

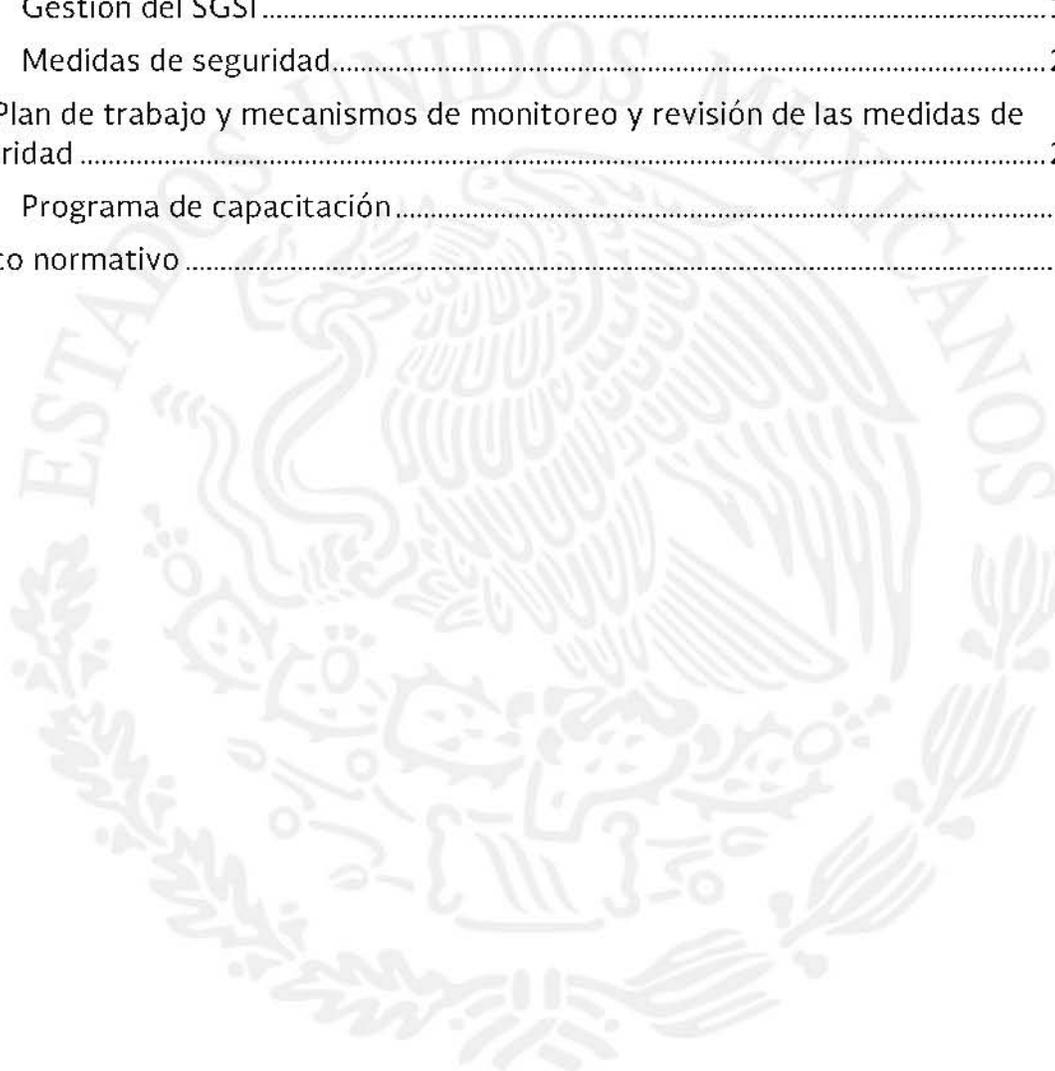


DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES
SECRETARÍA DE RELACIONES EXTERIORES

