DOCUMENTO DE SEGURIDAD EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Servicios de Salud de Nuevo León, Organismo Público Descentralizado

Matamoros 520 Ote., Zona Centro, Monterrey, N.L. C.P. 64000 | Tel. 81 8130 7000
@saludNL

1. Introducción.

Servicios de Salud de Nuevo León, es un Organismo Público Descentralizado de la Administración Pública Paraestatal, con personalidad jurídica y patrimonio propios, tiene como objeto prestar en el Estado los servicios de salud a población abierta, de conformidad con lo dispuesto por la Ley que crea el Organismo Público Descentralizado Servicios de Salud de Nuevo León, la Ley General de Salud y la Ley Estatal de Salud, el Acuerdo de Coordinación para la Descentralización Integral de los Servicios de Salud y las demás disposiciones legales aplicables.

En función de lo antes mencionado, se cuenta con una amplia estructura Orgánica, que contempla tanto unidades administrativas como de atención médica, en las cuales e realiza un intensivo tratamiento de datos personales no solo de carácter confidencial sino también de carácter sensible, por lo que a fin de garantizar la protección de los datos personales así como el ejercicio de los Derechos ARCO establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, se han realizado actividades para concientizar al personal, y cumplir con los principios y deberes establecidos en la Ley, dando como resultado el presente instrumento, el cual ha sido creado en cumplimiento a las obligaciones establecidas en el artículo 41 de la Ley, el cual en síntesis refiere que el responsable de los datos personales deberá de elaborar un documento de seguridad que contenga, un inventario de datos personales y de los sistemas de tratamiento; las funciones y obligaciones de las personas que traten datos personales; un análisis de riesgo; un análisis de brecha; el plan de trabajo; los mecanismo de monitoreo y revisión de las medidas de seguridad; y el programa general de capacitación.

2. Glosario.

Bases de datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Consentimiento: Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual autoriza el tratamiento de los mismos.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, alfanumérica, gráfica, fotográfica, acústica o en cualquier otro formato. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información, siempre y cuando esto no requiera plazos, medios o actividades desproporcionadas.

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. Se consideran sensibles, de manera enunciativa más no limitativa, los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente o futuro, datos genéticos o datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Encargado: La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

Ley: Ley de Protección de Datos Personales del Estado de Nuevo León.

Ley de Transparencia: Ley de Transparencia y Acceso a la Información Pública del Estado de Nuevo León.

Ley General: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Ley General de Transparencia: Ley General de Transparencia y Acceso a la Información Pública.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan garantizar la confidencialidad, disponibilidad e integridad de los datos personales.

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de los datos personales a nivel organizacional, la identificación, clasificación y borrado seguro de los datos personales, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir el acceso no autorizado al perímetro de la organización del responsable, sus instalaciones físicas, áreas críticas, recursos y datos personales;

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización del responsable, recursos y datos personales;

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización del responsable; y

d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir que el acceso a los datos personales, así como a los recursos, sea por usuarios identificados y autorizados;

b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware; y

d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Responsable: Cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, fideicomisos y fondos públicos y partidos políticos del estado de

Nuevo León, que decide y determina los fines, medios y demás cuestiones relacionadas con determinado tratamiento de datos personales.

Titular: La persona física a quien corresponden los datos personales.

Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados aplicados a los datos personales, relacionadas de manera enunciativa más no limitativa, con la obtención, uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, transferencia y en general cualquier uso o disposición de datos personales.

3. Inventario de Datos Personales y Sistemas de Tratamiento.

A continuación, se muestra el inventario de datos personales y los sistemas de tratamiento, el cual se muestra de manera simplificada a fin de no ampliar el contenido del presente Documento de Seguridad, no obstante, el Inventario completo se encuentra disponible en al ANEXO I, como parte integral del presente instrumento.

En cumplimiento con las finalidades establecidas y debidamente fundamentadas en los diversos avisos de privacidad con los que se cuenta recaba y les da tratamiento a los siguientes datos personales:

4. Las Funciones y obligaciones de las personas que traten datos personales.

Servicios de Salud de Nuevo León, es un Organismo Público Descentralizado de la Administración Pública Paraestatal, con personalidad jurídica y patrimonio propios, tiene como objeto prestar en el Estado los servicios de salud a población abierta, de conformidad con lo dispuesto por la Ley que crea el Organismo Público Descentralizado Servicios de Salud de Nuevo León, la Ley General de Salud y la Ley Estatal de Salud, el Acuerdo de Coordinación para la Descentralización Integral de los Servicios de Salud y las demás disposiciones legales aplicables.

Los datos personales que se recaban son utilizados por las y los servidores públicos en conformidad de lo establecido en el Reglamento Interior del Organismo Público Descentralizado Denominado Servicios de Salud de Nuevo León, y demás disposiciones que resulten aplicables únicamente para las finalidades que fueron recabados.

N°	TRATAMIENTO	DIRECCIÓN	DATOS PERSONALES QUE SE RECABAN	FINALIDAD PARA LA CUAL SE OBTUVIERON
1	SINBA-SIS (Generar la información de los servicios otorgados en las unidades médicas de la Secretaría de Salud) al otorgar una consulta médica	Unidad Shock Trauma Galeana	Datos Confidenciales	Control interno de Botica y Fines estadísticos y control de Medicamentos Controlados. Registro en los diarios de control para medicamentos de Fracción I, II y III
2	SIMA (Sistema Integral Médico Administrativo).	Dirección de Hospitales	Datos confidenciales: CURP, Fecha de nacimiento, Lugar de nacimiento, Nombre completo, Género, Subsidio, Estado Civil, Escolaridad, Ocupación, Domicilio y Teléfonos/ Datos sensibles: Grupo étnico, Discapacidad, Identidad de género, Orientación sexual y Religión	Creación del Expediente Clínico y Electrónico

