Hospital General "Dr. Manuel Gea González"

DOCUMENTO DE SEGURIDAD

VIGENTE

Glosario

El presente glosario se encuentra acorde a lo descrito en el artículo 3° de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Aviso de privacidad: Documento de forma física, electrónica o en cualquier formato, que es generado por el responsable y puesto a disposición de los titulares de los datos personales, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

Bases de datos: Conjunto ordenado de datos personales bajo criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Comité de Transparencia: Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

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. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones.

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

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: 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.

Evaluación de impacto en la protección de datos personales: Evaluación mediante la cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra

tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable.

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, 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, sus instalaciones físicas, áreas críticas, recursos e información;
b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, 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 las bases de datos o a la información, 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 obligaciones;

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.

Portabilidad de datos personales: Prerrogativa del titular de obtener una copia de los datos que ha proporcionado al responsable del tratamiento en un formato estructurado que le permita seguir utilizándolos.

Programa: Programa de Protección de Datos Personales.

Remisión: Toda comunicación de datos personales realizada exclusivamente entre el responsable y el encargado, dentro o fuera del territorio mexicano.

Responsable: Sujeto obligado de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados que decide sobre el tratamiento de los datos personales.

Revisión: Actividad estructurada, objetiva y documentada, llevada a cabo con la finalidad de constatar el cumplimiento continuo de los contenidos establecidos en este Programa**.**

Riesgo: Combinación de la probabilidad de un evento y su consecuencia desfavorable.

SNT: Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Sujeto obligado: Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del ámbito federal.

Titular: Persona física a quien corresponden los datos personales.

Transferencias: 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 manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Unidad Administrativa: Área a la que se le confieren atribuciones específicas en el Estatuto Orgánico del HGMGG y demás normatividad aplicable.

Unidad de Transparencia: Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública

Acrónimos

HGMGG: Hospital General "Dr. Manuel Gea González".

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

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

LinGPDPPSP: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

SAPPN: Sistema de Administración de Personal y Pago de Nómina.

SIGHO: Sistema Integral de Gestión Hospitalaria.

SEU-GEA: Sistema Electrónico de Urgencias.

RDPAC_CE: Registro Diario de Pacientes de Consulta Externa.

HEXABANK: Sistema de Gestión de Bancos de Sangre, Hemocentros, Servicios de Transfusión y Postas de Donación.

Introducción

El Hospital General Dr. Manuel Gea González, es un organismo descentralizado con personalidad jurídica y patrimonio propio, creado por Decreto del Ejecutivo Federal publicado en el Diario Oficial de la Federación el 26 de julio de 1972, se rige por el Decreto del Hospital General Doctor Manuel Gea González, publicado en el Diario Oficial de la Federación el 22 de agosto de 1988, cuyo objeto primordial es otorgar servicios de salud.

El 26 de enero del 2017 se expidió la LGPDPPSO la cual tiene como objetivo establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales que estén en posesión de los sujetos obligados, de cuyo artículo primero se desprende la calidad de sujeto obligado del HGMGG, al ser una entidad de la Administración Pública Federal que lleva a cabo el tratamiento de datos personales y, por ello, debe observar lo dispuesto por dicho instrumento normativo en el tratamiento de datos personales que lleve a cabo. Asimismo, la LGPDPPSO detalla el alcance y los procedimientos para el ejercicio de los cuatro derechos que el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos reconoce a los titulares de los datos personales: acceso, rectificación, cancelación y oposición (derechos ARCO), y reconoce uno más, el de portabilidad. En ese sentido, el 26 de enero del 2018, se publicaron los Lineamientos Generales de Protección de Datos personales para el Sector Público, derivado de lo anterior, a partir de la publicación de dichos instrumentos jurídicos, el HGMGG, adquirió el carácter de "Responsable" con el deber de tratar dichos datos conforme a los principios (licitud, lealtad, información, consentimiento, finalidad, proporcionalidad, calidad y responsabilidad) y (confidencialidad y seguridad). Estos principios, deberes y derechos imponen una serie de obligaciones para los sujetos regulados por la LGPDPPSO, que tienen como finalidad que el tratamiento se realice de manera tal que se garantice la protección de los datos personales, con el objeto de respetar el derecho a la autodeterminación informativa de los titulares.

