SHCP
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

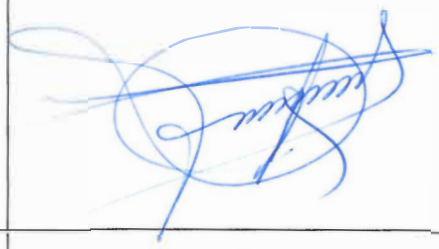
SAT
SERVICIO DE ADMINISTRACIÓN TRIBUTARIA

Documento

De Seguridad de los Sistemas de Datos Personales en Posesión del SAT

Servicio de Administración Tributaría
Administración General de Servicios al Contribuyente
Administración General de Comunicaciones y Tecnologías de la Información

Firmas de Validación del Documento de Seguridad de los Sistemas de Datos Personales en Posesión del SAT.

Nombre y Puesto	Firma
Lic. Oscar Manuel Montoya Landeros Coordinador Nacional de las Administraciones Desconcentradas de Servicios al Contribuyente Suplente de la Titular de la Unidad de Transparencia del SAT	
Carlos Gerardo Malanche Flores Administrador Central de Seguridad Monitoreo y Control. Responsable de la Seguridad de la Información en el SAT	
Eleuterio Díaz María Administrador Central de Apoyo Jurídico de Recursos y Servicios Responsable de sistemas de datos personales	
Mtro. Zenén Miguel Cruz Administrador de Apoyo Jurídico de Aduanas "9" Responsable de sistemas de datos personales	
Lic. Alejandra Cañizares Tello Administrador Central de Estudios Tributarios y Aduaneros Responsable de sistemas de datos personales	

Nombre y Puesto	**Firma**
Lic. Marco A. Hernandez Lara Administrador Central de Apoyo Jurídico de Auditoria Fiscal Federal Responsable de sistemas de datos personales	
Lic. Obed Jesé Luján Caracas Administrador Central de Apoyo Jurídico de Recaudación Responsable de sistemas de datos personales	
Lic. Claudia Fabiola Villagrán Díaz Administradora Central de Apoyo Jurídico de Auditoria de Comercio Exterior Responsable de sistemas de datos personales	

Índice

Introducción

Para el ejercicio del derecho de acceso a la información de acuerdo al artículo 6, apartado A, fracción II. de la Constitución Política de los Estados Unidos Mexicanos, toda información que se refiere a la vida privada y datos personales, será protegida en los términos y con las excepciones que fijen las leyes.

En este tenor el pasado 26 de enero del 2017, se publicó en el Diario Oficial de la Federación, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, que en su artículo 35, hace referencia a que los sujetos obligados deberán realizar un documento de seguridad, el cual será un instrumento que describa y dé cuenta de manera general, sobre las medidas de seguridad técnicas, físicas y administrativas, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Asimismo, el pasado 26 de enero de 2018, se publicaron los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en los que se desarrollan y concentran las obligaciones exigibles del derecho a la protección de datos personales en el sector público federal.

El presente documento, es un instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el Servicio de Administración Tributaria (SAT) con el fin de garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee; para responder a los derechos de los tutelados, frente a su alteración, pérdida, transmisión, con ello se garantizará la privacidad de los individuos velando porque terceras personas no incurran en conductas que puedan afectarla arbitrariamente.

Capítulo I
Marco jurídico – administrativo

Constitución Política de los Estados Unidos Mexicanos.
Publicada en D.O.F. 05-II-1917, última reforma D.O.F. 27-VIII-2018

Leyes / Códigos Federales

1. Ley del Servicio de Administración Tributaria.
   Publicada en D.O.F. 15-XII-1995, última reforma D.O.F 04-XII-2018

2. Ley General de Transparencia y Acceso a la Información Pública.
   Publicada en D.O.F. 04-V-2015

3. Ley General de Responsabilidades Administrativas.
   Publicada en el D.O.F. 18-VII-2016

4. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
   Publicada en el D.O.F. 26-I-2017

5. Ley Federal de Transparencia y Acceso a la Información Pública.
   Publicada en el D.O.F. 27-I-2017

Reglamentos

1. Reglamento Interior del Sevicio de Administración Tributaria.
   Publicado en D.O.F. 24-VIII-2015

Estrategias, Manuales y Lineamientos

1. Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el sector público.
   Publicado en D.O.F. 26-I-2018

2. Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual Administrativo de Aplicación General en dichas materias.
   Publicado en D.O.F. 23-VII-2018

AG

Capítulo II
Objetivo y alcance

Objetivo

Establecer el documento para garantizar la protección de sus datos personales, en posesión del SAT, y que deberán observar las Unidades Administrativas del SAT.

Alcance

Este documento, es un instrumento normativo y de apoyo administrativo, de observancia obligatoria para todos los servidores públicos del SAT que generen, consulten, custodien información que contenga datos personales y/o datos personales sensibles que obren en los sistemas destinados para tal fin.

Capítulo III
Inventario de datos personales y de los sistemas de datos personales

Los datos personales que contienen los sistemas de datos personales en el SAT son los siguientes:

1. Teléfono
2. Edad
3. Sexo
4. Registro Federal de Contribuyentes
5. Clave Única del Registro de Población
6. Estado Civil
7. Nombre de usuario en redes sociales
8. Correo electrónico
9. Lugar y fecha de Nacimiento
10. Fotografía
11. Nacionalidad
12. Datos sobre pasatiempos, entretenimiento y diversión
13. Puesto de trabajo
14. Lugar de trabajo
15. Experiencia Laboral
16. Datos de contacto laborales
17. Idioma o lengua
18. Escolaridad
19. Títulos
20. Certificados
21. Información migratoria
22. Cédula Profesional
23. Domicilio
24. Información de tránsito de personas
25. Saldos bancarios
26. Estados de cuenta
27. Números de cuenta
28. Cuentas de inversión
29. Bienes muebles
30. Bienes inmuebles
31. Información fiscal
32. Historial crediticio
33. Ingresos
34. Egresos
35. Buró de Crédito
36. Seguros
37. Afores

38. Salario
39. Fianzas
40. Número de Tarjeta Bancaria
41. Número de Tarjeta de Débito
42. Usuarios
43. Contraseñas
44. Identificaciones oficiales
45. Información biométrica
46. Firma autógrafa
47. Firma electrónica
48. Otros mecanismos de autenticación
49. Antecedentes penales
50. Amparos
51. Demandas
52. Contratos
53. Litigios
54. Procedimientos administrativos
55. Procedimientos penales
56. Procedimientos laborales
57. Procedimientos civiles
58. Origen racial o étnico
59. Estado de salud
60. Cicatrices
61. Tipo de sangre
62. Información genética
63. Pertenencia a un partido/Posturas políticas
64. Creencias religiosas filosóficas o morales
65. Afiliación sindical
66. Opiniones políticas
67. Hábitos sexuales
68. Dependientes
69. Beneficiarios
70. Familiares
71. Referencias laborales
72. Referencias personales
73. Otros datos que pueden originar discriminación
74. Información adicional al número de tarjeta bancaria