3	Tratamiento de datos de personal de nuevo ingreso laboral.	Dirección administrativa	Datos Confidenciales: Información de Contacto, identificación, escolaridad. Datos Sensibles: Resultados psicométricos y estado de salud.	Acreditar la identidad del titular de los datos personales, validar su perfil académico y psicológico y en su caso, autorizar el ingreso a laborar al organismo.
4	Solicitud de diversas prestaciones laborales y trámites administrativos.	Dirección administrativa	Datos Confidenciales: Datos personales de identificación, de familiares, de nómina, de gastos (facturas), según corresponda. Datos sensibles: Estado de salud, actas de defunción, porcentaje y montos de pensiones de alimentos, según corresponda.	Conceder prestaciones laborales, realizar trámites administrativos.
5	Alta de cuenta personal de empleados de los servicios de salud en Sistema Visor de Recibos de Nómina	Dirección administrativa	Datos confidenciales: Datos de identificación y contacto como domicilio.	Generar representación impresa del recibo de pago y actualización del catálogo del personal.
6	Solicitud de Resguardo por Síntomas de COVID	Dirección administrativa	Datos confidenciales: Datos de identificación, datos de contacto como domicilio. Datos sensibles: Estado de salud (síntomas, comorbilidades, valoración médica, resultado de prueba).	Generar certificado de autorización para resguardo por síntomas de COVID.
7	Recibir datos confidenciales y sensibles para apertura el expediente clínico.	Centro de Rehabilitación Física y Ortopedia "Solidaridad"	Datos confidenciales: Datos de identificación y contacto, Datos laborales, Datos académicos; Datos Sensibles: creencias religiosas, identidad de género y orientación sexual.	Acreditar la identidad del titular de los datos personales para apertura el expediente clínico
8	Recibir datos confidenciales y sensibles para complemento del diagnóstico médico.	Centro de Rehabilitación Física y Ortopedia "Solidaridad"	Datos confidenciales: Datos de identificación y contacto, Datos laborales, Datos académicos, Datos socioeconómicos; Datos Sensibles: antecedentes patológicos.	Acreditar la identidad del titular de los datos personales y antecedentes para realizar el diagnóstico clínico correspondiente.

9	Recibir datos confidenciales y sensibles para programar las sesiones de terapia.	Centro de Rehabilitación Física y Ortopedia "Solidaridad"	Datos confidenciales: Datos de identificación y contacto; Datos Sensibles: diagnóstico médico.	Acreditar la identidad del titular de los datos personales y antecedentes para realizar la programación de terapias correspondiente.
10	Recibir datos confidenciales y sensibles para realizar el estudio socioeconómico.	Centro de Rehabilitación Física y Ortopedia "Solidaridad"	Datos confidenciales: Datos de identificación y contacto, Datos laborales, Datos académicos, Datos socioeconómicos; Datos Sensibles: creencias religiosas.	Acreditar la identidad del titular de los datos personales y antecedentes para realizar el estudio socioeconómico correspondiente.
11	Recibir datos confidenciales y sensibles del expediente clínico.	Centro de Rehabilitación Física y Ortopedia "Solidaridad"	Datos confidenciales: Datos de identificación y contacto, Datos laborales, Datos académicos, Datos socioeconómicos; Datos Sensibles: creencias religiosas, identidad de género y orientación sexual.	Acreditar la identidad del titular de los datos personales para resguardar físicamente el expediente clínico.
12	Recibir datos confidenciales y sensibles para complemento del diagnóstico psicológico.	Centro de Rehabilitación Física y Ortopedia "Solidaridad"	Datos confidenciales: Datos de identificación y contacto, Datos laborales, Datos académicos, Datos socioeconómicos; Datos Sensibles: antecedentes patológicos.	Acreditar la identidad del titular de los datos personales y antecedentes para realizar el diagnóstico psicológico correspondiente.
13	Recibir datos confidenciales y sensibles para complemento del diagnóstico de Comunicación Humana.	Centro de Rehabilitación Física y Ortopedia "Solidaridad"	Datos confidenciales: Datos de identificación y contacto, Datos laborales, Datos académicos, Datos socioeconómicos; Datos Sensibles: antecedentes patológicos.	Acreditar la identidad del titular de los datos personales y antecedentes para realizar el diagnóstico clínico correspondiente.
14	Recibir datos confidenciales y sensibles para complemento de indicaciones de terapia física y ocupacional.	Centro de Rehabilitación Física y Ortopedia "Solidaridad"	Datos confidenciales: Datos de identificación y contacto, Datos laborales, Datos académicos, Datos socioeconómicos; Datos Sensibles: antecedentes patológicos.	Acreditar la identidad del titular de los datos personales y antecedentes para complemento de indicaciones de terapia física y ocupacional.

15	Recibir datos confidenciales para traslado de pacientes.	Centro de Rehabilitación Física y Ortopedia "Solidaridad"	Datos confidenciales: Datos de identificación y contacto, Datos socioeconómicos; Datos Sensibles: enfermedad.	Acreditar la identidad del titular de los datos personales para traslado de paciente con discapacidad.
16	Recibir datos confidenciales y sensibles para atender quejas, sugerencias, felicitaciones y gestiones.	Centro de Rehabilitación Física y Ortopedia "Solidaridad"	Datos confidenciales: Datos de identificación y contacto, Datos socioeconómicos; Datos Sensibles: antecedentes patológicos.	Acreditar la identidad del titular de los datos personales para seguimiento del caso.
17	Recibir datos confidenciales y sensibles para conectar a salas del ZOOM para telemedicina.	Centro de Rehabilitación Física y Ortopedia "Solidaridad"	Datos confidenciales: Datos de identificación y contacto, Datos socioeconómicos; Datos Sensibles: enfermedad.	Acreditar la identidad del titular de los datos personales para dar acceso a sala de telemedicina.
18	Recibir datos confidenciales y sensibles para cobro de cuotas de recuperación.	Centro de Rehabilitación Física y Ortopedia "Solidaridad"	Datos confidenciales: Datos de identificación y contacto, Datos socioeconómicos; Datos Sensibles: antecedentes patológicos.	Acreditar la identidad del titular de los datos personales para cobro de cuotas de recuperación.
19	Recibir datos confidenciales y sensibles para integrar expediente laboral.	Centro de Rehabilitación Física y Ortopedia "Solidaridad"	Datos confidenciales: Datos de identificación y contacto, Datos socioeconómicos; Datos Sensibles: antecedentes patológicos.	Acreditar la identidad del titular de los datos personales para la integración del expediente laboral.
20	Recibir datos confidenciales y sensibles para complemento del diagnóstico de enfermería.	Centro de Rehabilitación Física y Ortopedia "Solidaridad"	Datos confidenciales: Datos de identificación y contacto, Datos laborales, Datos académicos, Datos socioeconómicos; Datos Sensibles: antecedentes patológicos.	Acreditar la identidad del titular de los datos personales y antecedentes para realizar el diagnóstico de enfermería correspondiente.