INSTITUTO MATÍAS ROMERO

Contenido

Considerandos	3
Definiciones.....	6
I. Inventario de datos personales y de los sistemas de tratamiento y funciones y obligaciones de las personas que traten datos personales.....	9
II. Análisis de riesgos y análisis de brecha.....	177
III. Gestión del SGSI.....	199
IV. Medidas de seguridad.....	221
V. Plan de trabajo y mecanismos de monitoreo y revisión de las medidas de seguridad	299
VI. Programa de capacitación.....	33
Marco normativo	34



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 del Instituto Matías Romero (IMR), señaladas en el artículo 48 del Reglamento Interior de la Secretaría de Relaciones Exteriores (RISRE), se lleva a cabo el tratamiento de datos personales que permiten contar con insumos para las acciones destinadas a:

- Preparar recursos humanos de alto nivel analítico y técnico en materia de diplomacia, política internacional y política exterior de México, en beneficio del Servicio Exterior Mexicano, la Secretaría y otras instituciones de interés público (fracción I del citado numeral).
- Formar a los miembros del Servicio Exterior Mexicano en las distintas disciplinas de la política exterior y las relaciones internacionales, además de las habilidades de la negociación internacional y la capacidad de análisis necesarias para

- enfrentar los retos de la labor diplomática contemporánea (fracción II del citado numeral).
- Ofrecer programas de educación continua y capacitación, presencial y a distancia, que contribuyan a que los participantes adquieran nuevos conocimientos y los servidores públicos de la Secretaría y miembros del Servicio Exterior Mexicano, se mantengan actualizados en materia de diplomacia, política internacional y política exterior de México (fracción IV del citado numeral).
 - Contribuir mediante cursos especiales y otros proyectos académicos, a la formación de miembros de Ministerios de Relaciones Exteriores de países de particular interés para la política exterior de México (fracción V del citado numeral).
 - Colaborar con las dependencias y entidades de la Administración Pública Federal, el Poder Legislativo, el Poder Judicial y los gobiernos estatales y municipales, así como con organizaciones de la sociedad civil, en la organización de cursos y otras actividades académicas, relacionadas con las materias de relaciones internacionales y política exterior de México (fracción VI del citado numeral).
 - Fungir como entidad coordinadora de la difusión y selección de candidatos de todas las oportunidades de capacitación que ofrezcan a la Secretaría entidades públicas y privadas, nacionales e internacionales, en materia de diplomacia, asuntos internacionales y política exterior de México (fracción IX del mismo numeral).

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 LGPDPSO.

Que por lo antes expuesto, el IMR 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.

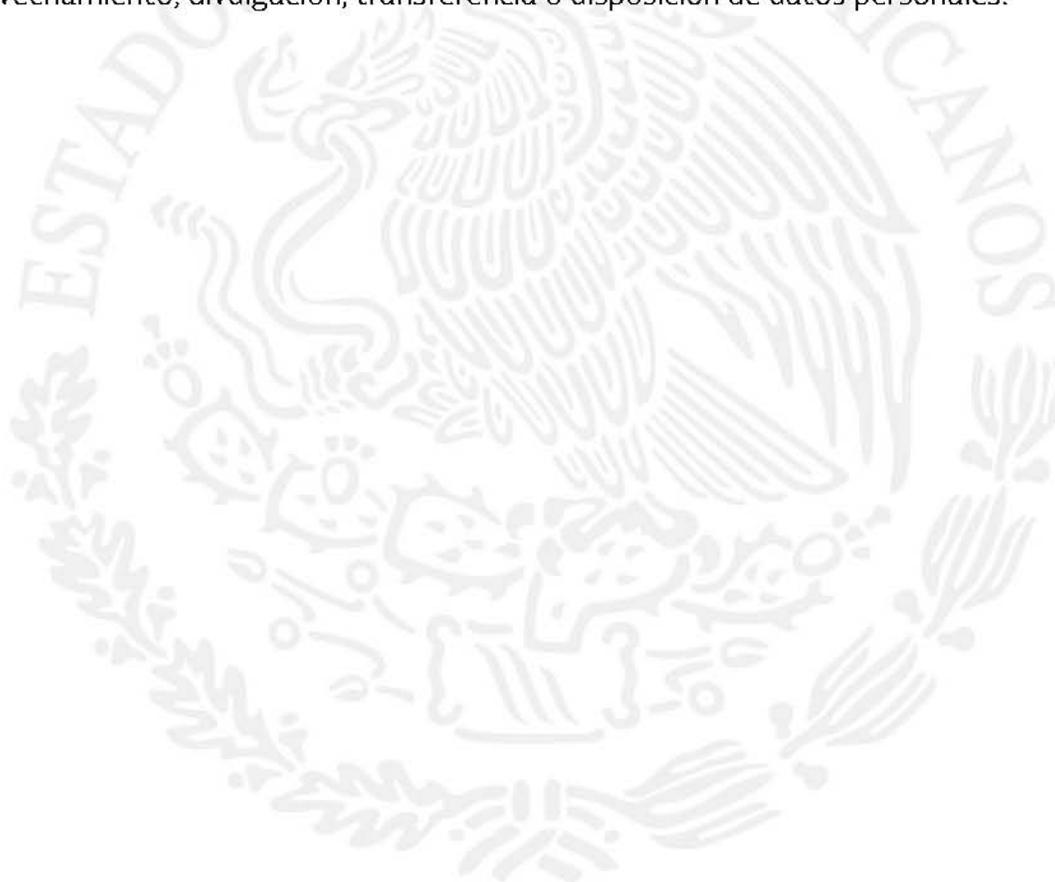
Responsable: Los sujetos obligados del ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial,