A continuación, se listan los sistemas de datos personales que se tienen a la fecha de la publicación de este documento:

Nombre del Sistema	Estado del Sistema	AG dueña del aplicativo	Custodia
(Antes SAAI_WEB - Sistema de Operación Integral Aduanera (SOIA)_PEA_SIRET	En funcionamiento	AGA	AGA
Administración Técnica	En funcionamiento	AGA	AGA
AGS-HRMS Solución Integral	En funcionamiento	AGRS	ACOST
Análisis Dinámico y Carga de Manifiestos	En funcionamiento	AGA	AGA
Apis_legado (para 2008 y 2009)	En funcionamiento	AGA	AGA
Apoyo a incorporación de Firma Electrónica Avanzada (FEA) y Datos Biométricos	En funcionamiento	AGSC	ACOST
Automatizar el Monitoreo de PPEE's (Personas Política y Económicamente Expuestas)	En funcionamiento	AGE	ACOST
Bóveda de Créditos Express	En funcionamiento	AGR	ACOST
Buscador de localidades sin acceso a internet	En funcionamiento	AGSC	ACOST
Captura y Validación Contables (Esquema anterior)	En funcionamiento	AGP	ACOST
Componente de Evaluación	En funcionamiento	AGRS	ACOST

Nombre del Sistema	Estado del Sistema	AG dueña del aplicativo	Custodia
Consulta de Devoluciones Automáticas Cálculos Aritméticos	En funcionamiento	AGAFF	ACOST
Consulta de Devoluciones Manuales Web	En funcionamiento	AGAFF	ACOST
Consulta de Lotes	En funcionamiento	AGR	ACOST
Consulta de Permisos de Importación Temporal de Vehículos	En funcionamiento	AGA	AGA
Consulta de Transacciones	En funcionamiento	AGR	ACOST
Consulta interna de información de intereses para 2016.	En funcionamiento	AGR	ACOST
Consulta MAT de declaraciones y pagos del RIF	En funcionamiento	AGR	ACOST
Consulta Remota de Pedimentos	En funcionamiento	AGA	AGA
Consulta Web de Devoluciones Automáticas	En funcionamiento	AGAFF	ACOST
Contabilidad Central (Esquema anterior)	En funcionamiento	AGP	ACOST
Contabilidad Electrónica	En funcionamiento	AGAFF	ACOST
Contabilidad Electrónica Mi PyMES	En funcionamiento	AGAFF	ACOST
Contabilidad General	En funcionamiento	AGP	ACOST

Nombre del Sistema	Estado del Sistema	AG dueña del aplicativo	Custodia
Contabilidad Regional (Esquema anterior)	En funcionamiento	AGP	ACOST
Control de Pagos Disponibles en TESOFE	En funcionamiento	AGAFF	ACOST
Créditos Fiscales	En funcionamiento	AGR	ACOST
Cubo de Información SAC	En funcionamiento	AGSC	ACOST
Cuenta Única Web	En funcionamiento	AGR	ACOST
Declaración Anual de Personas Físicas	En funcionamiento	AGR	ACOST
Declaración Anual de Personas Morales	En funcionamiento	AGR	ACOST
Declaración de Pasajeros y Excedente de Franquicia	En funcionamiento	AGA	AGA
Declaración de Proveedores IVA	En funcionamiento	AGR	ACOST
Declaración Informativa de Aprovechamientos por el manejo, almacenaje y custodia de mercancías de comercio exterior	En funcionamiento	AGR	ACOST
Declaración informativa de empresas manufactureras, maquiladoras y de servicios de exportación	En funcionamiento	AGR	ACOST
Declaración Informativa de los Regímenes Fiscales Preferentes	En funcionamiento	AGR	ACOST

Nombre del Sistema	Estado del Sistema	AG dueña del aplicativo	Custodia
Declaración Informativa de Notarios Públicos y demás Fedatarios.	En funcionamiento	AGR	ACOST
Declaración Informativa de Operaciones con partes relacionadas	En funcionamiento	AGR	ACOST
Declaración Informativa de Operaciones con Terceros	En funcionamiento	AGR	ACOST
Declaración Informativa de Operaciones realizadas por cuenta de los integrantes del consorcio petrolero	En funcionamiento	AGR	ACOST
Declaración Informativa de Operaciones Relevantes (Art. 31 A del CFF)	En funcionamiento	AGR	ACOST
Declaración Informativa del fomento al primer empleo	En funcionamiento	AGR	ACOST
Declaración Informativa Mensual y Anual del Impuesto a los Depósitos en Efectivo	En funcionamiento	AGR	ACOST
Declaración Informativa Múltiple del IEPS	En funcionamiento	AGR	ACOST
Declaración Informativa Múltiple DIM	En funcionamiento	AGR	ACOST

Nombre del Sistema	Estado del Sistema	AG dueña del aplicativo	Custodia
Declaración Informativa por Contraprestaciones o Donativos Recibidos Superiores a $ 100,000.00	En funcionamiento	AGR	ACOST
Declaraciones de pagos de derechos, productos y aprovechamientos	En funcionamiento	AGR	ACOST
Declaraciones de pagos provisionales o definitivos de impuestos federales	En funcionamiento	AGR	ACOST
Declaraciones de pagos provisionales o definitivos de impuestos federales de personas morales – Mi contabilidad	En funcionamiento	AGR	ACOST
Declaraciones de pagos provisionales o definitivos de impuestos federales de personas físicas RIF - Arrendamiento	En funcionamiento	AGR	ACOST
Declaraciones Informativas en Medios Magnéticos (DIMM)	En funcionamiento	AGR	ACOST
Declaraciones que se reciben por contingencia en papel de PEMEX	En funcionamiento	AGR	ACOST
Devoluciones Automáticas	En funcionamiento	AGAFF	ACOST