21	Recibir datos confidenciales y sensibles para complemento de indicaciones de terapia física y ocupacional.	Centro de Rehabilitación Física y Ortopedia "Solidaridad"	Datos confidenciales: Datos de identificación y contacto, Datos laborales, Datos académicos, Datos socioeconómicos; Datos Sensibles: antecedentes patológicos.	Acreditar la identidad del titular de los datos personales y antecedentes para complemento de indicaciones de terapia física y ocupacional.
22	Recibir datos confidenciales y sensibles para realizar el estudio socioeconómico.	Centro de Rehabilitación Física y Ortopedia "Solidaridad"	Datos confidenciales: Datos de identificación y contacto, Datos laborales, Datos académicos, Datos socioeconómicos; Datos Sensibles: creencias religiosas.	Acreditar la identidad del titular de los datos personales y antecedentes para realizar el estudio socioeconómico correspondiente.
23	Se solicitan en forma electrónica la identificación (INE) de los servidores públicos por Registro de firmas en instituciones bancarias	Dirección administrativa	Datos de Identificación: Los contenidos en una Copia electrónica del INE	Acreditar la identidad del titular de los datos personales ante instituciones bancarias
24	Se solicita a proveedores que proporcionen información para su proceso de pago y entre ellas se le requiere nos hagan llegar copia del INE de Representante Legal	Dirección administrativa	Datos de Identificación: Los contenidos en una Copia electrónica del INE	Acreditar la identidad del Representante Legal de los Proveedores
25	Tratamiento de datos del nuevo ingreso laboral.	Dirección administrativa	Datos Confidenciales: Información de Contacto, identificación, escolaridad. Datos Sensibles: Resultados psicométricos y estado de salud.	Acreditar la identidad del titular de los datos personales, validar su perfil académico y psicológico y en su caso, autorizar el ingreso a laborar al organismo.
26	Solicitud de diversas prestaciones laborales y trámites administrativos	Dirección administrativa	Datos Confidenciales: Datos personales de identificación, de familiares, de nómina, de gastos (facturas), según corresponda. Datos sensibles: Estado de salud, actas de defunción, porcentaje y montos de pensiones de alimentos, según corresponda.	Conceder prestaciones laborales, realizar trámites administrativos.

27	Alta de cuenta personal de empleados de los servicios de salud en Sistema Visor de Recibos de Nómina	Dirección administrativa	Datos confidenciales: Datos de identificación y contacto como domicilio.	Generar representación impresa del recibo de pago y actualización del catálogo del personal.
28	Validación de casos de segundo y tercer nivel de atención	Dirección de Hospitales	Datos Confidenciales: información de contacto y de identificación. Datos Sensibles: Estado de Salud	Corroborar atención médica para validación y comprobación de pago
29	Base de Datos SQL del Expediente Clínico Electrónico Hospitalario	Departamento de archivo clínico y estadísticas	Comprobar la identidad de los pacientes y crear su archivo clínico electrónico y físico.	NOM-004 NOM-024
30	Base de Datos de la Web de Registro Cuidar tu Salud	Departamento de Informática, Dirección de Planeación	Datos confidenciales: Datos de identificación e información de contacto.	Artículo 59 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.
31	Base de Datos de la Plataforma "Estudio de Factibilidad"	Departamento de Informática, Dirección de Planeación	Datos confidenciales: Datos de identificación e información de contacto.	Comprobar Identidad
32	Bases de Datos "gafetes de regulación sanitaria"	Departamento de Informática, Dirección de Planeación	Datos confidenciales: Datos de identificación e información de contacto.	Comprobar Identidad

33	Bases de Datos "tramites de regulación sanitaria"	Departamento de Informática, Dirección de Planeación	Datos confidenciales: Datos de identificación e información de contacto.	Comprobar Identidad.
34	Bases de Datos de la Plataforma "Aula Virtual"	Departamento de Informática, Dirección de Planeación	Datos confidenciales: Datos de identificación e información de contacto.	Comprobar Identidad
35	Bases de Datos de "Boleta de Alumbramiento"	Departamento de Informática, Dirección de Planeación	Datos confidenciales: Datos de identificación e información de contacto.	Comprobar Identidad
36	Bases de Datos "Sistema de Gestoría"	Departamento de Informática, Dirección de Planeación	Datos confidenciales: Datos de identificación e información de contacto.	Comprobar Identidad
37	Solicitudes ARCO	DIRECCIÓN JURÍDICA	Datos Confidenciales: información de contacto teléfono, correo, domicilio y de identificación nombre, identificación, corp., numero de credencial IFE/INE Datos Sensibles: Estado de Salud	Acreditar la identidad del titular de los datos personales y en su caso hacer entrega de la información personal solicitada
38	Almacenamiento de datos personales por departamentos de RH en las distintas jurisdicciones sanitarias.	Jurisdicciones Sanitarias	Datos confidenciales: Datos de identificación (nombre) y contacto (domicilio, núm. teléfono casa y celular y correo electrónico), Datos laborales, Datos académicos, Datos Financieros tales talones de cheques, datos biométricos (huella dactilar, toma de fotografía para gafete) Datos Sensibles: Estado de salud pasado, presente, datos biométricos como huella dactilar, toma de fotografía para gafete.	Finalidad principal: para contratación de personal con la validación de datos académicos acorde al profesiograma institucional; validación de datos personales y laborales para cálculo de estímulos acorde a la antigüedad laboral; datos biométricos como toma de la huella digital para el registro electrónico de asistencia en el reloj checador, toma de fotografías para elaboración de gafete institucional

