DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES

SECRETARÍA DE RELACIONES EXTERIORES

Subsecretaría de Relaciones Exteriores

SRE
SECRETARÍA DE RELACIONES EXTERIORES

Contenido

Considerandos 3

Definiciones 5

I. Inventario de datos personales y de los sistemas de tratamiento y funciones y obligaciones de las personas que traten datos personales 8

II. Análisis de riesgos y análisis de brecha 13

III. Gestión del SGSI 15

IV. Medidas de seguridad 18

V. Plan de trabajo y mecanismos de monitoreo y revisión de las medidas de seguridad .. 28

VI. Programa de capacitación 32

Marco normativo 33

Considerandos

Que la protección de los datos personales es un derecho humano consagrado en los artículos 6, base A y 16, segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos.

Que todas las disposiciones de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) son de aplicación y observancia directa para los sujetos obligados pertenecientes al orden federal.

Que entre los objetivos de la LGPDPPSO se encuentra garantizar la observancia de los principios de protección de datos personales, proteger los datos personales en posesión de cualquier autoridad, así como promover, fomentar y difundir una cultura de protección de datos personales.

Que la LGPDPPSO define el documento de seguridad como el 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.

Que como parte del ejercicio de las facultades de la Subsecretaría de Relaciones Exteriores, señaladas en el artículo 8 del Reglamento Interior de la Secretaría de Relaciones Exteriores, se lleva a cabo el tratamiento de datos personales que permiten contar con insumos para las acciones destinadas a coordinar la participación en la Reunión de Cumbre de Jóvenes *Youth 20* del G20.

Que la Dirección General de Bienes Inmuebles y Recursos Materiales (DGBIRM) tiene entre sus funciones desarrollar los programas de seguridad institucional para salvaguardar la integridad del personal de la SRE, las instalaciones y bienes propiedad de este, de conformidad con el artículo 34 del Reglamento Interior de la Secretaría de Relaciones Exteriores.

Que la Dirección General de Tecnologías de la Información e Innovación (DGTII) instrumenta y vigila los recursos de infraestructura de informática y

telecomunicaciones dentro de un margen de seguridad acorde con los estándares internacionales en el manejo de la información, conforme a lo establecido en el artículo 36 del Reglamento Interior de la Secretaría de Relaciones Exteriores.

Que la Unidad de Transparencia (UDT) tiene entre sus facultades asesorar a las unidades administrativas de la Secretaría en materia de protección de datos personales, conforme a lo señalado en el artículo 85 de la LGPDPPSO.

Que por lo antes expuesto, la Subsecretaría de Relaciones Exteriores, en colaboración con la DGBIRM, la DGTII y la UDT elaboró el presente documento de seguridad.

Definiciones

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.

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 políticas y preferencia sexual.

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.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

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 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: Los sujetos obligados del ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial,

órganos autónomos, partidos políticos, fideicomisos y fondos públicos, a que se refiere el artículo 1 de la Ley que deciden sobre el 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 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.

I. Inventario de datos personales y de los sistemas de tratamiento y funciones y obligaciones de las personas que traten datos personales

La información puede ser extraída de la ficha para la generación de avisos de privacidad

Trámite 1.

A) Participación de México en la Cumbre de Jóvenes del "Youth 20".

B) Fundamento legal: Artículo 8, fracción III del Reglamento Interior de la Secretaría de Relaciones Exteriores.

C) Finalidad con que se recaban los datos personales. La Cumbre de Jóvenes *Youth 20* del G20 está abierta a un número limitado de participantes por país miembro del G20. Los datos que se recaban tienen como objetivo verificar que el participante cumple los requisitos previstos por el Comité Organizador del país sede del G20, así como proporcionarle información sobre la Cumbre y los arreglos logísticos

- Identificar al participante
- Verificar que cumple con el límite de edad requerida para participar en Cumbre de Jóvenes *Youth 2*0 del G20
- Verificar la nacionalidad mexicana del candidato a participar en Cumbre de Jóvenes en representación de México
- Contar con el número de una identificación oficial vigente y verificar la identidad de la persona que desea participar en Cumbre de Jóvenes
- Es requisito para participar en Cumbre de Jóvenes ser estudiante universitario o haber concluido una licenciatura o un posgrado

D) Datos personales recabados derivados del trámite y la finalidad con la que se recaba cada uno de los mismos. (Enlistar cada uno de los datos personales)

Datos personales recabados derivados del trámite
Nombre
Edad
Nacionalidad
Acta de nacimiento
Identificación oficial
Comprobante de estudios
Número de teléfono
Correo electrónico

Por ejemplo[1]:

- Datos de identificación: nombre, domicilio, teléfono particular, teléfono celular, correo electrónico particular, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros.
- Datos laborales: documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros (existen excepciones tratándose de servidores públicos).
- Datos patrimoniales: bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros,

[1] Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales publicadas por el Instituto Federal de Acceso a la Información Pública, ahora Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

afores, fianzas, servicios contratados, referencias personales, entre otros.