Nombre del Sistema	Estado del Sistema	AG dueña del aplicativo	Custodia
Devoluciones y Compensaciones	En funcionamiento	AGAFF	ACOST
Devoluciones y Compensaciones Interface de MAT a SIR	En funcionamiento	AGAFF	ACOST
Dictámenes.NET	En funcionamiento	AGAFF	ACOST
Evaluación EIDD 360°	En funcionamiento	AGRS	ACOST
Fichas CPED	En funcionamiento	AGA	AGA
FIEL_CIEC	En funcionamiento	AGSC	ACOST
Firma Electrónica Avanzada (FEA Aduanas)	En funcionamiento	AGSC	ACOST
Firma Electrónica: Validador del estatus del certificado de Firma Electrónica	En funcionamiento	AGSC	ACOST
Fiscalización electrónica AGAFF	En funcionamiento	AGAFF	ACOST
Fiscalización Electrónica Básica	En funcionamiento	AGAFF	ACOST
Funcionarios con permisos de consulta a Personas Políticamente Expuestas (FPPE)	En funcionamiento	AGE	ACOST
Generar registros para la contabilidad	En funcionamiento	AGR	ACOST
IBM Cognos Conection (IDE)	En funcionamiento	AGR	ACOST
IMMEX: Automatización del Modelo de Riesgo	En funcionamiento	AGACE	ACOST

Nombre del Sistema	Estado del Sistema	AG dueña del aplicativo	Custodia
Intersecretarias (Secretarias de Estado / Entidades Internas / Entidades Externas)	En funcionamiento	AGA	AGA
Inventario de Recursos Humanos (antes llamado Sistema de reclutamiento de personal)	En funcionamiento	AGRS	ACOST
JUPITER	En funcionamiento	AGJ	ACOST
JUPITER Archivo	En funcionamiento	AGJ	ACOST
JUPITER Asistencia Legal	En funcionamiento	AGJ	ACOST
JUPITER Asuntos Penales	En funcionamiento	AGJ	ACOST
JUPITER Clasificación arancelaria	En funcionamiento	AGJ	ACOST
JUPITER Extracción Horizontal	En funcionamiento	AGJ	ACOST
JUPITER Generación de Informes	En funcionamiento	AGJ	ACOST
JUPITER Generalidades	En funcionamiento	AGJ	ACOST
JUPITER Herramienta de créditos controvertidos	En funcionamiento	AGJ	ACOST
JUPITER Juicio de Nulidad	En funcionamiento	AGJ	ACOST
JUPITER Oficialía de partes	En funcionamiento	AGJ	ACOST
JUPITER Pestaña, Carátula y Volantes	En funcionamiento	AGJ	ACOST
JUPITER Recursos Administrativos	En funcionamiento	AGJ	ACOST

Nombre del Sistema	Estado del Sistema	AG dueña del aplicativo	Custodia
JUPITER Reportes de Emisión Local	En funcionamiento	AGJ	ACOST
JUPITER Reportes de Emisión Central	En funcionamiento	AGJ	ACOST
JUPITER Servicios al Contribuyente	En funcionamiento	AGJ	ACOST
Listados de conceptos IETU	En funcionamiento	AGR	ACOST
MAEFIEL	En funcionamiento	AGSC	ACOST
Manifiesto Único Ferroviario	En funcionamiento	AGA	AGA
MAT - Control de Obligaciones	En funcionamiento	AGR	ACOST
MAT- Sistema de Devoluciones Automáticas	En funcionamiento	AGAFF	ACOST
MAT-NyV: Módulo de impresión de actos administrativos para notificación personal	En funcionamiento	AGR	ACOST
MAT-NyV: Módulo de Notificación electrónica	En funcionamiento	AGR	ACOST
Modelo de Administración de Riesgo Corrupción	En funcionamiento	AGE	ACOST
Modelo de Administración Tributaria de Cobranza	En funcionamiento	AGR	ACOST
Modelo de Administración Tributaria Devoluciones y Compensaciones	En funcionamiento	AGAFF	ACOST

Nombre del Sistema	Estado del Sistema	AG dueña del aplicativo	Custodia
Modelo de Administración Tributaria Proceso Masivo de Inscripción	En funcionamiento	AGSC	ACOST
Monitor de Lotes "Modelo" (NEPE)	En funcionamiento	AGR	ACOST
MORSA IVA	En funcionamiento	AGP	ACOST
Movimientos SAC	En funcionamiento	AGSC	ACOST
Nómina RIF	En funcionamiento	AGSC	ACOST
Notificación por Estrados o Edictos	En funcionamiento	AGR	ACOST
Opinión del Cumplimiento del Contribuyente	En funcionamiento	AGR	ACOST
Pasaporte Electrónico de Aduanas	En funcionamiento	AGA	AGA
PNR - Passenger Name Record	En funcionamiento	AGA	AGA
Portal AGRS de la IntraSAT	En funcionamiento	AGRS	ACOST
Portal empleado de consulta de documentos digitales	En funcionamiento	AGR	ACOST
Reconocimiento Aduanero	En funcionamiento	AGA	AGA
Régimen de Incorporación al Seguro Social (RISS-IMSS E INFONAVIT)	En funcionamiento	AGSC	ACOST
Registro de Contadores Públicos y Despachos	En funcionamiento	AGAFF	ACOST
Registro y Control de Bienes Embargados	En funcionamiento	AGR	ACOST

Nombre del Sistema	Estado del Sistema	AG dueña del aplicativo	Custodia
Reimpresión de acuses	En funcionamiento	AGR	ACOST
Resultados Evaluación Minnesota Recursos Humanos	En funcionamiento	AGE	ACOST
SAT-Móvil: Re-ingeniería del servicio de Factura Electrónica Móvil	En funcionamiento	AGSC	ACOST
Sede Electrónica Buzón Tributario	En funcionamiento	AGR	ACOST
Servicio de DyP	En funcionamiento	AGR	ACOST
SIOS Devoluciones y Compensaciones	En funcionamiento	AGAFF	ACOST
Sistema Automatizado Integral de Marbetes y Precintos	En funcionamiento	AGSC	ACOST
Sistema de Análisis Automatizado a Priori Aduanal	En funcionamiento	AGA	AGA
Sistema de Asignación y Donación de Bienes por el SAT	En funcionamiento	AGRS	ACOST
Sistema de Capital humano	En funcionamiento	AGRS	ACOST
Sistema de Captación de Documentos Digitales	En funcionamiento	AGR	ACOST
Sistema de Captura de Parámetros	En funcionamiento	AGAFF	ACOST
Sistema de Códigos de Tabacos	En funcionamiento	AGSC	ACOST