39	Registro de visitas en libros e imágenes de Circuito Cerrado (CCTV).	Unidad de Seguridad	Datos confidenciales: Información de contacto, identificación y firma de la Compañía.	Acreditar la identidad del titular de los datos personales, orden y control del ingreso a instalaciones.
40	Entrega de resumen medico Solicitado por medio de oficio del CODE, Localización de pacientes para agenda de citas en otras unidades médicas y/o reagendar citas dentro de nuestra unidad.	Unidad Shock Trauma Galeana	Datos confidenciales y Datos sensibles	Atender casos medico legales, según lo solicite alguna autoridad. Solicitar resumen medico según la autoridad lo solicite por medio de oficio. Agendar citas tanto en la unidad como fuera de la misma.
41	Realiza los listados de pacientes que son requeridos para contestar los oficios de transparencia, registros de productividad, registros de pacientes embarazadas y con sobrepeso	Unidad Shock Trauma Galeana	Datos confidenciales y Datos sensibles	Atender casos estadísticos y de productividad, además de registro de certificados de nacimiento, defunción y muerte fetal.
42	Revisar expedientes que cumplan con todos los rubros adecuadamente llenados para subrogar aquellos servicios brindados de urgencia a pacientes con seguridad social.	Unidad Shock Trauma Galeana	Datos confidenciales y Datos sensibles	Realizar subrogación de servicios de otros servicios de salud que lo soliciten en la unidad. Ameritando revisar que los formatos sean adecuadamente llenados, así como que se cuente con el número de afiliación adecuado.
43	Resguardo de recetas de medicamentos donde incluye además de los medicamentos proporcionadas, o información sobre nombre, edad, genero, fecha de nacimiento, domicilio y diagnósticos	Unidad Shock Trauma Galeana	Datos Confidenciales	Control interno de Botica y Fines estadísticos y control de Medicamentos Controlados. Registro en los diarios de control para medicamentos de Fracción I, II y III
44	Revisión de expedientes clínicos para ver si cumplen con los criterios de calidad que exige el comité de MECIC y los estándares de calidad, además de identificar fallas en su llenado y hacer las observaciones pertinentes al área de enfermería.	Unidad Shock Trauma Galeana	Datos confidenciales y Datos sensibles	Acreditar identidad del titular de los datos

45	Revisión de expedientes clínicos para ver si cumplen con los criterios de calidad que exige el comité de MECIC y los estándares de calidad, además de identificar fallas en su llenado y hacer las observaciones pertinentes al área medica	Unidad Shock Trauma Galeana	Datos confidenciales y Datos sensibles	Acreditar identidad del titular de los datos y congruencia de los diagnósticos y tratamientos. Así como revisar que se cuente con los expedientes con firma del médico tratante.
46	Atención Médica	Departamento de archivo clínico y estadísticas	Comprobar la identidad de los pacientes y crear su archivo clínico electrónico y físico.	NOM-004 NOM-024

El tratamiento de sus Datos Personales se realiza con apego al aviso de privacidad diseñado para cada uno de los tratamientos con fundamento en lo establecido en los artículos 1 párrafo 5, 3 fracción X, XI, XXXIII, XXXVIII, 16,17,18, 22, 23 fracciones I, III, VI, 27, 52, 53, 54, 55, 56, 59, 60, 76, 77, 78, 79, 80, 81 y 99 la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León los artículos 58 y 91 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Nuevo León, artículos 1, 1Bis, 2, 3 y 77 Bis 1 de la Ley General en Salud, lo dispuesto en la Ley que crea el Organismo Público Descentralizado Servicios de Salud de Nuevo León, la Ley Estatal de Salud, el Acuerdo de Coordinación para la Descentralización Integral de los Servicios de Salud, el Reglamento Interior del Organismo Público Descentralizado denominado Servicios de Salud de Nuevo León, y demás normativa que resulte aplicable en el ámbito de la competencia de este Organismo.

Asimismo, de manera enunciativa mas no limitativa, las Unidades Administrativas deberán de garantizar las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, mantener actualizado el inventario de datos personales, recabar el consentimiento en caso de ser necesario, dar difusión al aviso de privacidad, así como recibir capacitación en la materia.

5. El análisis de Riesgos.

En atención a lo establecido por la fracción III del artículo 41 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León; se realiza el siguiente análisis de los riesgos que se pueden presentar respecto del tratamiento que este organismo realiza referente a los datos personales que en ejercicio de sus atribuciones recaba.

Para establecer el valor de la "PROBABILIDAD" de que ocurra el riesgo se estableció una métrica del 1 al 5, según la probabilidad de ocurrencia del riesgo mencionado, donde 1 es nada probable, 2 es muy poco probable, 3 es poco probable, 4 es probable y 5 es muy probable. Y para establecer la "GRAVEDAD" del riesgo se estableció un valor del 1 al 5 según la gravedad del riesgo, donde 1 es nada riesgoso, 2 muy poco riesgoso, 3 poco riesgoso, 4 algo riesgoso y 5 muy riesgoso; a su vez, la "CALIFICACIÓN" otorgada al riesgo es obtenida de la multiplicación de la probabilidad por gravedad.

Derivado de lo anterior, se determinaron 3 Niveles de Riesgo: Alto, Medio y Bajo; los cuales se identifican con los colores rojo, amarillo y verde de acuerdo con lo establecido en la siguiente tabla:

Analisis de Riesgos

Valor de Gravedad (1-5)					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
		1	2	3	4	5

Valor de probabilidad (1-5)

Nivel de riesgo
Alto (20-25)
Medio (10-16)
Bajo (1-9)

Análisis de Riesgos

N°	Tipificación		Análisis		Evaluación		Área de Control
	Tratamiento de Datos Personales	Riesgo	Probabilidad	Gravedad	Calificación	NIVEL DE RIESGO	
1	SINBA-SIS (Generar la información de los servicios otorgados en las unidades médicas de la Secretaría de Salud) al otorgar una consulta médica.	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	DIRECCIÓN DE PLANEACIÓN
		Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	3	3	BAJO	

2	SIMA (Sistema Integral Médico Administrativo).	Acceso de personal no autorizado a base de datos	1	3	3	BAJO	SUBDIRECCIÓN DE RECUROS FINANCIEROS
		Fuga de Información contenida en la Base de Datos	1	4	4	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	3	3	BAJO	
3	Tratamiento de datos de personal de nuevo ingreso laboral.	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Departamento de Reclutamiento y Selección de la Subdirección de Recursos Humanos
		Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	5	5	BAJO	
4	Solicitud de diversas prestaciones laborales y trámites administrativos.	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Departamento de Relaciones Laborales
		Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	5	5	BAJO	
5	Alta de cuenta personal de empleados de los servicios de salud en Sistema Visor de Recibos de Nómina	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Subdirección de Recursos Humanos
		Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	5	5	BAJO	
6	Solicitud de Resguardo por Síntomas de COVID	Acceso de personal no autorizado a base de datos	1	2	2	BAJO	Subdirección de Recursos Humanos
		Fuga de Información contenida en la Base de Datos	1	2	2	BAJO	