En específico, con relación al deber de seguridad, el artículo 31 de la LGPDPPSO señala que el Responsable del tratamiento deberá establecer y mantener 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. Por su parte, el artículo 35 de la LGPDPPSO establece como una obligación la elaboración de un documento de seguridad, que describa y de 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. En ese sentido, en cumplimiento a las obligaciones antes descritas, a continuación, se presenta el documento de seguridad del HGMGG con los elementos informativos que establece la normativa de la materia.

I. Inventario de datos personales y de los sistemas de tratamiento

La LGPDPPSO en sus fracciones I y III del artículo 33 establece la obligación elaboración de contar con un inventario de datos personales y de los sistemas de tratamiento para la implementación de medidas de seguridad para la protección de los datos personales, mismo que forma parte del documento de seguridad; los inventarios de datos personales forman parte integral del presente documento.

Sobre el particular, el HGMGG elaboró los inventarios de los distintos tratamientos de datos personales que realiza, identificando los elementos informativos, basados en el ciclo de vida de cada uno de éstos; de conformidad con lo dispuesto en los artículos 58 y 59 de los LinGPDPPSP de Protección de Datos Personales para el Sector Público.

Área Administrativa o Médica Responsable	**Nombre del Sistema de Tratamiento**	**Inventario de Datos Personales**
1.- Subdirección de Recursos Humanos, a través de sus Departamentos: - Relaciones Laborales - Remuneraciones e Incidencias. - Departamento de Empleo y Capacitación - Departamento de Análisis y Programación. 2.- Departamento de Administración y Desarrollo de Sistemas (administrador del SAPPN).	**Sistema Electrónico:** Sistema de Administración de Personal y Pago de Nómina (SAPPN) **Sistemas Físicos:** Expedientes de Personal. Candidatos de Nuevo Ingreso Control de Asistencia Área de Checadores Contratos de personal Constancias de personal Plantillas de personal	Datos de identificación, datos patrimoniales, datos laborales, datos ideológicos, origen étnico. R.F.C. CURP, Deducciones, domicilio particular, teléfono o celular, RFC, CURP, edad, estado civil, sexo, cuenta bancaria, nacionalidad, No. de seguridad social, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, datos escolares: Nivel de Estudios, Cédula Profesional, datos de salud, datos sobre procedimientos administrativos seguidos en forma de juicio y/o jurisdiccionales, resultados de evaluación psicométrica.
Departamento de Admisión y Archivo Clínico	**Sistema Físico:** Sistema de Expediente Clínico	Nombre, domicilio, teléfono, estado civil, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad. características físicas: estatura, peso, complexión. vida sexual: preferencias sexuales, vida sexual. Datos patrimoniales: bienes muebles e inmuebles, ingresos y egresos.

		características personales: tipo de sangre, huella digital. Datos de salud: estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, discapacidades, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos. Datos laborales: puesto actual, domicilio, teléfono, y trabajos anteriores.
Departamento de Administración y Desarrollo de Sistemas y los Servicios de Urgencias Adultos, Ginecología y Pediatría	Sistema de Información para la Gerencia Hospitalaria	Datos de Identificación: Nombre, domicilio, teléfono particular, estado civil, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios. Características Físicas: estatura, peso. Características Personales: Tipo de sangre. Datos Ideológicos: creencia religiosa. Datos Patrimoniales: bienes muebles e inmuebles, ingresos y egresos. Datos de Salud: estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, discapacidades, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas y uso de aparatos oftalmológicos, ortopédicos, auditivos, entre otros (anteojos, aparatos de oído, prótesis, etc.).
Departamento de Administración y Desarrollo de Sistemas, las Áreas Médicas de Urgencias y la División de Bioestadística	**Sistema Electrónico:** Sistema Electrónico de Urgencias (SEU_GEA)	Datos de Identificación: Nombre, domicilio, teléfono particular, estado civil, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y