Nombre del Sistema	Estado del Sistema	AG dueña del aplicativo	Custodia
Sistema de Control de Agentes y Apoderados Aduanales	En funcionamiento	AGA	AGA
Sistema de Control de Catálogos	En funcionamiento	AGA	AGA
Sistema de Control de Cuentas de Créditos y Garantías	En funcionamiento	AGACE	ACOST
Sistema de Control de Devoluciones	En funcionamiento	AGAFF	ACOST
Sistema de Control de Registro de Denuncias	En funcionamiento	AGE	ACOST
Sistema de Control y Seguimiento de Muestras	En funcionamiento	AGA	AGA
Sistema de Denuncias, Quejas y Supervisiones	En funcionamiento	AGE	ACOST
Sistema de Firmado Electrónico de Notificaciones	En funcionamiento	AGR	ACOST
Sistema de Importación y Exportación Temporal de Remolques y Semi remolques	En funcionamiento	AGA	AGA
Sistema de Incidencias y Alertas	En funcionamiento	AGA	AGA
Sistema de Indicadores de la AGE	En funcionamiento	AGE	ACOST
Sistema de Monitoreo de Auditoria	En funcionamiento	AGAFF	ACOST

Nombre del Sistema	Estado del Sistema	AG dueña del aplicativo	Custodia
Sistema de Operaciones de Comercio Exterior	En funcionamiento	AGA	AGA
Sistema de Revocación con Firma Electrónica	En funcionamiento	AGSC	ACOST
Sistema de Seguimiento y Control de Licitaciones	En funcionamiento	AGRS	ACOST
Sistema de Seguridad para el Monitoreo de Aplicaciones	En funcionamiento	AGE	ACOST
Sistema Electrónico para Declaración Aduanal de Pasajeros	En funcionamiento	AGA	AGA
Sistema Integral de Comprobantes	En funcionamiento	AGSC	ACOST
Sistema Único de Información Integral	En funcionamiento	AGAFF	ACOST
Sistema Único de Información para Entidades Federativas Integral	En funcionamiento	AGAFF	
Solicitud de Certificados Digital	En funcionamiento	AGSC	ACOST
Solución Integral Servicios al Contribuyente	En funcionamiento	AGSC	ACOST
Test de Compatibilidad y Valores (antes llamado Sistema de evaluación de Integridad)	En funcionamiento	AGRS	ACOST
Tránsitos sin Papel	En funcionamiento	AGA	AGA

Nombre del Sistema	Estado del Sistema	AG dueña del aplicativo	Custodia
Vacaciones y Permisos al Personal	En funcionamiento	AGRS	ACOST
Visor de acciones de Control de Obligaciones	En funcionamiento	AGR	ACOST
Visualizador de declaraciones de PEMEX	En funcionamiento	AGR	ACOST
Webservice externos (IMSS e INFONAVIT)	En funcionamiento	AGSC	ACOST

Capítulo IV
Funciones y obligaciones de las personas que traten datos personales

1. Las funciones de los empleados del SAT, que manejen datos personales y/o datos personales sensibles, serán aquellas que hayan sido autorizadas expresamente, en sus descriptivos de puesto, o bien en el documento de designación de funciones o actividades emitido por sus superiores jerárquicos.

2. Asimismo, aquellos servidores públicos que generen, consulten, o traten con datos personales, deben adoptar las medidas de seguridad previstas en el capítulo denominado "**Mecanismos de monitoreo y revisión de las medidas de seguridad**", del presente documento.

3. Estarán obligados a conocer y aplicar el marco jurídico y normativo emitido por el INAI, SAT y SFP en materia de transparencia, acceso a la información y protección de datos personales; y lo citado por el Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia digital Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información así como el Manual Administrativo de Aplicación General en dichas matérias.

4. De igual forma los principios y directrices que rigen la actuación de los servidores públicos en el marco normativo vigente, como lo es la Ley General de Responsabilidades Administrativas, el Código de conducta del SAT y el Código de Ética de las personas públicas del Gobierno Federal.

Adicionalmente, el SAT cuenta con una Estrategia Institucional de Seguridad en Tecnologías de la Información, la cual está conformada por un modelo de gobierno donde participan:

- Grupo de trabajo Estratégico de Seguridad de la Información (GESI) (Conformado por los Administradores centrales de la AGCTI).
  Responsable de aprobar las acciones a implementar en materia de:
  - Programa de análisis de riesgos.
  - Resolución de las problemáticas derivadas de la implementación de controles de seguridad de la información y manejo de riesgos.
  - Programas para el desarrollo, actualización y/o pruebas de los planes de continuidad.
- Responsable de Seguridad de la Información en la Institución (Administrador General de Comunicaciones y Tecnologías de la Información), a cargo de:
  - Autorizar la Estrategia Institucional de Seguridad en Tecnologías e Información (EINSTEIN).
  - Autorizar las Directrices de operación en materia de seguridad de la información aplicables a los servidores públicos y terceros del SAT.
  - Autorizar el Programa de seguridad de la información.
- Responsable de Seguridad de la Información en la Institución Suplente, a cargo de:
  - Establecer el Grupo Estratégico de Seguridad de la Información (GESI).
  - Coordinar las acciones y resultados de ejecución de la estrategia y programas de seguridad.
  - Coordinar las actividades de seguridad de la información del SAT.
  - Asegurar la comunicación con el GESI sobre:
    - Los indicadores de seguridad de la información.
    - Continuidad operativa institucional.
    - Programa de controles mínimos de seguridad de la información.
    - El programa de Seguridad de la Información.
  - Convocar a los Administradores de la Administración Central de Monitoreo y Control (ACSMC) en caso de que requiera atender alguna problemática en seguridad de la información.
- Grupo de trabajo de implementación de Seguridad de la Información (GISI) (Conformado por personal del SAT responsable de controles de seguridad de la información), a cargo de:

- Diseño de los controles de seguridad que resulten del plan de tratamiento de riesgos que emita el Equipo de Infraestructura Crítica y Análisis de Riesgos (EICAR)
- Definir el alcance del programa de implementación de controles mínimos de seguridad, coordinar su validación y supervisar su implementación.
- Ejecutar el "Programa de implementación de controles y contingencia de riesgos" y el "Programa de implementación de controles mínimos".
- Definir acciones de mejora derivado de la medición de eficiencia de los controles de seguridad.
- Designar al Responsable de la Supervisión de la Implementación de los Controles de Seguridad de la Información y manejo de riesgos (RSICSI), quien supervisará el diseño, implementación y seguimiento de los controles de seguridad de la información.

Capítulo V
Análisis de riesgo

En el SAT, se cuenta con procesos sistemáticos, documentados, que constituyen el Sistema de Gestión de la Seguridad de la Información, preservando la documentación tanto física y electrónica que contienen datos personales y datos personales sensibles.