		Entrega de medio de identificación a Persona no Autorizada	1	2	2	BAJO	
7	Recibir datos confidenciales y sensibles para apertura el expediente clínico.	Acceso de personal no autorizado a base de datos	1	3	3	BAJO	Centro de Rehabilitación Física y Ortopedia "Solidaridad"
		Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	3	3	BAJO	
8	Recibir datos confidenciales y sensibles para complemento del diagnóstico médico.	Acceso de personal no autorizado a base de datos	1	2	2	BAJO	Centro de Rehabilitación Física y Ortopedia "Solidaridad"
		Fuga de Información contenida en la Base de Datos	1	2	2	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	1	1	BAJO	
9	Recibir datos confidenciales y sensibles para programar las sesiones de terapia.	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Centro de Rehabilitación Física y Ortopedia "Solidaridad"
		Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	3	3	BAJO	
10	Recibir datos confidenciales y sensibles para realizar el estudio socioeconómico.	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Centro de Rehabilitación Física y Ortopedia "Solidaridad"
		Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	5	5	BAJO	
11	Recibir datos confidenciales y sensibles del expediente clínico.	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Centro de Rehabilitación Física y Ortopedia "Solidaridad"
		Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	3	3	BAJO	

12	Recibir datos confidenciales y sensibles para complemento del diagnóstico psicológico.	Acceso de personal no autorizado a base de datos	1	3	3	BAJO	Centro de Rehabilitación Física y Ortopedia "Solidaridad"
		Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	3	3	BAJO	
13	Recibir datos confidenciales y sensibles para complemento del diagnóstico de Comunicación Humana.	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Centro de Rehabilitación Física y Ortopedia "Solidaridad"
		Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	3	3	BAJO	
14	Recibir datos confidenciales y sensibles para complemento de indicaciones de terapia física y ocupacional.	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Centro de Rehabilitación Física y Ortopedia "Solidaridad"
		Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	3	3	BAJO	
15	Recibir datos confidenciales para traslado de pacientes.	Acceso de personal no autorizado a base de datos	1	3	3	BAJO	Centro de Rehabilitación Física y Ortopedia "Solidaridad"
		Fuga de Información contenida en la Base de Datos	1	3	3	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	4	4	BAJO	
16	Recibir datos confidenciales y sensibles para atender quejas, sugerencias, felicitaciones y gestiones.	Acceso de personal no autorizado a base de datos	1	3	3	BAJO	Centro de Rehabilitación Física y Ortopedia "Solidaridad"
		Fuga de Información contenida en la Base de Datos	1	3	3	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	3	3	BAJO	
17	Recibir datos confidenciales y sensibles	Acceso de personal no autorizado a base de datos	1	2	2	BAJO	Centro de Rehabilitación Física y

	para conectar a salas del ZOOM para telemedicina.	Fuga de Información contenida en la Base de Datos	1	3	3	BAJO	Ortopedia "Solidaridad"
		Entrega de medio de identificación a Persona no Autorizada	1	3	3	BAJO	
18	Recibir datos confidenciales y sensibles para cobro de cuotas de recuperación.	Acceso de personal no autorizado a base de datos	1	2	2	BAJO	Centro de Rehabilitación Física y Ortopedia "Solidaridad"
		Fuga de Información contenida en la Base de Datos	1	2	2	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	1	1	BAJO	
19	Recibir datos confidenciales y sensibles para integrar expediente laboral.	Acceso de personal no autorizado a base de datos	1	2	2	BAJO	Centro de Rehabilitación Física y Ortopedia "Solidaridad"
		Fuga de Información contenida en la Base de Datos	1	2	2	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	1	1	BAJO	
20	Recibir datos confidenciales y sensibles para complemento del diagnóstico de enfermería.	Acceso de personal no autorizado a base de datos	1	2	2	BAJO	Centro de Rehabilitación Física y Ortopedia "Solidaridad"
		Fuga de Información contenida en la Base de Datos	1	2	2	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	2	2	BAJO	
21	Recibir datos confidenciales y sensibles para complemento de indicaciones de terapia física y ocupacional.	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Centro de Rehabilitación Física y Ortopedia "Solidaridad"
		Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	3	3	BAJO	
22	Recibir datos confidenciales y sensibles para realizar el estudio socioeconómico.	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Centro de Rehabilitación Física y Ortopedia "Solidaridad"
		Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	

		Entrega de medio de identificación a Persona no Autorizada	1	5	5	BAJO	
23	Se solicitan en forma electrónica la identificación (INE) de los servidores públicos por Registro de firmas en instituciones bancarias	Acceso de personal no autorizado a base de datos	1	3	3	BAJO	Dirección administrativa
		Fuga de Información contenida en la Base de Datos	1	3	3	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	4	4	BAJO	
24	Se solicita a proveedores que proporcionen información para su proceso de pago y entre ellas se le requiere nos hagan llegar copia del INE de Representante Legal	Acceso de personal no autorizado a base de datos	1	3	3	BAJO	Dirección administrativa
		Fuga de Información contenida en la Base de Datos	1	4	4	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	4	4	BAJO	
25	Tratamiento de datos del nuevo ingreso laboral.	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Dirección administrativa
		Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	5	5	BAJO	
26	Solicitud de diversas prestaciones laborales y trámites administrativos	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Dirección administrativa
		Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	5	5	BAJO	
27	Alta de cuenta personal de empleados de los servicios de salud en Sistema Visor de Recibos de Nómina	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Dirección administrativa
		Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	5	5	BAJO	

28	Validación de casos de segundo y tercer nivel de atención	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Dirección de Hospitales, Coordinación administrativa
		Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	3	3	BAJO	
29	Base de Datos SQL del Expediente Clínico Electrónico Hospitalario	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Servicios de Salud de Nuevo León, O.P.D. / Dirección de Planeación / Subdirección de Tecnologías e Información en Salud
		Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	3	3	BAJO	
30	Base de Datos de la Web de Registro Cuidar tu Salud	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Servicios de Salud de Nuevo León, O.P.D. / Dirección de Planeación / Subdirección de Tecnologías e Información en Salud
		Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	2	2	BAJO	
31	Base de Datos de la Plataforma "Estudio de Factibilidad"	Acceso de personal no autorizado a base de datos	1	3	3	BAJO	Servicios de Salud de Nuevo León, O.P.D. / Dirección de Planeación / Subdirección de Tecnologías e Información en Salud
		Fuga de Información contenida en la Base de Datos	1	3	3	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	1	1	BAJO	
32	Bases de Datos "gafetes de regulación sanitaria"	Acceso de personal no autorizado a base de datos	1	3	3	BAJO	Servicios de Salud de Nuevo León, O.P.D. / Dirección de Planeación / Subdirección de Tecnologías e Información en Salud
		Fuga de Información contenida en la Base de Datos	1	3	3	BAJO	

