOS del segundo piso del Pabellón Ciudadano, en el aviso simplificado de los portales del Instituto y en la leyenda que se muestra al iniciar sesión en los servidores del Instituto.

Fecha de la última actualización: 7 de octubre de 2026.