- Datos sobre procedimientos administrativos seguidos en forma de juicio y/o jurisdiccionales: información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.
- Datos académicos: trayectoria educativa, títulos, certificados y reconocimientos, entre otros (existen excepciones tratándose de servidores públicos).
- Tránsito y movimientos migratorios: información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.
- Datos ideológicos (datos personales sensibles): creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros.
- Datos de salud (datos personales sensibles): estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, entre otros.
- Características personales: tipo de sangre, ADN, huella digital, u otros análogos.
- Características físicas: color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros.
- Vida sexual (datos personales sensibles): Preferencia sexual, hábitos sexuales, entre otros.
- Origen (datos personales sensibles): étnico y racial.

E) Personal participante en el tratamiento de datos personales

1. Cargo del personal que participa en el tratamiento de los datos personales en la unidad administrativa

   Asesor en la Subsecretaría de Relaciones Exteriores

2. Funciones de la persona que trata datos personales (en relación con el trámite)
   - Recopilación de datos personales
   - Integración de base de datos
   - Transmisión de datos a comité organizador del país sede de la Cumbre de Jóvenes Youth 20 del G20

3. Obligaciones de la persona que trata datos personales (en relación con el trámite)

   - Tratar los datos personales para la finalidad con la que fueron recabados y de conformidad con las atribuciones conferidas en la normatividad aplicable.
   - Evitar obtener y tratar datos personales a través de medios engañosos o fraudulentos.
   - Garantizar la confidencialidad de los datos personales.
   - Evitar que terceros no autorizados tengan acceso a las bases de datos personales recabados.

   Ejemplo:

- Tratar los datos personales para la finalidad con la que fueron recabados y de conformidad con las atribuciones conferidas en la normatividad aplicable.
- Evitar obtener y tratar datos personales a través de medios engañosos o fraudulentos.

- Garantizar la confidencialidad de los datos personales evitando la difusión de los mismos.
- Evitar que terceros no autorizados tengan acceso a los expedientes o bases de datos.
- Mantener los expedientes de datos personales actualizados a fin de garantizar la integralidad y disponibilidad de los mismos.

Para el caso de la Dirección General de Servicios Consulares y la Dirección General de Delegaciones se deberá incluir las obligaciones de supervisión de los servicios externos contratados en relación con el tratamiento de los datos personales (Servicios de Call Center o similares), se recomienda revisar el artículo 59 de la LGPDPPSO.

Nota: se deberá enlistar a cada uno de los servidores públicos que participan en el tratamiento de los datos personales.

A) Personal participante en el tratamiento de datos personales

1. Cargo del personal que participa en el tratamiento de los datos personales en la unidad administrativa

2. Funciones de la persona que trata datos personales (en relación con el trámite)

3. Obligaciones de la persona que trata datos personales (en relación con el trámite)

Nota: se deberá enlistar a cada uno de los servidores públicos que participan en el tratamiento de los datos personales.

II. Análisis de riesgos y análisis de brecha

Política del Sistema de Gestión de Seguridad de la Información

Respecto a la política de Seguridad de Información, en la Secretaría de Relaciones Exteriores (SRE) se cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI), dentro del Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y Seguridad de la Información (MAAGTICSI) que ha sido establecido para poder asegurar que todas las actividades relacionadas a la información que gestiona la DGTII, cumplan con los requisitos de los usuarios, requisitos legales y demás establecidos por la propia dependencia, que permita en todo momento conservar la Confidencialidad, Integridad y Disponibilidad de la Información.

Objetivos de la seguridad de la información

Los objetivos a cumplir para la seguridad de la información son los siguientes:

CONFIDENCIALIDAD: que sea accesible solamente a aquellos que tengan autorización a su acceso.

INTEGRIDAD: que asegure precisión y exactitud en su contenido y en sus métodos de procesamiento.

DISPONIBILIDAD: que asegure que los usuarios autorizados tengan acceso a ella y a sus activos asociados, cuando sea requerido (Continuidad de la Operación).

CUMPLIMIENTO A LA NORMATIVIDAD: que los requerimientos de la normatividad aplicable en temas de Seguridad de Información, sea cubierta.

Descripción del Sistema de Gestión de Seguridad de la Información

Se cuenta con el Sistema de Gestión de Seguridad de la Información basado en las disposiciones del MAAGTICSI, con el objetivo de asegurar la efectividad y confiabilidad de todas las actividades. El alcance del sistema es el siguiente:

Es aplicable para todas las instalaciones de la SRE en territorio nacional y las representaciones de México en el exterior (Embajadas y Consulados). Lo anterior para todos los servicios y sistemas tecnológicos que la DGTII provee a las distintas áreas de la SRE.

El SGSI cubre los siguientes requisitos:

Análisis de Riesgos

Se cuenta con la Metodología de Análisis de Riesgo basada en el MAAGTICSI que consiste en:

a) Identificación de infraestructuras de información, esenciales y/o críticas.
b) Amenazas a dichas infraestructuras.
c) Análisis de Probabilidad e Impacto.
d) Definición de Riesgo Inicial y Residual.
e) Plan de Tratamiento de Riesgo.