		Entrega de medio de identificación a Persona no Autorizada	1	1	1	BAJO	
33	Bases de Datos "tramites de regulación sanitaria"	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Servicios de Salud de Nuevo León, O.P.D. / Dirección de Planeación / Subdirección de Tecnologías e Información en Salud
		Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	3	3	BAJO	
34	Bases de Datos de la Plataforma "Aula Virtual"	Acceso de personal no autorizado a base de datos	1	2	2	BAJO	Servicios de Salud de Nuevo León, O.P.D. / Dirección de Planeación / Subdirección de Tecnologías e Información en Salud
		Fuga de Información contenida en la Base de Datos	1	2	2	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	1	1	BAJO	
35	Bases de Datos de "Boleta de Alumbramiento"	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Servicios de Salud de Nuevo León, O.P.D. / Dirección de Planeación / Subdirección de Tecnologías e Información en Salud
		Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	3	3	BAJO	
36	Bases de Datos "Sistema de Gestoría"	Acceso de personal no autorizado a base de datos	1	3	3	BAJO	Servicios de Salud de Nuevo León, O.P.D. / Dirección de Planeación / Subdirección de Tecnologías e Información en Salud
		Fuga de Información contenida en la Base de Datos	1	3	3	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	2	2	BAJO	

37	Solicitudes ARCO	Acceso de personal no autorizado a base de datos	1	2	3	BAJO	Dirección Jurídica, Departamento de Acceso a la Información, Protección de Datos Personales y Archivo.
		Fuga de Información contenida en la Base de Datos	1	2	3	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	2	2	BAJO	
38	Almacenamiento de datos personales por departamentos de RH en las distintas jurisdicciones sanitarias.	Acceso de personal no autorizado a base de datos	2	2	4	BAJO	Jurisdicciones sanitarias, Departamento de Recursos Humanos
		Fuga de Información contenida en la Base de Datos	2	2	4	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	2	2	4	BAJO	
39	Registro de visitas en libros e imágenes de Circuito Cerrado (CCTV).	Acceso de personal no autorizado a base de datos	3	3	9	BAJO	Coordinación Institucional de Seguridad
		Fuga de Información contenida en la Base de Datos	1	2	2	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	4	4	BAJO	
40	Entrega de resumen medico Solicitado por medio de oficio del CODE, Localización de pacientes para agenda de citas en otras unidades médicas y/o reagendar citas dentro de nuestra unidad.	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Unidad Shock Trauma Galeana
		Fuga de Información contenida en la Base de Datos	2	4	8	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	5	5	BAJO	

41	Realiza los listados de pacientes que son requeridos para contestar los oficios de transparencia, registros de productividad, registros de pacientes embarazadas y con sobrepeso	Acceso de personal no autorizado a base de datos	1	4	4	BAJO	Unidad Shock Trauma Galeana
		Fuga de Información contenida en la Base de Datos	2	4	8	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	5	5	BAJO	
42	Revisar expedientes que cumplan con todos los rubros adecuadamente llenados para subrogar aquellos servicios brindados de urgencia a pacientes con seguridad social.	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Unidad Shock Trauma Galeana
		Fuga de Información contenida en la Base de Datos	2	4	8	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	5	5	BAJO	
43	Resguardo de recetas de medicamentos donde incluye además de los medicamentos proporcionadas, o información sobre nombre, edad, genero, fecha de nacimiento, domicilio y diagnósticos	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Unidad Shock Trauma Galeana
		Fuga de Información contenida en la Base de Datos	1	3	3	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	5	5	BAJO	
44	Revisión de expedientes clínicos para ver si cumplen con los criterios de calidad que exige el comité de MECIC y los estándares de calidad, además de identificar fallas en su llenado y hacer las observaciones pertinentes al área de enfermería.	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Unidad Shock Trauma Galeana
		Fuga de Información contenida en la Base de Datos	3	4	12	MEDIO	
		Entrega de medio de identificación a Persona no Autorizada	1	5	5	BAJO	
45	Revisión de expedientes clínicos para ver si cumplen con los criterios de calidad que exige el comité de MECIC y los estándares de calidad, además de identificar fallas en su	Acceso de personal no autorizado a base de datos	1	5	5	BAJO	Unidad Shock Trauma Galeana

	llenado y hacer las observaciones pertinentes al área medica	Fuga de Información contenida en la Base de Datos	1	5	5	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	5	5	BAJO	
46	Atención Médica	Acceso de personal no autorizado a base de datos	1	1	1	BAJO	Dirección de Hospitales, Hospital Metropolitano, Área de Admisión y Archivo
		Fuga de Información contenida en la Base de Datos	1	1	1	BAJO	
		Entrega de medio de identificación a Persona no Autorizada	1	1	1	BAJO	

6. El análisis de Brecha.

Tal como lo establece el artículo 41 en su fracción IV de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León; se realiza el análisis de brecha entre las medidas de seguridad existentes y aquellas faltantes. Recordemos que las medidas de seguridad son en tres modalidades como lo marca la ley:

- Técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento,
- Administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de los datos personales a nivel organizacional, la identificación, clasificación y borrado seguro de los