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

Proceso 1.

- A) Cursos de política exterior de México para diplomáticos extranjeros
- B) Fundamento legal: Artículo 48, fracción V del RISRE.
- C) Datos personales recabados/finalidad con la que se recaban respectivamente:
- **Nombre completo del solicitante**/Con la finalidad de identificar al solicitante.
 - **Copia del pasaporte**/A fin de contar con el número de una identificación oficial vigente.
 - **Teléfono particular**/Con la finalidad de contar con un medio de contacto para notificar diversos asuntos relacionados con el trámite correspondiente.
 - **Correo electrónico particular**/Con la finalidad de contar con un medio de contacto para notificar diversos asuntos relacionados con el trámite correspondiente.
 - **Domicilio particular**/Se recaba con la finalidad de contar con un lugar en dónde poder contactar al solicitante.
 - **Fecha de nacimiento**/Con la finalidad de tener conocimiento de la edad del postulante.
 - **Nacionalidad**/Se recaba en virtud de que se realiza un proceso interno de selección y, generalmente, sólo se acepta a un participante por país.
 - **Nombre del contacto de emergencia**/Se recaba para que en el caso de un siniestro, se pueda contactar a alguien cercano al beneficiario.
 - **Teléfono particular del contacto de emergencia**/Se recaba para que en el caso de un siniestro, se pueda contactar a alguien cercano al participante.

- **Dirección del correo electrónico del contacto de emergencia**/Se recaba para que en el caso de un siniestro, se pueda contactar a alguien cercano al participante.
- **Firma**/Con la finalidad de validar información proporcionada.
- **Certificado Médico Vigente**/Para conocer el estado de salud del participante.
- **Copia de Título Profesional del postulante**/Con la finalidad de sustentar su grado académico.
- **Dos fotografías tamaño pasaporte**/Con la finalidad de integrar el expediente del postulante.
- **Copia de Currículum Vitae**/Con el objetivo de tener conocimiento de su trayectoria profesional.

D) Personal participante en el tratamiento de datos personales

1. Cargo del personal que participa en el tratamiento de los datos personales: Dirección General Adjunta de Vinculación Internacional, Difusión y Control Interno/Directora de Vinculación Internacional e Interinstitucional.
2. Funciones de las personas que tratan datos personales: Obtener y tratar los datos referidos para los fines indicados.
3. Obligaciones de las personas que tratan datos personales (en relación con el proceso): Tratar los datos personales para la finalidad con la que fueron recabados y de conformidad con las atribuciones conferidas en la normatividad aplicable.

Proceso 2.