Existen diversas metodologías para la gestión de riesgos, pero comparten algo en común: identificar los activos de información, es decir, todos los recursos involucrados en la gestión de la información, desde los servicios, datos y los equipos físicos (el hardware), hasta los documentos y el personal (recurso humano). Sobre estos activos de información se hace la identificación de las amenazas y las vulnerabilidades que establecen los riesgos para su tratamiento.

La gestión de riesgos, proporciona al SAT la oportunidad de identificar los riesgos, para implementar los controles que permiten actuar ante una eventual materialización que evite algún impacto adverso. Esta gestión se mantiene en constante mejora y en equilibrio entre el costo que tiene la implementación del control, la importancia del activo de información para los procesos y el nivel de riesgo, con la criticidad de la infraestructura.

El resultado obtenido será un reporte ejecutivo de análisis de riesgos que contiene:

a) Alcance
b) Objetivo
c) Resumen de eventos (Metodología)
d) Resultado de la evaluación
e) Conclusiones

Dentro de los resultados de la evaluación, se describen los escenarios de riesgo identificados (considerando las amenazas y vulnerabilidades), se proponen las alternativas de control para el plan de tratamiento y las acciones de remediación en el diseño e implementación de los controles de seguridad de la información.

Estos resultados se integran dentro del documento "MAAGTICSI ASI F3 Documento de resultados del análisis de riesgos".

Capítulo VI
Análisis de brecha

A través de este mecanismo, será posible identificar la diferencia que existe entre el estado actual en que se encuentra el SAT, en materia de seguridad de la información y las mejores prácticas en la materia.

En este organismo administrativo desconcentrado, realizamos la siguiente serie de pasos:

1.- Identificar lo que se tiene o hace en la actualidad en materia de seguridad de la información.
2.- Analizar de acuerdo con las mejores prácticas aplicables en materia de seguridad de la información lo que debería ser.
3.- Detectar cuál es la brecha existente entre el deber ser a lo que actualmente se tiene.
4.- Proponer cómo se podría cubrir esa brecha y en cuánto tiempo.

Capítulo VII
Plan de trabajo

El plan de trabajo considera como prioridad los aplicativos listados en la página 10 del presente documento, posterior al Inventario de datos personales y de los sistemas de datos personales.

Las fases del plan de trabajo son las siguientes:

- Fase I. Identificación de responsables.
- Fase II. Comprobación de la información recolectada.
- Fase III. Actualización.

Capítulo VIII
Mecanismos de monitoreo y revisión de las medidas de seguridad

A1. Aplicable para los sistemas del Servicio de Administración Tributaria

I. Transmisiones de datos personales

1. Transmisiones mediante el traslado de soportes físicos:

C: Confidencial / I: Integridad / D: Disponibilidad

Tipo de control	Propiedad de información	Descripción del control
Administrativo	C, I	**Tipo de transmisión** 1. Los empleados del SAT que requieran el envío de documentación, realizan la solicitud al enlace administrativo (mensajería oficial). Para los documentos que contienen información reservada y/o confidencial, se especifica la clasificación del documento en la portada del sobre, en el extremo inferior derecho de manera visible.
Físico	C, I	**Integridad del paquete (Envío)** La transmisión de documentos con información reservada o confidencial se realiza en un sobre debidamente sellado con cinta adhesiva; y sobre dicha cinta se estampará la firma del remitente, con la finalidad de que sea perceptible si fue abierto antes de su entrega.
Administrativo / Físico	C, I	**Integridad del paquete (Recepción)** En caso que el destinatario identifique alteraciones en el paquete, se sigue el procedimiento definido en el punto 4.19.3 de las Directrices de Operación en materia de Seguridad de la Información aplicables a los Servidores Públicos y Terceros del Servicio de

Tipo de control	Propiedad de información	Descripción del control
		Administración Tributaria, se notifica al remitente y se registra el incidente.
Físico	C	**Entrega del paquete** 1. La entrega del paquete, se realiza sólo si el destinatario acredita su identidad. Para ello, deberá presentar una identificación oficial vigente con fotografía. El mensajero recaba nombre, número de referencia que aparece en la identificación y fecha de entrega. 2. El mensajero no entrega el paquete, si el destinatario no puede acreditar su identidad. En este caso, lo devuelve al remitente.
Físico	C	**Acuse de recibo / Mecanismo de monitoreo** Se utiliza el mecanismo de atentas notas como bitácora de envío, acuse de recibo y para la verificación del destinatario. Para el caso de transferencia de datos personales a otras dependencias o entidades, se debe registrar en el sistema persona.

2. Transmisiones mediante el traslado físico de soportes electrónicos:

Tipo de control	Propiedad de información	Descripción del Control
Administrativo	C, I	**Tipo de transmisión** 1. Los empleados internos del SAT que requiera el envío de documentación, realizan la solicitud al enlace administrativo (mensajería oficial). 2. Para los documentos que contienen información reservada y/o confidencial, se especifica dicha naturaleza en la portada del sobre, en el extremo inferior derecho de manera visible.

Tipo de control	Propiedad de información	Descripción del Control
Técnico / Físico	C, I	**Integridad del paquete (Envío)** 1. La transmisión de soportes electrónicos con información reservada o confidencial, se realiza mediante un proceso de cifrado que los protege durante su trayecto, aplicando un nivel de cifrado robusto y con ayuda de algoritmos asimétrico a través de la e.firma. 2. Posteriormente se guardan en un sobre debidamente sellado con cinta adhesiva y sobre dicha cinta se estampará la firma del remitente, con la finalidad de que sea perceptible si fue abierto antes de su entrega.
Administrativo / Físico	C, I	**Integridad del paquete (recepción)** En el caso de que el destinatario identifique alteraciones en el paquete, se sigue el procedimiento definido en las Directrices de Operación en materia de Seguridad de la Información aplicables a los Servidores Públicos y Terceros del Servicio de Administración Tributaria, se notifica al remitente y se registra el incidente.
Físico	C	**Entrega del paquete** 1. La entrega del paquete se realiza sólo si el destinatario acredita su identidad. Para ello, deberá presentar una identificación oficial vigente con fotografía. El mensajero recaba nombre, número de referencia que aparece en la identificación y fecha de entrega. 2. El mensajero no entrega el paquete si el destinatario no puede acreditar su identidad. En este caso, lo devuelve al remitente.