		beneficiarios. Características Físicas: estatura, peso. Características Personales: Tipo de sangre. Datos Ideológicos: creencia religiosa. Datos Patrimoniales: bienes muebles e inmuebles, ingresos y egresos. Datos de Salud: estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, discapacidades, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas y uso de aparatos oftalmológicos, ortopédicos, auditivos, entre otros (anteojos, aparatos de oído, prótesis, etc.).
Departamento de Administración y Desarrollo de Sistemas y los Servicios de Consulta Externa	**Sistema Electrónico** Registro Diario de Pacientes de Consulta Externa (RDPAC_CE)	Datos de Identificación: Nombre, domicilio, teléfono particular, estado civil, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios. Características Físicas: estatura, peso. Características Personales: Tipo de sangre. Datos Ideológicos: creencia religiosa. Datos Patrimoniales: bienes muebles e inmuebles, ingresos y egresos. Datos de Salud: estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, discapacidades, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas y uso de aparatos oftalmológicos, ortopédicos, auditivos, entre otros (anteojos, aparatos de oído, prótesis, etc.).

Dirección de Enseñanza e Investigación a través de sus Divisiones: - División de Enseñanza y Pregrado - División de Enseñanza y Posgrado	**Sistemas Físicos:** - Expedientes de alumnos pregrado ciclos clínicos. - Expediente de Médicos Internos de pregrado. - Expediente de Médicos Pasantes en Servicio Social en Vinculación. - Expedientes de médicos pasantes en servicio social en Modalidad de Investigación. - Expedientes de alumnos de especialidad y posgrado	Nombre, edad, nacionalidad, Clave única de Registro de Población, Registro Federal de Contribuyentes, domicilio, número de celular, teléfono particular, correo electrónico, notificación en caso de urgencia, firma, INE, Comprobante de domicilio, fotografías, Edad, Estado civil, Correo electrónico personal, Información de su contacto para casos de urgencia (Nombre, Parentesco, Teléfono), Acta de nacimiento, Firma, Forma FM3 (en caso de los extranjeros), Constancia del ENARM, Certificado de salud, Examen psicométrico.
Servicios de Medicina Transfusional	Sistema Electrónico: HEXABANK (Donadores) HEXABANK (Banco de sangre, Torre)	Elaboración de Historia Clínica de donadores con signos vitales, antecedentes personales, exposición a condiciones de riesgo, antecedentes, gineco-obstetras, exploración física. Nombre del donador, fecha de nacimiento, sexo, edad, domicilio, teléfono, delegación, colonia, C.P., escolaridad, ocupación, tipo de donación, Nombre del paciente por quien viene a donar, parentesco, servicio, N° de cama, N° de expediente, diagnóstico, Médico tratante. Solicitud de Hemocomponentes: Nombre del paciente, fecha de nacimiento, grupo y RH, servicio, edad, sexo, N° de cama, Número de expediente, diagnóstico.
Departamento de Tesorería	**Sistema Electrónico:** Sistema Integral de Gestión Hospitalaria (SIGHO)	Nombre completo, edad, sexo, fecha de nacimiento, lugar de nacimiento, nacionalidad, domicilio completo, teléfono fijo

Departamento de Administración y Desarrollo de Sistemas Departamento de Trabajo Social. Áreas Médicas	Módulos: Trabajo social Agenda electrónica Cajas Administración hospitalaria	y móvil, correo electrónico, número de identificación oficial (INE), Clave Única de Registro de Población (CURP), estatus de Afiliación y Número de Seguridad Social, de cualquier Institución de Derecho habiencia, a la cual se encuentre afiliado, estado civil, datos familiares (hijos, padres, hermanos), religión, origen racial, escolaridad, ocupación, aficiones y estilo de vida, datos socioeconómicos, ingresos económicos, egresos económicos, datos académicos y profesionales, puesto de trabajo y detalles de empleo, antecedentes heredo-familiares, información relacionada con su ambiente familiar, vivienda, hábitos alimenticios, higiene, consumo de sustancias como alcohol, tabaco o drogas, actividad física, sueño, antecedentes personales patológicos, antecedentes personales quirúrgicos, antecedentes perinatales, antecedentes gineco-obstétricos, antecedentes andrológicos, condición sicológica y/o psiquiátrica, y tratamientos médicos utilizados.