- A) Cursos de política exterior de México para diplomáticos de América Latina y el Caribe
- B) Fundamento legal: Artículo 48, fracción V del RISRE.
- C) Datos personales recabados/finalidad con la que se recaban respectivamente:
 - **Nombre completo del solicitante**/Con la finalidad de identificar al solicitante.
 - **Copia del pasaporte**/A fin de contar con el número de una identificación oficial vigente.

- **Teléfono particular**/Con la finalidad de contar con un medio de contacto para notificar diversos asuntos relacionados con el trámite correspondiente.
- **Correo electrónico particular**/Con la finalidad de contar con un medio de contacto para notificar diversos asuntos relacionados con el trámite correspondiente.
- **Domicilio particular**/Se recaba con la finalidad de contar con un lugar en dónde poder contactar al solicitante.
- **Fecha de nacimiento**/Con la finalidad de tener conocimiento de la edad del postulante.
- **Nacionalidad**/Se recaba en virtud de que se realiza un proceso interno de selección y, generalmente, sólo se acepta a un participante por país.
- **Nombre del contacto de emergencia**/Se recaba para que en el caso de un siniestro, se pueda contactar a alguien cercano al beneficiario.
- **Teléfono particular del contacto de emergencia**/Se recaba para que en el caso de un siniestro, se pueda contactar a alguien cercano al participante.
- **Dirección del correo electrónico del contacto de emergencia**/Se recaba para que en el caso de un siniestro, se pueda contactar a alguien cercano al participante.
- **Firma**/Con la finalidad de validar información proporcionada.
- **Certificado Médico Vigente**/Para conocer el estado de salud del participante.
- **Copia de Título Profesional del postulante**/Con la finalidad de sustentar su grado académico.
- **Dos fotografías tamaño pasaporte**/Con la finalidad de integrar el expediente del postulante.

D) Personal participante en el tratamiento de datos personales

1. Cargo del personal que participa en el tratamiento de los datos personales: Dirección General Adjunta de Vinculación Internacional, Difusión y Control Interno/Directora de Vinculación Internacional e Interinstitucional.
2. Funciones de las personas que tratan datos personales: Obtener y tratar los datos referidos para los fines indicados.
3. Obligaciones de las personas que tratan datos personales (en relación con el proceso): Tratar los datos personales para la finalidad con la que fueron recabados y de conformidad con las atribuciones conferidas en la normatividad aplicable.

Proceso 3.

A) Cursos de español para diplomáticos extranjeros.

B) Fundamento legal: Artículo 48, fracción V del RISRE.

C) Datos personales recabados/finalidad con la que se recaban respectivamente:

- **Nombre completo del solicitante**/Con la finalidad de identificar al solicitante.
- **Copia del pasaporte**/A fin de contar con el número de una identificación oficial vigente.
- **Teléfono particular**/Con la finalidad de contar con un medio de contacto para notificar diversos asuntos relacionados con el trámite correspondiente.
- **Correo electrónico particular**/Con la finalidad de contar con un medio de contacto para notificar diversos asuntos relacionados con el trámite correspondiente.
- **Domicilio particular**/Se recaba con la finalidad de contar con un lugar en dónde poder contactar al solicitante.
- **Fecha de nacimiento**/Con la finalidad de tener conocimiento de la edad del postulante.
- **Nacionalidad**/Se recaba en virtud de que se realiza un proceso interno de selección y, generalmente, sólo se acepta a un participante por país.
- **Nombre del contacto de emergencia**/Se recaba para que en el caso de un siniestro, se pueda contactar a alguien cercano al beneficiario.
- **Teléfono particular del contacto de emergencia**/Se recaba para que en el caso de un siniestro, se pueda contactar a alguien cercano al participante.
- **Dirección del correo electrónico del contacto de emergencia**/Se recaba para que en el caso de un siniestro, se pueda contactar a alguien cercano al participante.
- **Firma**/Con la finalidad de validar información proporcionada.
- **Certificado Médico Vigente**/Para conocer el estado de salud del participante.
- **Copia de Título Profesional del postulante**/Con la finalidad de sustentar su grado académico.
- **Copia de comprobante de posesión de español (sólo cuando no hubiera entrevista opcional al efecto)**/Como documento probatorio para la comprensión de los temas expuestos en el curso.
- **Dos fotografías tamaño pasaporte**/Con la finalidad de integrar el expediente del postulante.