Tipo de control	Propiedad de información	Descripción del Control
Físico	C	**Acuse de recibo** Se utiliza el mecanismo de atentas notas como bitácora de envío, acuse de recibo y para la verificación del destinatario. Para el caso de transferencia de datos personales a otras dependencias o entidades se debe registrar en el sistema persona.
Técnico	C, I	**Cifrado de contenido** La información trasladada en soportes electrónicos, se cifra utilizando un algoritmo asimétrico y con ayuda de la e.firma.

3. Transmisiones mediante el traslado sobre redes electrónicas:

Tipo de control	Propiedad de información	Descripción del Control
Técnico	C, I	**Cifrado de contenido** La información trasladada en soportes electrónicos se cifra utilizando un algoritmo asimétrico y con ayuda de la e.firma o aquellos expedidos por una autoridad certificadora que se acuerde previamente. Adicionalmente, se utilizan: 1. WS Policy y Security para el uso de Web Services 2. Certificados digitales autogenerados (siempre previo a ello, se comparta el certificado de la autoridad certificadora que los expide).

Tipo de control	Propiedad de información	Descripción del Control
Administrativo / Técnico	C, I	**Protección de canal** <u>Red Interna</u> 1. Para la comunicación de datos sobre redes electrónicas, se utiliza seguridad sobre redes MPLS. Adicionalmente, se cifra el canal de transporte con SSL. <u>Terceros</u> 1. La información transmitida a otras dependencias o entidades que se realiza a través de redes electrónicas, utiliza el servicio de Socket Seguro (medio cifrado utilizando el algoritmo AES256). 2. Para internet, dependiendo del tipo de información que se transporte, se utiliza sólo SSL o si es información sensible y crítica, se emplea autenticación mutua utilizando dos certificados digitales en formato x.509. Para ambas partes, Red interna y terceros, se utiliza: a. Servicio de SSL VPN b. Servicio de VPN para configuración y mantenimiento de equipos. c. Servicio de Socket de seguridad d. Servicio de Protección por HTTPS e. Protección por certificados - SSL f. Túnel de IPSEC g. Servicio de SSH

Tipo de control	Propiedad de información	Descripción del Control
Técnico	C, I, D	**Detección y prevención de intrusos en canal** El SAT cuenta con mecanismos de detección de intrusos, firewalls e IPS implantados en las fronteras de la red de los centros de datos. Adicionalmente, se utiliza: 1. Servicio de escaneo en la recepción y envió de correo electrónico 2. Servicio de protección de puestos de servicio (Host IDS) 3. Servicio de Firewalls Aplicativo 4. Servicio de Seguridad perimetral 5. Servicio de Separación de capas entre centros de datos. Servicio de Detección y Protección Contra Amenazas Avanzadas
Técnico	I	**Acuse de recibo** Todo intercambio de información que constituya un trámite fiscal, es entregado a través de un acuse con sello digital del SAT. Adicionalmente se utiliza: Time stamp.

II. Resguardo de sistemas de datos personales con soportes físicos

Tipo de control	Propiedad de información	Descripción del control
Físico	C	**Resguardo físico de documentos** 1. Los empleados del SAT que fungen como custodios de información, resguardan la información que está clasificada como confidencial en gavetas o estantes con cerradura.

Tipo de control	Propiedad de información	Descripción del control
		2. Los formatos impresos, documentos y expedientes, están foliados y/o engargolados. 3. La información reservada (con nivel alto) es resguardada en áreas de seguridad (bóvedas), las cuales cuentan con mecanismos para regular la temperatura y humedad, sistemas de detección y supresión de incendios, suministro continuo de energía eléctrica, controles y bitácoras de acceso, cámaras de seguridad, entre otras medidas.
Administrativo	C, I	**Responsabilidad de resguardo y protección** 1. Los custodios de la información reservada, definen al personal autorizado para su acceso. 2. Se registran en una bitácora, los accesos a la información, indicando nombre del empleado, fecha, hora, número de expediente solicitado y justificación de consulta.

III. Bitácoras para accesos y operación cotidiana

Tipo de control	Propiedad de información	Descripción del control
Administrativo / Físico / Técnico	C,I,D	**Generación de bitácoras** 1. Los empleados del SAT que fungen como custodios de información, resguardan la información confidencial en gavetas o estantes con cerradura. 2. Los formatos impresos, documentos y expedientes, están foliados y/o engargolados.

Tipo de control	Propiedad de información	Descripción del control
		3. Los custodios de la información reservada, definen al personal autorizado para su acceso. 4. Se registran en una bitácora, los accesos a la información, indicando nombre del empleado, fecha, hora, número de expediente solicitado y justificación de consulta. Los sistemas que contienen datos personales, generan bitácoras de acceso o modificación a la información por parte de los usuarios, mismas que pueden ser sujetas de auditoría. Todo sistema y/o herramienta utilizado en el SAT deberá contener pistas de auditoria, trabajando en conjunto con diferentes áreas (Arquitectura de seguridad, Soluciones de Negocio, Desarrollo y Monitoreo y Control Deberán apegarse al MTR denominando "Lineamientos para la generación de Pistas de Auditoria". En caso de no contar con pistas de auditoria, se deberá evaluar la posible reingeniería o la causal de baja o en su caso el motivo de que continúe operando, para lo cual se debe firmar la aceptación de Riesgo. La Auditoria, se deberá realizar por las áreas facultadas al interior del SAT conforme al RISAT vigente, entre las que se encuentra la Administración General de Evaluación (AGE) y el Órgano Interno de Control (OIC), Las auditorías internas son programadas por cada administración y/o área, para determinar riesgos y toma de decisiones.

Tipo de control	Propiedad de información	Descripción del control
		Después de cada auditoria, se generan recomendaciones y/o observaciones, para actualizar procesos de operación.
Técnico	C,I,D	**Tipo de bitácoras** Existen los siguientes tipos de bitácoras: • De acceso de usuarios (Intentos fallidos y exitosos). • Modificación de configuración y privilegios. • Errores en los sistemas. • Log de Transacciones de base de datos Las mismas, se encuentran almacenadas en soporte electrónico, y son explotadas por las herramientas de análisis de auditoría o correlación de eventos.
Técnico	C,I,D	**Análisis de bitácoras** 1. Las áreas de Tecnología de Información y Seguridad (Monitoreo y Control) designan a personal especializado y con la ayuda de las herramientas (correlacionador de eventos y protección de base de datos) se cuenta con el análisis automático y continuo de las bitácoras. 2. Se cuenta con el reporteo de la auditoria concentrada en el correlacionador de eventos el cual se establece periódico o bajo demanda dando atención a las solicitudes que hacen las áreas autorizadas en la institución. 3. Dicha información es analizada de acuerdo a los criterios marcados por las áreas en comento. El área de monitoreo y control cuenta con herramientas de análisis forense para el análisis

Tipo de control	Propiedad de información	Descripción del control
		de bitácoras e información relacionada con incidentes de seguridad para la elaboración de informes o dictámenes que podrán ser utilizados para procesos legales o administrativos ante las autoridades o entidades correspondientes. Se deben considerar los periodos de conservación aplicables a las bitácoras de acuerdo a los requerimientos legales vigentes. Las herramientas de análisis forense, se encuentran bajo resguardo de áreas como AGE (CECTI) y la AGCTI (ACSMC) al interior del SAT, mismas que se apegan conforme a las facultades que les otorga el RISAT.