Lo anterior permite la identificación de los riesgos más críticos a los activos sustanciales de la DGTII, y generar las acciones para mitigarlos, transferirlos, minimizarlos y/o eliminarlos.

Una vez ejecutada la metodología de análisis de riesgos se procede a la fase de análisis con las Direcciones Generales Adjuntas de la DGTII, para evaluar la necesidad de activar los controles de los procesos necesarios.

Análisis de Brecha

La SRE cuenta con un Sistema de Gestión de Seguridad de la Información que tiene por objetivo asegurar la efectividad y confiabilidad de todas las actividades relacionadas con los servicios que se brindan a los ciudadanos mexicanos.

El sistema está constituido para el análisis de brecha que lleve al mejoramiento del mismo sistema.

III. Gestión del SGSI

1.- Compromiso de la SRE. Se ha definido que los comités de Grupo de Estudios sobre Seguridad Internacional (GESI), Equipo de Trabajo de Análisis de Riesgo (ETAR) y Equipo de Respuesta a Incidentes de Seguridad en TIC (ERISC), son foros a nivel directivo que se reúne y evalúa, periódicamente, las siguientes actividades:

- Evaluar que el Sistema de Gestión de Seguridad de la Información, en todo momento cumpla con los ordenamientos jurídicos aplicables a la SRE.
- Revisar y evaluar los riesgos más importantes sobre los activos de información, apoyado en todo momento por cada miembro de la SRE, así como cada incidente que se reporte sobre el aspecto de Seguridad de la Información.
- Evaluar y promover los cambios necesarios en el Sistema de Gestión de Seguridad de la Información, con el objeto de avanzar en la mejora continua del Sistema.
- El coordinador y responsable de estas actividades, es la DGTII.

2.- Coordinación de la seguridad de la información. Se define en el MAAGTICSI, que la DGTII es la coordinadora en cuanto a seguridad tecnológica para la SRE, la cual validará la aplicación adecuada de los temas de seguridad de la información.

3.- Asignación de responsabilidades para la seguridad de la información. La definición de responsabilidades hacia la seguridad de la Información, es compartida por todos y cada uno de los miembros de la SRE. Los lineamientos generales sobre seguridad para todo el personal están definidos en los siguientes documentos:

- Lineamientos de Seguridad Informática.
- Documentos del MAAGTICSI, Proceso de Administración de la Seguridad de la Información (ASI) y del Proceso de Operación de Controles de Seguridad de la Información y del ERISC (OPEC)

Todas las descripciones de puesto, incluyen una responsabilidad general del empleado (puesto), hacia la seguridad de la información. De manera más específica, se detallan en la descripción de cada puesto, actividades orientadas a la seguridad de la información.

Finalmente, en el documento de *Lineamientos de Seguridad Informática,* se establecen responsabilidades macro de seguridad informática para todas las áreas de la SRE, mismas que deben de ser atendidos y ampliados por sus respectivas Direcciones Generales.

4.- Compromisos de confidencialidad. Los compromisos de confidencialidad necesarios para la protección de la información, están reflejados en los contratos de empleados y proveedores en la SRE, así como en los perfiles de puesto debidamente aceptados y firmados por cada empleado.

5.- Contacto con las autoridades. Es responsabilidad de la SRE establecer los mecanismos que permitan el contacto e intercambio de recomendaciones con las áreas afines de Tecnología de las Secretarías del ámbito Federal. Lo anterior tendrá como fin homologar los canales de comunicación, difusión y de lineamientos que las Áreas Tecnológicas de estas Secretarías implantan para el cumplimiento de las normas vigentes en temas relacionados con la seguridad de la información.

Para la firma de convenios de colaboración entre otras dependencias y la SRE, la DGTII funge como participante de los mismos en los aspectos técnicos, y la formalización de estos convenios es realizada exclusivamente por las áreas sustantivas de la SRE. Las áreas sustantivas de la SRE que firmen los convenios de colaboración deberán de definir canales seguros y una trazabilidad de información emanada de estos convenios.

6.- Contacto con grupos especiales de interés. Las actividades de la SRE, requieren del contacto con diversas entidades, tanto proveedores, cuerpos regulatorios, usuarios y diversas representaciones, para lograr un control efectivo de estas actividades.