II. Funciones y obligaciones de las personas que traten datos personales

En cumplimiento a la fracción II del artículo 33 de la LGPDPPSO, el HGMGG, identifica las funciones y obligaciones del personal que lleva a cabo el tratamiento de datos personales de la siguiente manera:

1. Atendiendo lo dispuesto en la LGPDPPSO y los LinGPDPPSP, mismos que se encuentran asociados con cada una de las áreas responsables de su cumplimiento.

2. Atendiendo a los servidores públicos que realizan el tratamiento, área a la cual se encuentra adscrito y finalidad de dicho tratamiento.

El HGMGG cuenta con roles y funciones del personal con respecto al tratamiento y protección de los datos personales, los cuales se describen en el presente apartado de manera general y

particular, con independencia de que el inventario de datos personales funja como una bitácora donde quedan establecidos los responsables, encargados y usuarios de los datos personales.

Cabe señalar que el Comité de Transparencia, es el área responsable de dar a conocer a los servidores públicos del HGMGG el Programa de Protección de Datos Personales, a fin de que el personal conozca sus funciones las cuales se encuentran definidas en la legislación y normatividad que rige el actuar del Hospital, por lo cual, para efectos del presente documento de seguridad, el marco normativo de referencia se encuentra establecido en el Manual de Organización Específico del Hospital General "Dr. Manuel Gea González". En ese sentido, resulta importante señalar que la legislación y normatividad aplicable al HGMGG que define las atribuciones, responsabilidades, autoridades, funciones y obligaciones al interior de la organización, se encuentra disponible de manera actualizada en el apartado Normatividad de la Plataforma Nacional de Transparencia disponible en el vínculo siguiente: https://consultapublicamx.inai.org.mx/vut-web/?method=post&idSujetoObigadoParametro=152&idEntidadParametro=33&idSectorParametro=21. Adicionalmente, a fin de identificar la relación de las funciones por unidades administrativas del HGMGG y el marco normativo aplicable a dicha gestión, deberá consultarse en el apartado de normatividad de la página del HGMGG, o directamente en el vínculo siguiente: http://www.hospitalgea.salud.gob.mx/contenido/menu/normatividad/normateca.html.

III, IV y V. Análisis de riesgos, Análisis de brecha y Plan de Trabajo

Dentro de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el análisis de riesgo, análisis de brecha y plan de trabajo, forman parte del documento de seguridad del HGMGG de conformidad con lo dispuesto en los artículos 32, 35 fracciones IV, V y V de la LGPDPPSO así como 60, 61 y 62 de los LinGPDPPSP.

Análisis de riesgo

Al efecto, el análisis de riesgo realizado por el HGMGG, prevé aquellos atinentes a:

1) Infraestructura tecnológica (software y hardware),
2) Hábitos de seguridad del personal,
3) Inventarios de tratamiento de datos personales y
4) Cumplimiento de obligaciones normativas en materia de datos personales.

En ese sentido, el cumplimiento previsto en los artículos 33 fracción IV de la LGPDPPSO así como 60 de los LinGPDPPSP, se prevé de la siguiente manera:

ELEMENTO REQUERIDO	FUENTE
Amenazas y vulnerabilidades existentes. Art. 33, fracción IV, de la LGPDPPSO	- Infraestructura tecnológica; - Hábitos de seguridad del personal; - Inventarios de tratamientos de datos personales, y - Cumplimiento de obligaciones normativas en materia de datos personales.
Recursos involucrados en el tratamiento de datos personales. Art. 33, fracción IV, de la LGPDPPSO	- Infraestructura tecnológica - Inventarios de tratamientos de datos personales.
Requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico. Art. 60, fracción I, de los LinGPDPPSP	- Cumplimiento de obligaciones normativas en materia de datos personales.
El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida. Art. 60, fracción II, de los LinGPDPPSP	- Inventarios de tratamientos de datos personales.
El valor y exposición de los activos involucrados en el tratamiento de los datos personales Art. 60, fracción III, de los LinGPDPPSP	- Hábitos de seguridad del personal.
Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida. Art. 60, fracción IV, de los LinGPDPPSP	- Ponderación de riesgos.
El riesgo inherente a los datos personales tratados. Art. 32, fracción I, de la LGPDPPSO	- Inventarios de tratamientos de datos personales.
La sensibilidad de los datos personales tratados. Art. 32, fracción II, de la LGPDPPSO	- Inventarios de tratamientos de datos personales.
El desarrollo tecnológico. Art. 32, fracción III, de la LGPDPPSO	- Infraestructura tecnológica.
Las posibles consecuencias de una vulneración para los titulares. Art. 32, fracción IV, de la LGPDPPSO.	- Ponderación de riesgos.
Las transferencias de datos personales que se realicen. Art. 32, fracción V, de la LGPDPPSO	- Inventarios de tratamientos de datos personales.
El número de titulares.	- Ponderación de riesgos.

Art. 32, fracción VI, de la LGPDPPSO	
Las vulneraciones previas ocurridas en los sistemas de tratamiento. Art. 32, fracción VII, de la LGPDPPSO	- Reportes de vulneraciones al Comité de Transparencia.
El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión. Art. 32, fracción VIII, de la LGPDPPSO	- Ponderación de riesgos.

Con la finalidad de identificar los riesgos inherentes al tratamiento de datos personales así como el establecimiento de controles de seguridad, el HGMGG lleva a cabo el siguiente procedimiento:

A. Se analizan los posibles riesgos existentes a través de implementación de la matriz de riesgos por la que se analizan y evalúan los posibles riesgos al tratamiento de datos personales en cada una de las áreas administrativas, así como el cumplimiento a la normativa en materia de datos personales.

B. Detectadas las posibles vulnerabilidades y amenazas, la unidad administrativa establece controles de seguridad preventivos y en su caso correctivos a fin de mitigar las mismas.

C. Se efectúa un análisis de brecha que permita identificar y definir actividades de control preventivas y en su caso correctivas que sean necesarias.

D. La unidad administrativa responsable, realiza una ponderación de los riesgos a fin de determinar y priorizar las medidas de seguridad a implementar, tomando en cuenta las consecuencias de una probable vulneración, así como el probable riesgo al tratamiento de datos personales.

E. Se elabora un plan de trabajo en el cual se establecen las medidas de seguridad faltante, las actividades a desarrollar y el plazo de cumplimiento.

Las evidencias de la implementación de los análisis forman parte de los elementos que brindan el contexto para la identificación de los riesgos, basado en las etapas siguientes:

1. Contexto de la organización (basado en los elementos factores previstos por el artículo 32 de la LGPDPPSO).
2. Identificación del riesgo.
3. Análisis del riesgo.
4. Administración del riesgo.

5. Tratamiento del riesgo.

Análisis cuyos resultados se implementan para la mejora en los mecanismos de monitoreo y seguimiento de las medidas de seguridad, o en su defecto, se incorporan dentro del Plan de Trabajo.

El análisis de riesgos se realiza cuando menos una vez cada dos años de manera general, tomando en consideración de manera genérica todos los tratamientos de datos personales. No obstante, las unidades administrativas pueden realizar análisis de riesgos sobre sus propios tratamientos, los cuales son susceptibles de ser reconocidos como parte integrante del presente documento de seguridad.

Análisis de brecha

Para efectos del presente documento, el análisis de brecha solamente comprenderá los riesgos que conforme el análisis realizado sea necesario tratar, así como aquellos otros supuestos que, en términos de la LGPDPPSO se requiera dicho análisis.