IV. Registro de incidentes

Tipo de control	Propiedad de información	Descripción del control
Administrativo / Técnico	C,I,D	**Registro de incidentes de seguridad** 1. Conforme a las *Directrices de Operación en materia de Seguridad de la Información aplicables a los Servidores Públicos y Terceros del Servicio de Administración Tributaria*, establecidos a nivel Institucional, los empleados del SAT comunican oportunamente a la AGCTI y a las autoridades competentes los casos detectados respecto al incumplimiento de las directrices de seguridad, así como aquellos relacionados con incidentes de seguridad. 2. La información recabada en el registro de incidentes es: fecha y hora de reporte, identificador del reporte, prioridad, nombre de persona de la mesa de soporte que atiende el caso, descripción detallada del incidente, persona que lo reporta, teléfono de persona que reporta, localidad donde se presenta el

Tipo de control	Propiedad de información	Descripción del control
		incidente, bitácora de actividades, solución, estatus, tiempo de atención del incidente. 3. Los incidentes de seguridad identificados a través de los servicios de la ACSMC son administrados por el proceso de gestión de incidentes de seguridad que, en su caso, de ser identificados con afectación mayor serán atendidos por el Líder del Equipo de Respuesta a Incidentes de Seguridad Críticos (ERISC) y el personal asignado a este fin. Si del análisis se considera necesario se notifica al CISEN a través del enlace. 4. Se notifica a la AGE, cualquier requerimiento de información relacionado con: Pistas de auditoría, análisis forenses, etc. Lo anterior, en el entendido de que la AGE es el único canal para gestionarlo ante la AGCTI.
Técnico	C,I,D	**Protección de reportes de incidentes** 1. El registro de incidentes se realiza a través de medios electrónicos que se encuentran en los centros de datos (Triara Querétaro, INFOTEC, CPN y los que el SAT implemente), los cuales cuentan con controles de seguridad física en los centros de datos. 2. La herramienta de Administración de Incidentes cuenta con mecanismos de validación de integridad de la información y se complementa con un proceso periódico de mantenimiento de sus componentes. 3. La autorización para recuperación de datos de la herramienta de Administración de Incidentes es otorgada por la Administración Central de Operaciones y Servicios Tecnológicos.

V. Acceso a las instalaciones

Tipo de control	Propiedad de información	Descripción de control
Físico	C,I,D	**Seguridad perimetral exterior** <u>Para las personas que acceden a las áreas de operación del SAT.</u> 1. El personal externo es registrado en el área de seguridad exterior, el personal de vigilancia se encarga de la validación y autentificación de los datos recibidos, contra el permiso de acceso registrado en su sistema de accesos. Una vez autenticado el personal (interno y externo), se continúa con la revisión física de sus pertenencias por el personal de seguridad. 2. El personal interno del SAT se autentica mediante un sistema con doble factor: Credencial magnética y biométricos. 3. El personal externo con acceso permanente, se autentica con un sistema de credencial y lector de scanner. <u>Para el personal que accede a los Centros de datos</u> Triara Querétaro, INFOTEC, CPN y los que el SAT implemente. 1. Todo el personal (Interno y externo) que accede debe solicitar su ingreso con al menos 24 horas de anticipación ante un área autorizada del SAT, enviando los datos completos que garanticen su identificación física, la institución o razón social a la que pertenece, el objetivo de su visita y el período de tiempo que estará dentro de las instalaciones.

Tipo de control	Propiedad de información	Descripción de control
Físico	C,I,D	**Seguridad perimetral interior** 1. Una vez realizada la identificación, autentificación y revisión física de las pertenencias del personal que solicita el acceso, el área de seguridad lo dirige ante personal del SAT para su atención, donde se realiza una nueva identificación y se da el aviso al área del SAT que tramitó el acceso, confirmando su arribo. El área del SAT que originó el trámite es quien autoriza el acceso al área restringida para dar inicio a sus labores. 2. Todo acceso a las áreas restringidas, cuenta con mecanismos de control a través de tarjetas electrónicas de proximidad programadas para permitir el acceso exclusivamente a las áreas que corresponden al SAT. Estas tarjetas sólo la porta el personal del SAT y son ellos quienes trasladan al visitante hasta las áreas restringidas, previo registro del visitante en la bitácora física de accesos. 3. El ingreso al búnker de producción del SAT, está controlado mediante un mecanismo biométrico en el que sólo personal del SAT está registrado, siendo necesario que el visitante esté siempre acompañado para poder ingresar o retirarse.

VI. Actualización de la información contenida en el sistema

Tipo de control	Propiedad de información	Descripción de control
Técnico	C,I,D	**Protección de Base de datos** 1. La actualización a la información contenida en el sistema se realiza, únicamente por medio de la aplicación desarrollada para tal fin, 2. Para garantizar que la información se actualice por el medio y usuario autorizado, las bases de datos cuentan con agentes de aseguramiento, los cuales envían auditoría a un componente externo a la base de datos que se está protegiendo, dicha auditoría se valida y si cumple con un comportamiento diferente al autorizado, se alerta con un correo electrónico al equipo de análisis de incidentes de seguridad, dicho comportamiento puede ser bloqueado por el mismo agente de protección. El componente externo se encuentra custodiado en el mismo centro de datos de la institución.