IV. Medidas de seguridad

a) Medidas técnicas

- Control Antivirus: se cuenta con una solución cliente-servidor que protege a los equipos (Laptop, PC y Servidores), de malware en la red a nivel nacional. Combina una protección avanzada contra amenazas de forma proactiva, para asegurar los equipos de ataques conocidos y amenazas desconocidas.
- Control Antivirus – Exterior (nube): la solución en la nube con que cuenta esta Secretaría, brinda protección contra la propagación de código malicioso en la red y acceso no autorizado a recursos de sistema, además cuenta con la capacidad de detener malware, virus, gusanos, troyanos y spyware. Así mismo, previene los ataques de seguridad por malware desconocido, evita los intrusos y ataques antes de que lleguen a los equipos en las representaciones del exterior.
- Control Filtrado de Contenido Web: se cuenta con una solución en la nube, la cual proporciona herramientas para la protección de amenazas y análisis en tiempo real, obteniendo protección para cada usuario (antivirus).
- Control Firewall perimetral: la solución de Firewall (FW) con que cuenta la Secretaría, proporciona análisis puntual de los estados de las comunicaciones y aplicaciones, para controlar el flujo de tráfico que ingresa/sale a/desde las redes de ésta, lo anterior se realiza por medio de reglas puntuales por cada servicio, controlando los diversos orígenes y destinos.
- Control de Correlación: la solución proporciona visibilidad en tiempo real que suministra información procesable e integraciones para priorizar, investigar y responder a las amenazas o la neutralización de los problemas de seguridad.
- Control de Acceso Remoto seguro: la solución provee a usuarios, entidades del exterior o terceros, acceso remoto seguro a las aplicaciones, sistemas y servidores a través de la implementación de túneles.

- Control de Monitor de la Infraestructura: la aplicación de monitoreo supervisa aspectos de todos los sistemas, dispositivos y aplicaciones de la infraestructura mediante diferentes tipos de sensores.
- Control de Monitor de Base de Datos: la aplicación proporciona una pista de auditoría completa de todas las actividades de la Base de Datos: consultas, resultados, autenticación y elevación de privilegios, todo lo anterior en función de reglas de detección basadas en directivas; además utiliza la supervisión pasiva de los registros de la Base de Datos (BD).
- Servidores Críticos: la herramienta ofrece servicios de protección contra malware, IPS (Intrusion Prevention System) de red y reputación de archivos dentro del servidor, además de proporcionar una instancia por host, protegiendo todas las máquinas virtuales dentro del servidor físico.
- Doble Autenticación: la solución brinda defensas contra ataques maliciosos a los datos e identidades de la Cancillería, consolidando la gestión al asociar un tipo específico de usuario o transacciones con tipo de autenticado.
- Control de acceso físico independiente al centro de datos: la Dirección de Infraestructura, controla los accesos del personal autorizado para llevar a cabo actividades en el centro de datos.
- Cámaras de video vigilancia, en el edificio y dentro del centro de datos, llevan registros sobre grabaciones de los ingresos, egresos y actividades que se realizan en el centro de datos y en las distintas áreas del edificio validando los accesos autorizados.

- La Dirección de Servicios Informáticos cuenta con un formato de resguardo que se encuentra firmado por cada uno de los usuarios de la SRE con equipo de cómputo, con el objetivo de responsabilizarse del/los equipo(s) asignados, para permitir el control de los bienes informáticos.

  Adicionalmente, se provee la salida de datos en las redes de Wifi con el filtrado de equipos FW perimetrales y equipos IPS, para evitar daños en la comunicación por malware o accesos a ligas dudosas.

Asimismo, la herramienta de filtrado de contenido que reside en la Nube y que cuenta con los módulos de Antivirus y Data Loss Prevention, permite que el usuario al moverse con sus equipos portátiles en comisión en otras localidades o a cualquier parte del mundo, sea "seguido" por el filtrado, protegiendo de esta manera sus datos y permitiendo una navegación segura.

- Los equipos se encuentran bajo un esquema contractual de arrendamiento el cual incluye actividades de mantenimiento correctivo y preventivo para asegurar la disponibilidad e integridad de los mismos.
- Control DLP (Data Loss Prevention): esta aplicación permite la detección y contención de intentos de fuga de información, cumpliendo con los criterios definidos por las áreas sustantivas, ya sea a través de protocolos de Internet o medios de almacenaje removible.
- Esquema de defensa de profundidad: modelo que aplica controles de seguridad para proteger los datos en diferentes capas, es decir, el acceso a datos se encuentra restringido a través diferentes capas tales como: defensas perimetrales (hacia el exterior de la red), defensas en la red interna, defensas en los servidores, defensas en las aplicaciones y sistemas, defensas en las bases de datos.
- Uso de información confidencial para la autenticación.
- Monitoreo de la actividad de los sistemas, dispositivos y aplicaciones de la infraestructura.

- Doble Autenticación que proporciona defensa contra ataques maliciosos sobre los datos e identidades de la Cancillería.
- La DGTII ha adoptado los controles de seguridad necesarios para garantizar la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales, mediante acciones que evitan su alteración, pérdida, transmisión y acceso no autorizado.
- Generación de bitácoras y pistas de auditoría.
- Control de acceso a las redes, a los servicios de red y a los aplicativos.

- Restricción del acceso a la información (usuarios y contraseñas con niveles jerárquicos).
- Para dar cumplimiento a la custodia y cuidado de la información, la DGTII mantiene los aplicativos actuales alojados en el Centro de Datos propiedad de la S.R.E. y sólo se puede tener acceso lógico a través de un segmento de red interna o por Certificados SSL en la parte pública. En dicho caso, la DGTII cuenta con componentes de seguridad que cuidan la integridad de la información generada y resguardada en dichos aplicativos.

b) Medidas físicas

1. Desarrollar e implementar los programas de seguridad institucional, intramuros y extramuros, para salvaguardar la integridad del personal de la SRE, la información y las instalaciones.