En ese sentido, a fin de cubrir con los requerimientos previstos por el artículo 61 de los LinGPDPPSP, para la realización del análisis de brecha se deberán considerar las medidas de seguridad existentes y efectivas; las medidas de seguridad faltantes, y la existencia de nuevas medidas de seguridad que pudieran reemplazar a uno o más controles implementados actualmente; en el que se identifican los siguientes elementos:

- Confirmación de la existencia de la brecha.
- Confirmación de que la brecha es gestionable, o en su caso, que se han implementado acciones para su contención.
- Identificación de alternativas de corto plazo para su atención.
- Elaboración de un cronograma que defina las principales actividades, resultados y responsables para que la brecha pueda ser atendida.

Plan de Trabajo

El plan de trabajo define las principales acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer. Lo anterior, considerando los recursos asignados; el personal interno y externo en su organización y las fechas de compromiso para la implementación de las medidas de seguridad nuevas o faltantes.

No obstante, dentro del Plan de Trabajo también podrá agregarse cualquier actividad que resulte como requisito para la mejora institucional que se traduzca de manera directa o indirecta en la protección de datos personales.

VI. Mecanismos de monitoreo y revisión de las medidas de seguridad

Mecanismos de monitoreo

En cumplimiento a lo previsto en el artículo 35 fracción VI de la LGPDPPSO y 63 de sus LinGPDPPSP, el HGMGG lleva a cabo la revisión del cumplimiento de la normatividad interna relacionada con el tratamiento de datos personales.

Para tal efecto, de conformidad con el Plan de Trabajo establecido, cada una de las unidades administrativas, deberán remitir la evidencia que sustente las acciones realizadas para su cumplimiento en el mes de noviembre, a efecto de informar dichos avances al Comité de Transparencia tales como:

1. Revisar y en su caso actualizar los procesos involucrados en el tratamiento de datos personales.
2. Revisar y en su caso actualizar los avisos de privacidad, funciones y obligaciones del personal y los inventarios de datos personales, según corresponda.
3. Evaluar si hubo cambios en las amenazas, vulnerabilidades o impacto de los riesgos relacionados con las modificaciones a la normativa, para actualizar los análisis de riesgos, análisis de brecha y plan de trabajo.
4. Revisar y en su caso adecuar los sistemas de tratamiento para cumplir con los cambios normativos.
5. Monitoreo del entorno físico (personal de vigilancia, control de acceso, control de asistencia, circuito cerrado, según corresponda).
6. Monitoreo del entorno electrónico (verificaciones área informática).
7. Actualización del plan de trabajo.
8. Revisión de avances del plan de trabajo.
9. Actualización de tecnología.
10. Vulneraciones a la seguridad de datos personales.

Para tales efectos, cada unidad administrativa define las medidas de seguridad en atención a las responsabilidades y autoridades inherentes a cada puesto, y, los elementos establecidos previamente constituyen controles generales adicionales a los ya implementados por cada una de las áreas administrativas.

No obstante, cuando derivado de los resultados del análisis de riesgos, del análisis de brecha y del plan de trabajo reconocidos en el presente documento de seguridad se desprendan actividades o compromisos específicos, la unidad de transparencia dará seguimiento a cada uno de los compromisos reconocidos. Adicionalmente, con independencia de lo establecido por el presente documento de seguridad, se podrá establecer un periodo de un año para la

evaluación y actualización del documento de seguridad, periodo durante el cual, se mantendrá vigente la versión disponible.

Las mejoras y actualizaciones del documento de seguridad deberán ser comunicadas a todo el personal del HGMGG dentro de los 6 meses siguientes a que sea presentado ante el Comité de Transparencia.

Mecanismos de supervisión o revisión

Actualmente no se han llevado a cabo auditorías específicas en materia de protección de datos personales a los tratamientos del HGMGG. Al respecto, se prevé la realización de una auditoría anual ya sea por terceros según la disponibilidad presupuestal, por solicitud al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales o bien, por personal del HGMGG.

El programa anual de auditoría, así como la realización de las mismas, será determinado por el Comité de Transparencia en el Programa de Protección de Datos Personales del HGMGG, conforme a los términos de referencia que se determinen para tal efecto dentro de la institución que podrán tomar como referencia el procedimiento de auditorías voluntarias por parte del INAI, sin perjuicio que, de considerarse conveniente en el marco de la mejora institucional, se solicite ante dicho Instituto la práctica de dicho ejercicio.