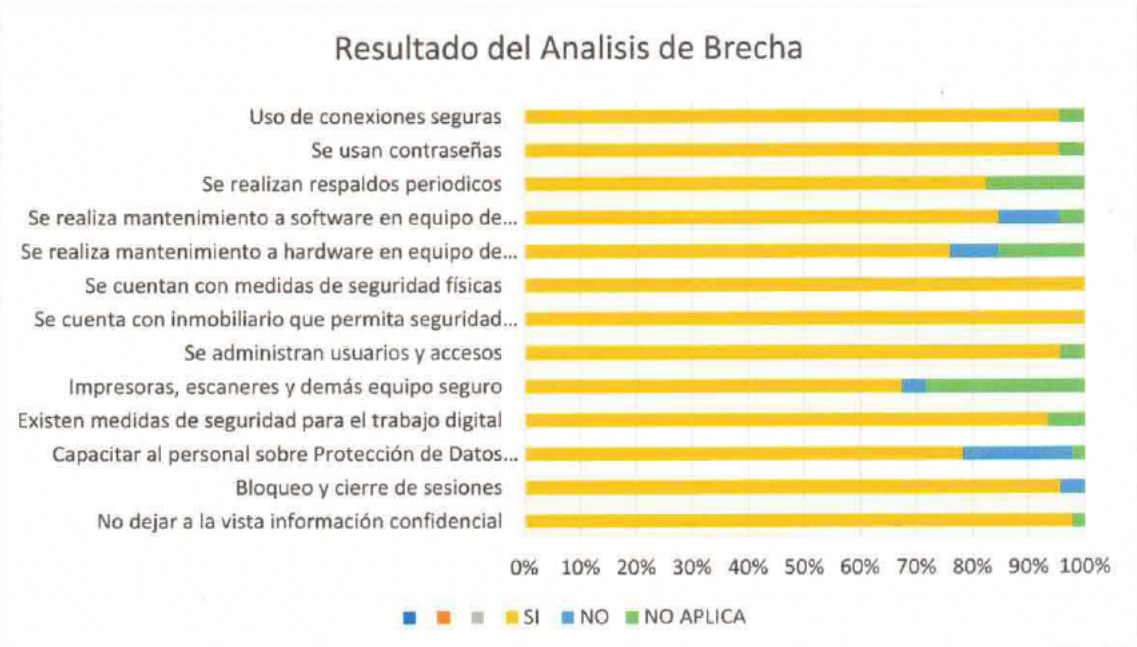
datos personales, así como la sensibilización y capacitación del personal, en materia de protección de datos personales, y

- Físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

Dicho análisis se realizó conforme al siguiente cuestionario:

Medidas de seguridad	Se cuenta con la medida		
	Si	No	No aplica
No dejar a la vista información confidencial			
Impresoras, escáneres y demás equipo seguro			
Capacitar al personal sobre Protección de Datos Personales			
Se realizan respaldos periódicos			
Se cuentan con medidas de seguridad físicas			
Se cuenta con inmobiliario que permita seguridad física			
Se realiza mantenimiento a hardware en equipo de computo			
Se realiza mantenimiento a software en equipo de computo			
Existen medidas de seguridad para el trabajo digital			
Se usan contraseñas			
Bloqueo y cierre de sesiones			
Se administran usuarios y accesos			
Uso de conexiones seguras			

Dando como resultado los siguientes porcentajes de cumplimiento:



7. El Plan de Trabajo.

En concordancia con lo establecido por la fracción V del artículo 41 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, y a fin de aplicar y mantener las medidas de seguridad que permitan garantizar la confidencialidad de los datos personales, se establecieron las siguientes prácticas: Políticas de protección de datos personales; El procedimiento para recibir y responder dudas y quejas de los titulares de los Datos Personales; y El Programa Anual de Capacitación y Actualización del Personal sobre las Obligaciones y Demás Deberes en Materia de Protección de Datos Personales.

Herramientas de trabajo encaminadas a la sensibilización de las y los servidores públicos que dan tratamiento a los datos personales al interior de este Organismo, así como el reconocimiento de áreas de oportunidad y mejora continua de las mismas.

8. Los mecanismos de monitoreo y revisión de las medidas de seguridad.

A fin de monitorear y revisar las medidas de seguridad implementadas en el interior de este Organismo, se cuenta con diferentes mecanismos que permiten detectar áreas de oportunidad, así como prevenir posibles vulneraciones, de manera enunciativas los mecanismos con los que se cuentan son los siguientes:

- Correo habilitado exclusivamente para dar atención en materia de datos personales: oficial.datospersonales.ssnl@saludnl.gob.mx
- Procedimiento para recibir y responder dudas y quejas de los Titulares de los Datos Personales.
- Bitácora de Vulneraciones, que permita atender y dar seguimiento a las posibles vulneraciones de seguridad en materia de protección de datos personales.

Ahora bien, en cumplimiento al artículo 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, se establecieron de manera enunciativa medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

8.1 Medidas de Seguridad Administrativas

La difusión y sensibilización en materia de Protección de Datos Personales, con prácticas tales como: Políticas de protección de datos personales; El procedimiento para recibir y responder dudas y quejas de los titulares de los Datos Personales; y El Programa Anual de Capacitación y Actualización del Personal sobre las Obligaciones y Demás Deberes en Materia de Protección de Datos Personales.

8.2 Medidas de Seguridad Técnicas

1.-Infraestructura

• Un [redacted] donde se registran todos los usuarios y las computadoras conectadas a la red Institucional.

• Configuración de política en los usuarios de [redacted] y correo electrónico para uso de contraseña segura.

• El acceso desde internet hacia nuestra red está protegido por [redacted]

• Aplicamos [redacted] para que la navegación a internet este restringida dependiendo de las diversas funciones de los usuarios

• Todas las computadoras y servidores de datos están protegidos con a [redacted]

• Se cuenta, por parte de la Dirección de Administración, con el debido registro, asignación y resguardo de inventario.

• Diariamente se revisan las consolas de monitoreo del antivirus [redacted] lo cual es de alta utilidad para realizar los ajustes necesarios y mantener un nivel de seguridad suficiente.

• Cada usuario cuenta con contraseñas seguras para su acceso tanto para el uso de las computadoras como para los sistemas y el correo electrónico.

• Los usuarios tienen solo los permisos necesarios para realizar sus funciones como trabajadores.

• Los servidores de almacenamiento y bases de datos tienen acceso restringido a usuarios y son monitoreados para verificar su buen funcionamiento y estado de salud.

• El personal de Soporte Técnico configura (sistema operativo, software, antivirus), supervisa y da el mantenimiento necesario a los equipos de cómputo para que estén protegidas de cualquier eventualidad de riesgo informático.

• En cada edificio administrativo se cuenta con un SITE que alberga los servidores en uso. Estos espacios cuentan con acceso restringido y con los dispositivos necesarios para que cuenten con el medio ambiente necesario para su buen funcionamiento.

• Nuestro site de Comunicaciones cuenta con seguridad fisca [redacted]

• Para los servidores se cuenta con procedimientos de respaldo del sistema operativo y bases de datos que se efectúan con regularidad.

• Se cuenta con el soporte técnico de empresas ([redacted] que nos apoyan tanto en las configuraciones necesarias como en los bloqueos necesarios y eventualidades que se presenten.