- Se realiza la identificación de áreas vulnerables, medidas y necesidades de seguridad por la Dirección de Servicios Generales a través de la Subdirección de Seguridad Física.

2. Supervisar los registros de los accesos, entradas y salidas a las instalaciones de la SRE, tanto de las personas, vehículos, como de los bienes propiedad de la institución, a fin de llevar un control de los mismos a través de las siguientes medidas:

- Existen límites de acceso a las instalaciones, es decir el ingreso está delimitado a ciertas puertas o entradas que permanecen cerradas en horario inhábil.

- Personal de Protección Federal se encuentra custodiando cada uno de los puntos de acceso a las instalaciones de la Secretaría.

- Se cuenta con arcos detectores de metales para la revisión de las personas que ingresan a los inmuebles de la Secretaría.

- Se cuenta con bandas de rayos X para la revisión de las pertenencias (bolsas, mochilas, portafolios, etc) de las personas, previo a su ingreso a las instalaciones de la Secretaría.

- Las personas que deseen ingresar a las instalaciones con un equipo de cómputo debe registrarlo en la bitácora correspondiente proporcionando la fecha, el nombre de la persona que ingresa el equipo de cómputo, modelo del equipo, número de serie, hora de ingreso, hora de salida y firma.

- Las personas ajenas a la institución, previo a su ingreso al área que visita debe acudir a los módulos de registro de la Secretaría a fin de proporcionar la siguiente información:

  I. Visitantes (personal externo a la Secretaría): nombre completo, servidor público a quien visita, área que visita, identificación oficial con la que se acredita(entregada), tipo de visita, hora de entrada y de salida, extensión de la persona que visita, el nombre del servidor público que autoriza el ingreso del visitante.
  II. Prestadores de servicio social y prácticas profesionales que no portan gafete: nombre completo, unidad administrativa en donde presta el servicio o práctica profesional; coordinador del servicio o práctica; extensión de la persona que visita, piso; escuela de procedencia, hora de entrada y de salida e identificación oficial con la que se acredita.
  III. Personal de la SRE que no porta gafete: nombre completo, unidad administrativa en la que labora; piso, extensión telefónica, hora de entrada, salida, identificación oficial con la que se acredita, nombre de quien autoriza la entrada y su extensión.
  IV. Proveedores y/o prestadores de servicio: nombre completo, procedencia, servidor público a quien visita, asunto, hora de entrada y de salida, firma, identificación oficial con la que se acredita, y en su caso la herramienta que ingresa al inmueble.
  V. Mensajería o entrega de oficios: nombre completo, servidor público a quien visita, área que visita, tipo de visita, hora de entrada y de salida, identificación oficial con la que se acredita, nombre y extensión del servidor público que autoriza el ingreso del visitante.
  VI. Registro de equipos de cómputo: nombre completo, marca del equipo de cómputo, número de serie, hora de entrada y de salida, y firma.

- A efecto de llevar a cabo un control de los gafetes otorgados, el personal de los módulos de registro conservará las identificaciones oficiales de las personas que ingresan. Una vez concluida la visita y para la devolución de la identificación oficial deberá entregar el gafete al personal del módulo de registro.

- Las personas que laboran en la SRE deben portar en todo momento el gafete que los identifica como trabajadores de la Dependencia, mismo que es expedido por la Dirección General del Servicio Exterior y de Recursos Humanos.

- Por lo que respecta al ingreso, se atiende lo establecido en la Norma para la Administración del Estacionamiento del Edificio Tlatelolco.

- Para permitir el ingreso de servidores públicos al estacionamiento de la Secretaría, se observa lo siguiente:

  - Cada usuario cuenta con un tarjetón de acceso, el cual es intransferible y es presentado a la entrada del estacionamiento.
  - El personal de seguridad solicita la presentación de la credencial de empleado de la Secretaría a los usuarios para verificar la correspondencia de la misma con el tarjetón.
  - En caso de pérdida o extravío del tarjetón de acceso, el usuario notifica al titular de la coordinación administrativa.

- Para permitir el acceso de personas que no laboran en la Secretaría se observan las siguientes medidas:
  - La entrada de vehículos de visitantes es solicitada a la Subdirección de Seguridad Física por servidores públicos de la Secretaría, misma que de ser procedente asigna un número de folio de autorización.
  - Los visitantes deben proporcionar su nombre completo, placas y modelo del vehículo, hora de entrada y de salida, nombre de los acompañantes, organización o institución de procedencia e identificación oficial con la que se acredita.
  - La Subdirección de Seguridad expide un "folio de visitante" para autorizar el acceso del visitante. El personal de seguridad verifica que los visitantes cuenten con el número de folio de acceso y solicita una identificación oficial vigente para corroborar los datos antes indicados.
  - El personal de seguridad proporciona un tarjetón de acceso que es colocado visiblemente en el automóvil, el cual es devuelto en la salida del estacionamiento para la entrega de la identificación oficial del visitante.
  - Para el caso de los proveedores acuden al módulo de registro que se encuentra en área de carga y descarga de proveedores o en la reja bahía del inmueble y el cual se encuentra resguardado por personal de seguridad.