VII. Programa general de capacitación

Con relación al programa de capacitación, la fracción VIII del artículo 33 de la LGPDPPSO señala que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

En ese sentido, de acuerdo con la fracción VII del artículo 35 de la LGPDPPSO, el programa de capacitación forma parte del documento de seguridad, el cual se encuentra previsto de conformidad con las acciones previstas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, así como la propuesta de capacitación definida por las unidades administrativas que integran el HGMGG.

En tal entendido, en el diseño e implementación del programa de capacitación, se toma en cuenta lo siguiente:

I. Los requerimientos y actualizaciones del sistema de gestión;
II. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;

III. Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y
IV. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

En el caso particular del HGMGG, el desarrollo del programa de capacitación está a cargo de la Unidad de Transparencia, el cual deberá ser revisado y reestructurado periódicamente, de manera anual, cuyos objetivos principales son los siguientes:

- La participación y acreditación de los involucrados en los tratamientos de datos personales, en los cursos de capacitación ofertados por el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI).

- La detección de necesidades de capacitación en materia de protección de datos personales al interior del HGMGG.

- La identificación de aquellas necesidades de capacitación derivadas de los análisis de riesgos y de brecha que impacten en la protección de datos personales.

En tal entendido, el Programa General de Capacitación del HGMGG, se establece a través de este apartado con el objetivo general que se señala a continuación:

Objetivos de Capacitación

El personal que integra el HGMGG deberá estar capacitado en su totalidad en materia de protección de datos personales en posesión de sujetos obligados conforme a los criterios siguientes:

- Todas las personas servidoras públicas de este Sujeto Obligado, desde el nivel de Jefatura de Departamento y División, hasta el Director General, deberán acreditar los cursos de Introducción a la Ley Federal de Transparencia y Acceso a la Información Pública, Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados e Introducción a la Ley General de Archivos.

- El personal operativo será capacitado de acuerdo a las necesidades señaladas por el titular de cada unidad administrativa.

Actualización del documento de seguridad

En cumplimiento a lo dispuesto por el artículo 36 de la LGPDPPSO, se establece la actualización del presente documento, cuando se lleve a cabo la creación de un nuevo sistema o base de datos que implique el tratamiento de datos personales, el titular de la unidad administrativa

deberá dar aviso por escrito al titular de la Unidad de Transparencia, así como remitir la información correspondiente para su inclusión en el Inventario del Sistema de Tratamiento de Datos del HGMGG. Aunado a lo anterior, el HGMGG, determinará la actualización del presente documento de conformidad con las herramientas metodológicas emitidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Cabe señalar que una vez que sufra alguna actualización el presente Documento de Seguridad, la misma será sometida a consideración y aprobación del Comité de Transparencia del HGMGG.

En la Ciudad de México a los cinco días del mes julio del año 2022, los miembros Integrantes del Comité de Transparencia del Hospital General "Doctor Manuel Gea González", en la Quinta Sesión Extraordinaria 2022, de dicho Órgano, aprobaron por unanimidad el presente Documento de Seguridad, y se instruye a su publicación en el apartado de Protección de Datos Personales en la página web de este Hospital General. Conste. ----------
-

LIC. ANA ELENA HERNÁNDEZ RESÉNDIZ
SUBDIRECTORA DE ASUNTOS JURÍDICOS, TITULAR DE LA UNIDAD DE TRANSPARENCIA Y PRESIDENTA DEL COMITÉ DE TRANSPARENCIA

LIC. PATRICIA CARRANZA ARMIJO
TITULAR DEL ÓRGANO INTERNO DE CONTROL EN EL HOSPITAL GENERAL "DOCTOR MANUEL GEA GONZÁLEZ"

LIC. JUAN CARLOS ALEJANDRO MOURET RAMÍREZ
RESPONSABLE DEL ÁREA COORDINADORA DE ARCHIVOS DEL HOSPITAL GENERAL "DOCTOR MANUEL GEA GONZÁLEZ"

VIGENTE