D) Personal participante en el tratamiento de datos personales

1. Cargo del personal que participa en el tratamiento de los datos personales: Dirección General Adjunta de Vinculación Internacional, Difusión y Control Interno/Directora de Vinculación Internacional e Interinstitucional.
2. Funciones de las personas que tratan datos personales: Obtener y tratar los datos referidos para los fines indicados.
3. Obligaciones de las personas que tratan datos personales (en relación con el proceso): Tratar los datos personales para la finalidad con la que fueron recabados y de conformidad con las atribuciones conferidas en la normatividad aplicable.

Proceso 4.

- A) Curso introductorio para diplomáticos acreditados en México.
- B) Fundamento legal: Artículo 48, fracción V del RISRE.
- C) Datos personales recabados/finalidad con la que se recaban respectivamente:

- **Nombre completo del solicitante**/Con la finalidad de identificar al solicitante.
- **Copia del pasaporte**/A fin de contar con el número de una identificación oficial vigente.
- **Teléfono particular**/Con la finalidad de contar con un medio de contacto para notificar diversos asuntos relacionados con el trámite correspondiente.
- **Correo electrónico particular**/Con la finalidad de contar con un medio de contacto para notificar diversos asuntos relacionados con el trámite correspondiente.
- **Domicilio particular**/Se recaba con la finalidad de contar con un lugar en dónde poder contactar al solicitante.
- **Fecha de nacimiento**/Con la finalidad de tener conocimiento de la edad del postulante.
- **Nacionalidad**/Se recaba en virtud de que se realiza un proceso interno de selección y, generalmente, sólo se acepta a un participante por país.
- **Nombre del contacto de emergencia**/Se recaba para que en el caso de un siniestro, se pueda contactar a alguien cercano al beneficiario.
- **Teléfono particular del contacto de emergencia**/Se recaba para que en el caso de un siniestro, se pueda contactar a alguien cercano al participante.
- **Dirección del correo electrónico del contacto de emergencia**/Se recaba para que en el caso de un siniestro, se pueda contactar a alguien cercano al participante.
- **Firma**/Con la finalidad de validar información proporcionada.
- **Dos fotografías tamaño pasaporte**/Con la finalidad de integrar el expediente del postulante.

D) Personal participante en el tratamiento de datos personales

1. Cargo del personal que participa en el tratamiento de los datos personales: Dirección General Adjunta de Vinculación Internacional, Difusión y Control Interno/Directora de Vinculación Internacional e Interinstitucional.
2. Funciones de las personas que tratan datos personales: Obtener y tratar los datos referidos para los fines indicados.
3. Obligaciones de las personas que tratan datos personales (en relación con el proceso): Tratar los datos personales para la finalidad con la que fueron recabados y de conformidad con las atribuciones conferidas en la normatividad aplicable.

Proceso 6.

A) Cursos en línea

B) Fundamento legal: Artículo 48, fracción IV del RISRE.

C) Datos personales recabados/finalidad con la que se recaban respectivamente:

- **CURP**/Se utiliza como clave única de identificación de cada participante.
- **Nivel de estudios**/Permite conocer el perfil de la audiencia de cada curso.
- **Dirección**/Requerida por UNITAR y DiploFoundation para el envío de constancias.
- **Teléfono particular**/En ocasiones se requiere entrar en contacto con los participantes con relación al respectivo curso.
- **Teléfono celular**/Misma finalidad.
- **Correo electrónico**/Es la vía de comunicación más importante con los participantes.
- **Nacionalidad**/Dato requerido para los informes estadísticos.

D) Personal participante en el tratamiento de datos personales

1. Cargo del personal que participa en el tratamiento de los datos personales: Dirección General Adjunta de la Academia Diplomática/Directora de Educación a Distancia.
2. Funciones de la persona que trata datos personales (en relación con el proceso): Obtener y tratar los datos referidos para los fines indicados.
3. Obligaciones (en relación con el proceso): Tratar los datos personales para la finalidad con la que fueron recabados y de conformidad con las atribuciones conferidas en la normatividad aplicable.