3. Supervisar las cámaras y demás tecnología de seguridad de la SRE con el propósito de salvaguardar la seguridad del personal, instalaciones, información y bienes propiedad de ésta.

- La SRE cuenta con un equipo de Circuito Cerrado de Televisión, el cual es operado por el personal asignado para garantizar la seguridad y en su caso la consulta de los videos de respaldo.

4. La DGBIRM elabora y coordina los procedimientos y protocolos a seguir en caso de emergencia o contingencia, con el propósito de garantizar la integridad del personal adscrito a la SRE, la información y sus instalaciones

- A través del Programa Interno de Protección Civil se realizan las siguientes acciones:
  - Establecen las acciones preventivas, de auxilió y recuperación o vuelta a la normalidad, destinadas a salvaguardar la integridad física de los empleados y visitantes, así como proteger las instalaciones, bienes e información vital, ante la ocurrencia de alguna calamidad.
  - Se diseñan, instrumentan y operan medidas para minimizar o evitar los riesgos y/o daños, tanto humanos como materiales, que pudiesen generar por su impacto o presencia de agentes perturbadores (Fenómenos de origen natural o aquellos provocados por la acción del hombre).
  - Existen medidas para la prevención y combate de incendios como son: la instalación de extinguidores y la revisión de hidrantes, la existencia de una brigada para la prevención y combate de incendios, vigilar el mantenimiento del equipo contra-incendio, evitar la sobrecarga de líneas eléctricas y que no exista acumulación de material inflamable, verificar que las instalaciones eléctricas el mantenimiento preventivo y correctivo de manera permanente, para que las mismas ofrezcan seguridad, conocer el uso de los equipos de extinción de fuego, así como el uso que se le dé, de acuerdo a cada tipo de fuego.

- El programa incluye entre otros elementos:
  - Sub-programa de prevención.
  - Documentación del programa interno.
  - Análisis de riesgos.
  - Señalización.
  - Programa de mantenimiento.
  - Normas de seguridad.
  - Equipo de seguridad.
  - Sub-programa de auxilio.
  - Plan de emergencia.
  - Evaluación de daños.
  - Sub-programa de recuperación
  - Ejercicios de evacuación y simulacros.

5. El personal de seguridad tiene presencia permanente en las diferentes unidades administrativas de la SRE y efectúa rondines a las instalaciones, a fin de detectar anomalías en materia de seguridad y tomar las medidas pertinentes.

- A la fecha se cuenta con una herramienta para monitoreo la seguridad consistente en sensores de apertura, sensores de movimiento y cámaras de monitoreo.

c) Medidas administrativas

Seleccionar las medidas de seguridad administrativas con las que cuenta el área. En caso de tener medidas adicionales, especificarlas en el apartado otros.

Medida administrativa	Incorporar X con las que se cuenta
No está permitido el libre acceso a personal ajeno a la Dependencia y el uso de equipos de cómputo se encuentra restringido a través de la asignación de usuarios y contraseñas dentro de la red institucional.	X
De existir ventanas o muros divisorios transparentes en el área de resguardo de los expedientes la visión está obstruida mediante película traslúcida u otros.	
En el área de resguardo existen las condiciones ambientales idóneas para preservar en buen estado los soportes físicos durante el tiempo de conservación.	
Existe señalización visible sobre las restricciones de acceso, las prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área.	
La puerta de acceso del área de resguardo cuenta con cerradura, dispositivo electrónico o cualquier otra tecnología que impida su libre apertura. Este mecanismo queda cerrado en horas no hábiles o cuando el personal autorizado que ahí labora abandona el área.	X
El mobiliario utilizado dentro del área de resguardo protege los datos personales en soportes físicos contra condiciones adversas	

Medida administrativa	Incorporar X con las que se cuenta
como la humedad, temperatura, iluminación solar, polvo y presencia de plagas, entre otras.	
El mobiliario utilizado para almacenar los datos personales en soportes físicos cuenta con cerraduras, dispositivos electrónicos o cualquier otra tecnología que impida la libre apertura de sus puertas, cajones o compartimientos.	
Al interior de la unidad administrativa se cuenta con un listado del personal autorizado para manipular los expedientes o bases con nombre completo y fotografía.	
Se actualiza el listado del personal autorizado para el tratamiento de datos personales.	
Existe un encargado al interior del área que autoriza y lleva el registro de la consulta de expedientes y/o bases de datos dentro de las instalaciones de la Secretaría y se anota quién solicita el acceso, cuándo lo solicita y la razón que lo motiva.	
Existe un encargado al interior del área que autoriza y lleva el registro de la salida de expedientes o bases de datos en soportes físicos y/o electrónicos dentro de las instalaciones de la Dependencia y se anota quién hace la solicitud, qué documentos se lleva, cuándo se los lleva, cuándo los devuelve y por qué necesita llevárselos.	
Existe un responsable que mantiene control y registro de la asignación de llaves, tarjetas, contraseñas de acceso y demás elementos para abrir los mecanismos de apertura de puertas y mobiliario en el área.	
No está permitido el uso de celulares, cámaras fotográficas o de video durante la consulta de expedientes o bases de datos	