• Se supervisa y se toman las acciones requeridas para que todos los servidores de datos cuenten con las actualizaciones de seguridad recomendadas por el fabricante (llevamos bitácora de estas funciones)

• Contamos con manuales de procedimiento para acceso al centro de cómputo, asignación de cuentas de usuario y correo electrónico, Políticas de Seguridad, Respaldo de Base de Datos y plan de recuperación en caso de desastres.

SOFTWARE

Controles de Acceso

• Acceso a las Bases de Datos: Estas credenciales serán de uso exclusivo del administrador de bases de datos y de servidores. Se podrán brindar accesos con ciertas limitaciones al grupo de soporte de software o desarrollo si existe.

• Administración acceso de usuarios: Los usuarios de las aplicaciones deberán tener su usuario y contraseña personal e intransferible y se asignarán previa solicitud por soporte de aplicaciones y autorización del jefe inmediato indicando perfil específico para cada aplicación.

Copias de seguridad o respaldos de la información

Para garantizar la seguridad de los datos frente a cualquier eventualidad, es necesario llevar a cabo un proceso preventivo denominado "respaldo" o "backup".

Se realizan respaldos de la base de datos de cada aplicación que se tiene dominio, con una periodicidad mensual en las siguientes ubicaciones:

1.- Dentro del equipo de desarrollo

2.- Dentro del servidor de la aplicación a respaldar

3.- En un disco duro externo.

Medidas de seguridad contra hackeos en las aplicaciones, se tienen las siguientes practicas:

• Buenas prácticas de desarrollo

• Promover el uso de contraseñas seguras para las cuentas de usuario

• Dentro de la Base de Datos las contraseñas son almacenadas de manera seguras por medio de encriptación

• Promover la actualización de los frameworks y herramientas de desarrollo en la medida de lo posible.

8.3 Medidas de Seguridad Físicas.

1. Prevenir el acceso no autorizado al perímetro de la organización

Se cuenta con protocolos de seguridad establecidos cuyo objetivo es prevenir el ingreso no autorizado, a las instalaciones y/o áreas críticas del Organismos, estas medidas de seguridad se dividen en 3 tipos:

Humanos: Se cuenta con Elementos de Seguridad y Vigilancia en las puertas de ingreso a las instalaciones de las Unidades Médicas, Técnicas y Administrativas, estos Elementos están capacitados y orientados a la prevención de ingresos no autorizados. Así mismo, en el interior de las unidades pueden localizarse elementos se seguridad en las puertas de ingreso a áreas críticas de la unidad.

Electrónicos: Se cuenta con sistemas de controles de acceso al interior de las instalaciones, cuyo objetivo es prevenir el ingreso de personal no autorizado a áreas críticas de las unidades, estos sistemas son utilizados mediante tarjetas magnéticas de proximidad o mediante identificación biométrica, huella dactilar.

Físicos: Las áreas críticas, que no cuenten con sistemas electrónicos de control de acceso, cuentas con medidas físicas como el resguardo de la información bajo llave, ya sea mediante archiveros y gavetas, o en general, el cierre de la puerta de ingreso al área con llave.

Medidas de Seguridad en caso de Emergencia

Las instalaciones estratégicas de este Organismo cuentan con Sistemas de Detección de Humo e Incendio, el cual resguarda las áreas estratégicas por medio de detectores de humo y de calor que, al ser activados, emiten una alarma sonora y lumínica, que alerta sobre el siniestro presentado y su lugar de origen.

Así mismo, se cuenta con sistemas y equipos de combate de incendio, tanto electrónicos (Sistema de Rociadores Automáticos o Sprincklers) como manuales (Extinguidores e Hidrantes), que son utilizados durante las emergencias, y cuyo objetivo es sofocar el fuego de manera rápida y eficaz, evitando la propagación del incendio y el aumento del daño, además de ser especiales para el combate de conatos de incendio en aparatos electrónicos y de materiales inflamables.

Sistemas Electrónicos de Seguridad

Otra de las medidas implementadas es el uso de Sistemas de Circuito

Cerrado de Televisión (C.C.T.V.), los cuales son instalados en unidades y áreas críticas de este Organismo, con el objetivo detectar de manera oportuna el ingreso de personal no autorizado a áreas críticas. Estos Sistemas de CCTV se encuentran en funcionamiento 24 horas al día los 365 días del año y fungen como un testigo visual y sonoro de lo ocurrido al interior y perímetro de las instalaciones.

9. El Programa General de Capacitación.

El Comité de Transparencia de este Organismo aprobó el pprograma de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales.

Dicho programa de capacitación contempla temas como:

- Marco Normativo
- Conceptos Básicos
- Derechos ARCO
- Principios de Protección de Datos Personales
- Medias de Seguridad
- Causas de Sanción

Dichas capacitaciones se realizan de manera presencial y a través de medios electrónicos, y; serán implementadas conforme a la carga de trabajo y necesidades de cada una de las unidades administrativas que conforman este Organismo.

10. Actualización del Documento de Seguridad.

El presente Documento de Seguridad se deberá de actualizar cuando ocurran los siguientes supuestos:

- Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
- Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
- Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida;
- Implementación de acciones correctivas y preventivas ante una vulneración de seguridad, y;
- Cuando surjan documentos, formatos, recomendaciones del Órgano Garante para la mejora del presente documento de seguridad.

De conformidad con los artículos 41, 42 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, el presente Documento de Seguridad, fue elaborado por el Director Jurídico, Responsable de la Unidad de Transparencia y Presidente del Comité de Transparencia y aprobado por la Titular del Sujeto Obligado; Monterrey, Nuevo León a los 15-quince días del mes de mayo del año 2024-dos mil veinticuatro.

ELABORÓ

LIC. SERGIO SALVADOR CHAPA VALENCIA
DIRECTOR JURÍDICO DE LOS SERVICIOS DE SALUD DE NUEVO LEÓN, O.P.D., RESPONSABLE DE LA UNIDAD DE TRANSPARENCIA Y PRESIDENTE DEL COMITÉ DE TRANSPARENCIA

AUTORIZÓ

DRA. MED. ALMA ROSA MARROQUÍN ESCAMILLA
DIRECTORA GENERAL DE LOS SERVICIOS DE SALUD DE NUEVO LEÓN, O.P.D.

La presente hoja de firmas corresponde, a la ultima pagina del Documento de Seguridad de Servicios de Salud de Nuevo León, Organismo Público Descentralizado----------