Proceso 7.

A) Cursos de formación diplomática para becarios de las ramas Diplomático-Consular y Técnico-Administrativa, ambas del Servicio Exterior Mexicano.

B) Fundamento legal: Artículo 48, fracciones I, II y IV del RISRE.

C) Datos personales recabados/finalidad con la que se recaban respectivamente:

- **Nombre Completo**/Con la finalidad de identificar a los becarios.
- **Lugar de nacimiento**/Dato requerido para los informes estadísticos.
- **Fecha de nacimiento**/Con la finalidad de tener conocimiento de la edad de los becarios.
- **Edad**/Misma finalidad.
- **Estado civil**/Dato que permite conocer si tienen o no dependientes económicos.
- **Domicilio particular**/Se recaba con la finalidad de contar con un lugar en dónde poder contactar al solicitante.
- **Teléfono particular**/Con la finalidad de contar con un medio de contacto para notificar diversos asuntos.
- **Teléfono celular**/Permite contar con un medio de contacto para notificar diversos asuntos.
- **Correo electrónico**/Es la vía de comunicación más importante con los becarios.
- **Cuenta de Twitter**/Se recaba para un control de registro.
- **Nombre del contacto de emergencia**/Se recaba para que en el caso de un siniestro, se pueda contactar a alguien cercano al beneficiario.
- **Teléfono particular del contacto de emergencia**/Misma finalidad.
- **Datos de seguro médico**/Es un dato que permite saber a quién recurrir en caso de algún siniestro.
- **Idiomas**/Permite conocer las habilidades lingüísticas de los becarios.
- **Antecedentes laborales**/Se recaba con la finalidad de conocer el perfil de los becarios y son datos para informes estadísticos.

D) Personal participante en el tratamiento de datos personales

1. Cargo del personal que participa en el tratamiento de los datos personales:
Dirección General Adjunta de la Academia Diplomática/Director de Educación Presencial.
2. Funciones de la persona que trata datos personales (en relación con el proceso):
Obtener y tratar los datos referidos para los fines indicados.
3. Obligaciones (en relación con el proceso): Tratar los datos personales para la finalidad con la que fueron recabados y de conformidad con las atribuciones conferidas en la normatividad aplicable.

Proceso 8.

- A) Curso presenciales varios (idiomas, temas de actualidad internacional, asimilados).
- B) Fundamento legal: Artículo 48, fracciones I, II y IV del RISRE.
- C) Datos personales recabados/finalidad con la que se recaban respectivamente:
- **Nombre Completo**/Con la finalidad de identificar a los participantes.
 - **CURP**/Se utiliza como clave única de identificación de cada participante.
 - **Nivel de estudios**/Permite conocer el perfil de la audiencia de cada curso.
 - **Adscripción y cargo**/Permite identificar el tipo de funciones que realizan los participantes.
 - **Teléfono celular**/ En ocasiones se requiere entrar en contacto con los participantes con relación al respectivo curso (ello en complemento al teléfono de oficina recabado con la misma finalidad).
 - **Correo electrónico**/Es la vía de comunicación más importante con los participantes.
- D) Personal participante en el tratamiento de datos personales
1. Cargo del personal que participa en el tratamiento de los datos personales: Dirección General Adjunta de la Academia Diplomática/Director de Educación Presencial.
 2. Funciones de la persona que trata datos personales (en relación con el proceso): Obtener y tratar los datos referidos para los fines indicados.
 3. Obligaciones (en relación con el proceso): Tratar los datos personales para la finalidad con la que fueron recabados y de conformidad con las atribuciones conferidas en la normatividad aplicable.

Proceso 9.

- A) Cursos de preparación para exámenes de ascenso
- B) Fundamento legal: Artículo 48, fracciones I, II y IV del RISRE.