Medida administrativa	Incorporar X con las que se cuenta
No está permitido el uso de memorias USB u otros dispositivos que puedan almacenar información durante la consulta de expedientes o bases de datos.	
El personal del área se encuentra capacitado en la protección de los datos personales.	
El personal del área tiene conocimiento de las sanciones por incumplimiento de las disposiciones de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.	X
La unidad administrativa tiene plenamente identificados los procedimientos en los cuales se lleva a cabo el tratamiento de datos personales.	X
La unidad administrativa a fin de robustecer la mejora continua de la Secretaría, comunica al Comité de Transparencia las mejoras implementadas para la protección de los datos de personales.	
La unidad administrativa solicita a la Unidad de Transparencia la capacitación y actualización en materia de protección de datos personales del personal que labora en el área.	
Se lleva a cabo la revisión periódica de los procedimientos en los que se tratan datos personales para identificar áreas de mejora o actualizar las etapas de los mismos y en su caso los avisos de privacidad correspondientes.	
Existen procedimientos claros en el tratamiento de datos personales, así como los servidores públicos autorizados para su tratamiento.	
Otro (especificar)	
Otro (especificar)	
Otro (especificar)	

V. Plan de trabajo y mecanismos de monitoreo y revisión de las medidas de seguridad

FASE 1.- *REVISIÓN Y MANTENIMIENTO AL ANÁLISIS DE RIESGO*. Se ejecuta la revisión de acuerdo al proceso ASI (Administración de la Seguridad de la Información), apartados ASI 1 (Procesos institucionales en materia de Seguridad de la Información) y ASI 2 (implementación, seguimiento y control), bajo la metodología del análisis de riesgo en un proceso de mejora continua.

FASE 2.- *ACTUALIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN*.

Se realiza la actualización a los documentos asociados al análisis de riesgo, conforme al seguimiento de los comités GESI (Grupo Estratégico de Seguridad de la Información), ETAR (Equipo de Trabajo de Análisis de Riesgos) y ERISC (Equipo de Respuesta a Incidentes de Seguridad en TIC), plasmados en los procesos ASI y OPEC (Operación de los Controles de Seguridad de la Información y del ERISC) del MAAGTICSI, para documentar, en su caso, algún incidente, para determinar el plan de tratamiento y determinación de riesgo de los activos de información que se ven en el alcance de SGSI. Así mismo, la revisión de los controles de seguridad informática establecidos y en caso de detectarse, la implantación de las medidas de seguridad faltantes.

FASE 3.- *EVALUACIÓN DEL SISTEMA*. Se revisan de modo periódico los documentos y controles del MAAGTCISI para la seguridad tecnológica del sistema de gestión de la información, y la política de seguridad, así como el cumplimiento de las observaciones (en caso que hubiesen), de las auditorías correspondientes.

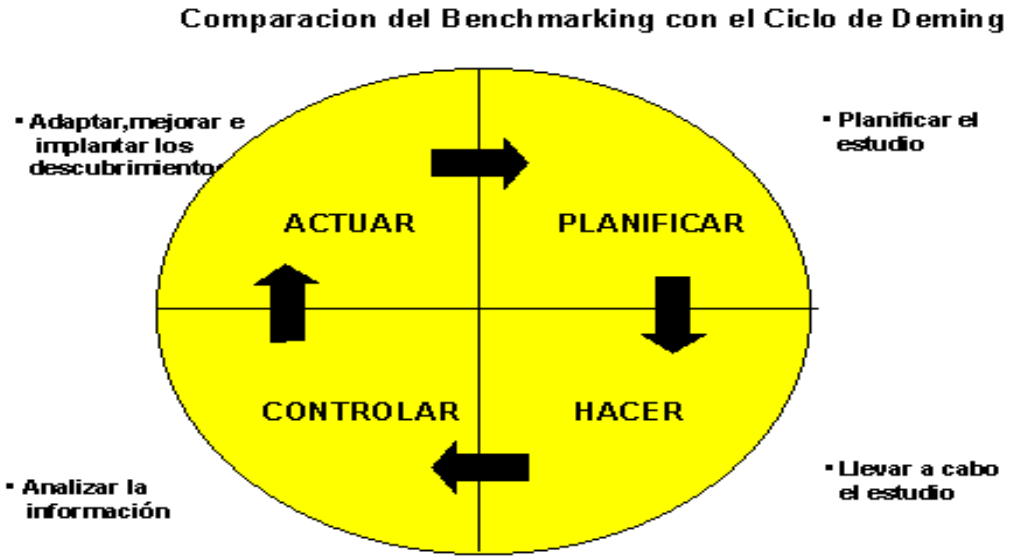
El sistema documental se apegó a los procesos ASI y OPEC, y se adicionó con las mejores prácticas en cuanto a seguridad informática de los estándares de

seguridad tecnológica internacionales. El sistema de gestión de la Información cuenta con la siguiente estructura:

ESTRUCTURA
Manual Administrativo de Aplicación General para Tecnologías de la Información, Comunicaciones y Seguridad de la Información – MAAGTICSI.
Sistema de Gestión de Seguridad de la Información - SGSI.
Política de seguridad de la información.
Análisis de riesgo de seguridad.
Lineamientos, controles e instrucciones de trabajo.
Registros (evidencias).