- C) **Datos personales recabados**/finalidad con la que se recaban respectivamente:
- **Nombre Completo**/Con la finalidad de identificar a los participantes.
 - **CURP**/Se utiliza como clave única de identificación de cada participante.
 - **Nivel de estudios**/Permite conocer el perfil de la audiencia de cada curso.
 - **Teléfono de oficina**/En ocasiones se requiere entrar en contacto con los participantes con relación al respectivo curso.
 - **Teléfono celular**/Misma finalidad.
 - **Correo electrónico**/Es la vía de comunicación más importante con los participantes.
- D) Personal participante en el tratamiento de datos personales
1. Cargo del personal que participa en el tratamiento de los datos personales: Dirección General Adjunta de la Academia Diplomática/Director de Educación Presencial.
 2. Funciones de la persona que trata datos personales (en relación con el proceso): Obtener y tratar los datos referidos para los fines indicados.
 3. Obligaciones (en relación con el proceso): Tratar los datos personales para la finalidad con la que fueron recabados y de conformidad con las atribuciones conferidas en la normatividad aplicable.

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

La información será proporcionada por la DGBIRM

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.	X
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 como la humedad, temperatura, iluminación solar, polvo y presencia de plagas, entre otras.	X

Medida administrativa	Incorporar X con las que se cuenta
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.	X
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.	X
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.	X
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.	X
No está permitido el uso de celulares, cámaras fotográficas o de video durante la consulta de expedientes o bases de datos	
No está permitido el uso de memorias USB u otros dispositivos que puedan almacenar información durante la consulta de expedientes o bases de datos.	

Medida administrativa	Incorporar X con las que se cuenta
El personal del área se encuentra capacitado en la protección de los datos personales.	x
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.	x
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.	x
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.	x
Existen procedimientos claros en el tratamiento de datos personales, así como los servidores públicos autorizados para su tratamiento.	x
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 continúa.

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 MAAGTICSI 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.

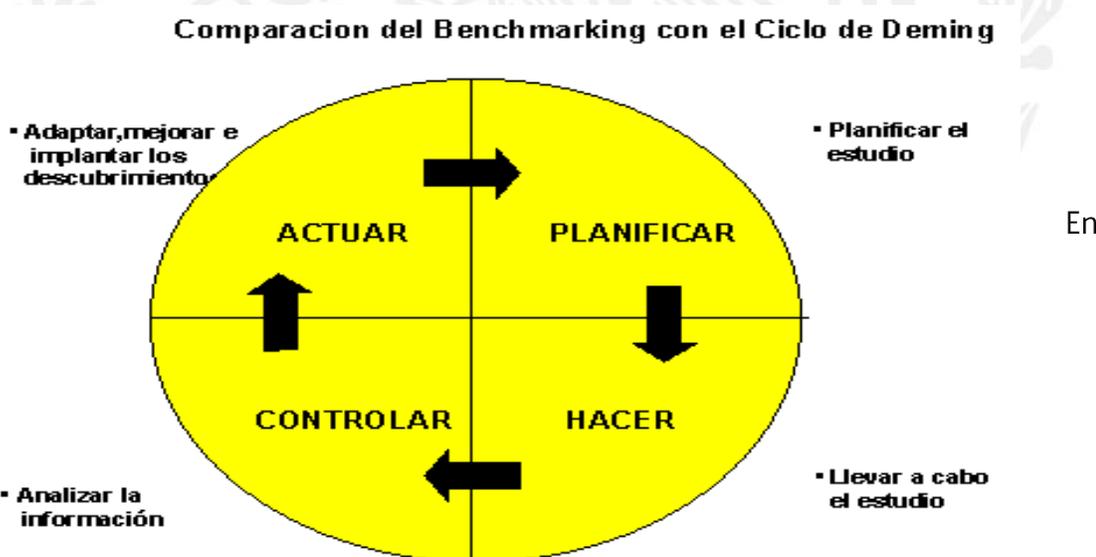
El sistema documental se apejó a los procesos ASI y OPEC, y se adicionó con las mejores prácticas en cuanto a seguridad informática de los estándares de

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:



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.