Mejora continua

El enfoque para la mejora continua se realiza con base en el Modelo Demming, de forma que todas las actividades de revisión al sistema de Gestión de Seguridad de la Información, deben enfocarse en el siguiente esquema:



En este sentido, se evalúa continuamente el sistema en las partes de revisión, únicamente

en aquellas partes en donde se pueda demostrar el cumplimiento de este ciclo y evaluado contra resultados, se puede hablar de la existencia de mejora continua.

Para las actividades de Acciones Correctivas, el sistema de Gestión de Seguridad de la Información se apoyará en la metodología definida en el proceso OPEC, apartados OPEC 2 (matriz rectora de respuesta a incidentes) y OPEC 3 (ejecución de acciones de control de Seguridad de la Información y Manejo de Riesgos), y los siguientes documentos:

- ERISC – Equipo de respuesta a incidentes y reuniones asociadas.

Mecanismos de monitoreo.

Los mecanismos de monitoreo, son parte sustancial de la verificación de la efectividad del Sistema de Gestión de Seguridad de la Información. Se realiza una vez por año en la reunión del comité GESI, en el momento que existan cambios relevantes en lineamientos legales, tecnologías, políticas o cualquier otro cambio que impacte al Sistema de Gestión de Seguridad de la Información.

Se deben revisar y registrar, al menos, los siguientes puntos, durante la fase de monitoreo del sistema:

a) Resultados de revisiones periódicas al Sistema de Gestión de Seguridad de la Información.
b) Política de Seguridad de la Información.
c) Retroalimentación de usuarios y partes interesadas.
d) Herramientas, técnicas, métodos, etc., para la mejora del desempeño y efectividad del sistema.
e) Estado de las acciones correctivas y preventivas y eventos registrados de seguridad (incidentes).
f) Vulnerabilidades y/o amenazas no contempladas en el más reciente análisis de riesgo.

g) Acciones de seguimiento a compromisos de revisiones previas.
h) Cualquier cambio que pudiera afectar al sistema.
i) Recomendaciones para la mejora del sistema.

Los resultados de la revisión directiva, incluyen, sin ser limitativos, aspectos relativos a:

a) Estado de los procesos ASI y OPEC del MAAGTICSI.
b) Mejora.
c) Modificaciones a metodologías o documentos del sistema.
d) Requisitos de Seguridad de Información.
e) Requisitos Legales.
f) Nuevos riesgos, sus niveles y su aceptación o no.
g) Necesidades de recursos.

VI. Programa de capacitación

La Unidad de Transparencia y el Comité de Transparencia en cumplimiento de los artículos 30, fracción III y 84, fracción VII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, elabora e implementa anualmente el Programa de Capacitación en Transparencia, Acceso a la Información, Protección de Datos Personales y temas relacionados para la Secretaría de Relaciones Exteriores y sus órganos desconcentrados.

El programa de capacitación es elaborado en coordinación con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), atendiendo a la oferta de cursos que ese instituto realiza, mismos que son impartidos por instructores del INAI o bien por alguna institución educativa de nivel superior.

El programa tiene por objetivo que las unidades administrativas tengan pleno conocimiento de las bases, principios y procedimientos establecidos en la LGPDPPSO, así como mantener actualizados a los servidores públicos en las disposiciones contenidas en la normatividad secundaria que emita el Sistema Nacional de Transparencia.

El programa de capacitación de la Secretaría de Relaciones Exteriores es aprobado anualmente por el Comité de Transparencia y se encuentra contenido en los anexos del Acta del Comité publicada en el Sistema de Portales de Obligaciones de Transparencia (SIPOT) en la fracción 39 del artículo 70 (formato informe de resoluciones del Comité de Transparencia) de la Ley General de Transparencia y Acceso a la Información Pública disponible en el siguiente vínculo electrónico: http://consultapublicamx.inai.org.mx:8080/vut-web/.

Marco normativo

Constitución Política de los Estados Unidos Mexicanos

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

Ley General de Transparencia y Acceso a la Información Pública

Ley Federal de Transparencia y Acceso a la Información Pública

Reglamento Interior de la Secretaría de Relaciones Exteriores

Lineamientos de Protección de Datos Personales publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005[2]

Recomendaciones en materia de seguridad de datos personales, publicadas en el Diario Oficial de la Federación el 30 de octubre de 2013[3]

Manual de Organización de la Dirección General de Bienes Inmuebles y Recursos Materiales

Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y Seguridad de la Información

Manual de Organización de la Subsecretaría de Relaciones Exteriores

Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales publicadas por el Instituto Federal de Acceso a la Información Pública, ahora Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).[2]

[2] Susceptibles de ser modificados por la normatividad que emita el Sistema Nacional de Transparencia
[3] De forma orientativa