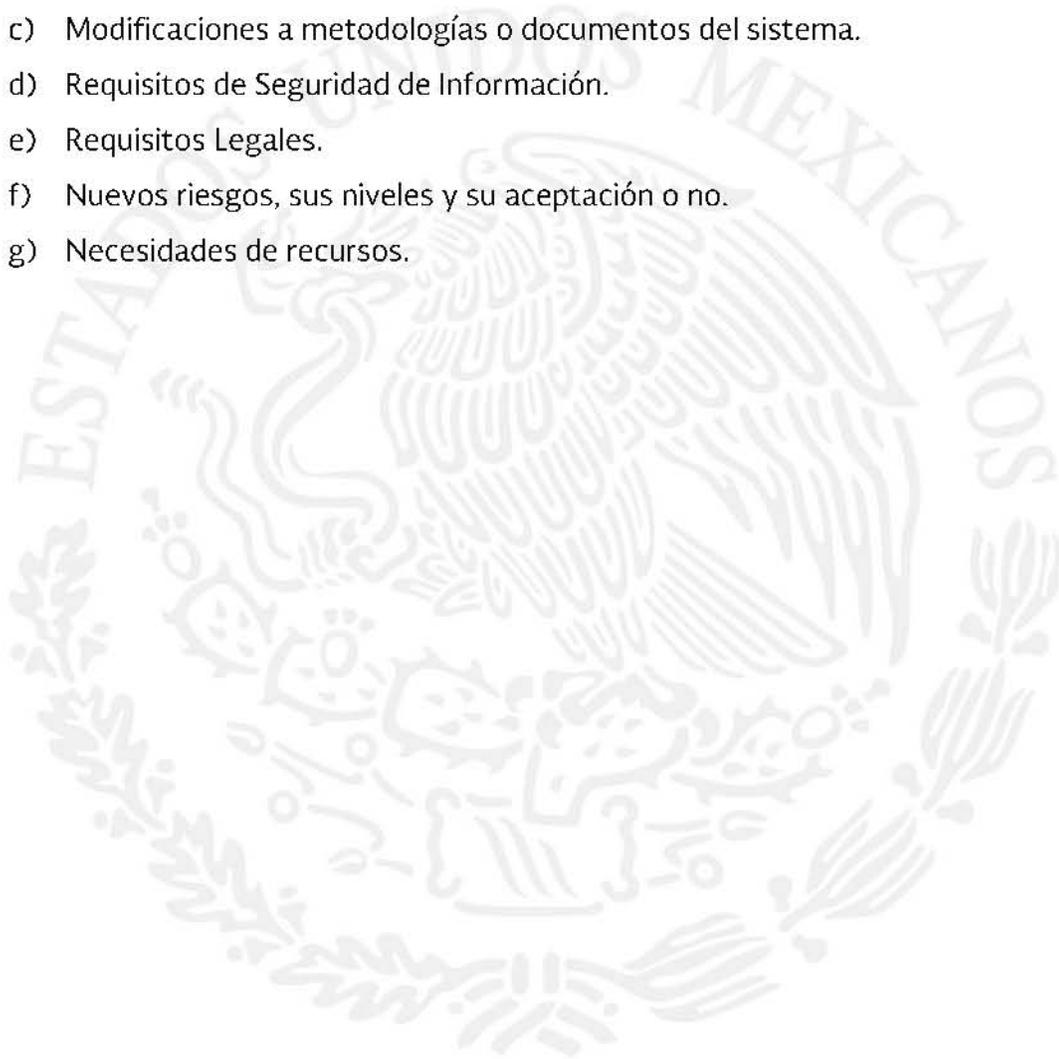
Se deben revisar y registrar, al menos, los siguientes puntos, durante la fase de monitoreo del sistema:

- 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 2005¹

Recomendaciones en materia de seguridad de datos personales publicadas en el Diario Oficial de la Federación el 30 de octubre de 2013²

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 del Instituto Matías Romero (enero de 2018)

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

¹ Susceptibles de ser modificados por la normatividad que emita el Sistema Nacional de Transparencia

² De forma orientativa