VII. Perfiles de usuario y contraseñas (soporte electrónico)

Tipo de control	Propiedad de información	Descripción de control
Técnico	C,I	**Modelo de control de acceso** 1. El modelo de control de acceso en el SAT se sustenta en una solución de control de acceso basado en roles y que son administrados en un sistema centralizado de manejo de identidades. 2. Para la gestión de identidades, se cuenta con servicios de directorio ex profeso para los contribuyentes que se encuentran enrolados por el SAT y otro separado para los

Tipo de control	Propiedad de información	Descripción de control
		empleados y usuarios externos que guardan estrecha relación en el consumo de los servicios de información que el SAT provee. Los roles le son asignados exclusivamente para el desempeño de sus funciones.
Técnico	C,I,D	**Perfiles de usuario y contraseñas (Sistema operativo de red)** 1. Los permisos de acceso a los sistemas que se encuentran en la infraestructura tecnológica del SAT, son proporcionados con base en los principios de la "necesidad de saber" y el "menor privilegio", por lo cual los usuarios solo deben ingresar a las aplicaciones, sistemas y recursos del SAT que les fueron asignados para el desempeño de sus funciones. **2.** Los usuarios deben tener conocimiento de las cuentas de acceso, contraseñas, certificados digitales y otros mecanismos de autenticación a sistemas y aplicaciones del SAT, éstos tienen carácter de personal, confidencial e intransferible, son sujetos de monitoreo y pueden ser auditados en cualquier momento. Se tiene un driver (proceso automático), que procesa las bajas que RH provee cada que hay movimientos de este tipo y la cuenta de usuario en el DII se deshabilita y a su vez también se eliminan los roles que permitían al usuario tener acceso a los aplicativos que autentican en dicha solución. Se tiene un driver (proceso automático) que elimina los roles en el DII, cuando existe un cambio de adscripción para el empleado, desde nivel Administración, Central y General.

Tipo de control	Propiedad de información	Descripción de control
		Para los sistemas legados, actualmente se hace manualmente con una revisión de facultades y a petición del Negocio
Administrativo / Técnico	C,I	**Perfiles de usuario y contraseñas (Sistema de datos personales)** 1. La herramienta de manejo de identidades implantada en el SAT, permite un manejo riguroso de usuarios y contraseñas, así como el cifrado de la información, de manera que se cumpla con lo establecido en los *Directrices de Operación en materia de Seguridad de la Información aplicables a los Servidores Públicos y Terceros del Servicio de Administración Tributaria.* 2. Los permisos de acceso a los sistemas que se encuentran en la infraestructura tecnológica del SAT, son proporcionados con base en los principios de la "necesidad de saber" y el "menor privilegio", por lo cual los usuarios solo deben ingresar a las aplicaciones, sistemas y recursos del SAT que les fueron asignados para el desempeño de sus funciones. 3. Los usuarios deben tener conocimiento de las cuentas de acceso, contraseñas, certificados digitales y otros mecanismos de autenticación a sistemas y aplicaciones del SAT, éstos tienen carácter de personal, confidencial e intransferible, son sujetos de monitoreo y pueden ser auditados en cualquier momento.
Administrativo / Técnico	C,I	**Administración usuario y contraseñas (Sistema de datos personales)**

Tipo de control	Propiedad de información	Descripción de control
		1. La Administración de Manejo de Identidades y FEA de la Administración Central de Seguridad, Monitoreo y Control, es la entidad a cargo de administrar el repositorio de identidades y de consolidar un registro de acciones de altas, bajas y modificaciones de perfiles. 2. Para efectos de la administración de los roles y perfiles de usuarios internos, en el SAT existe una Unidad Administrativa denominada Administración Central de Capital Humano que es quien se encarga de establecer junto con las áreas de negocio, la equivalencia válida entre un conjunto de habilitadores tecnológicos y las funciones que del usuario interno se esperan. 3. La validación y autorización para la generación de nuevos roles y perfiles como los cambios durante su evolución en el tiempo se realiza conforme lo establece la matriz de aprobadores jerárquicos y de información.
Administrativo / Técnico	C,I	**Acceso remoto a sistemas de datos personales** 1. La Administración Central de Seguridad, Monitoreo y Control, determina el flujo de actividades y autorizaciones que son requeridas para que entidades externas o terceros, a través de sistemas de información identificados, intercambien información con el SAT usando las tecnologías Token de Sesión de Servicios o Socket de Seguridad, Autenticación mutua con certificados, autenticación con usuarios aplicativos, etc, así como la forma de conectarse al SAT, tal como lo especifica la Guía de operaciones para conexión por entidades externas o terceros al SAT del SAT.

Tipo de control	Propiedad de información	Descripción de control
		La Administración Central de Operaciones y Servicios de Tecnología, administra y opera los servicios, enlaces y equipos productivos a través de los mecanismos definidos por la Administración de Arquitectura de Seguridad.

VIII. Procedimientos de respaldo y recuperación de datos (soporte electrónico)

Tipo de control	Propiedad de información	Descripción de control
Técnico	D	**Generación de respaldos** 1. La operación de los respaldos en los Centros de Datos (Triara Querétaro y Triara Monterrey) se realiza en primera instancia hacia disco duro; y posteriormente, hacia cinta magnética, conservando al menos dos respaldos actuales dentro del disco duro inteligente y las bibliotecas de cintas conectadas en la red de almacenamiento. 2. La información se respalda inicialmente de manera completa, ejecutando actualizaciones incrementales periódicas de acuerdo con la programación definida entre el programador y las áreas de soporte a la aplicación.
Técnico	D	**Protección de respaldos** 1. Los respaldos de uso cotidiano son realizados en cintas que se almacenan dentro de los equipos encargados de su operación (bibliotecas automatizadas de cintas) dentro de los centros de datos del SAT. 2. Las cintas magnéticas DLT y LTO con respaldos históricos extraídas de los robots,

Tipo de control	Propiedad de información	Descripción de control
		son almacenadas en una cintoteca interna, a la cual sólo personal del SAT tiene acceso.
Técnico	D	**Responsabilidad de respaldos** La Administración Central de Operaciones y Servicios de Tecnología es responsable de establecer el alcance de los respaldos, con base en los requisitos establecidos por el usuario del mismo y apoyados por el área de infraestructura interna del SAT, quienes en conjunto establecen las políticas de respaldo y quedan con la responsabilidad de la ejecución del programa solicitado.

IX. Borrado seguro de medios

Tipo de control	Propiedad de información	Descripción de control
Administrativo / Técnico	C	Borrado Seguro de Servidores 1. Cuando se daña, migra o finaliza el ciclo de vida de los componentes que almacenaron información, se realiza el borrado seguro del cual se obtiene un certificado que cumple con estándares internacionales y se asegura mediante análisis forense que no hay información legible en el componente. Para poder retirar algún componente del centro de datos donde se encuentre alojado, se deberá entregar el certificado de borrado seguro y si no fue posible obtenerlo o no se tiene la certeza de que no contiene información legible se procede a la destrucción del medio.
Técnico	C	Borrado Seguro de Puestos de Servicio 1. Cuando se da de baja un empleado o se realiza la actualización tecnológica en la institución, se realiza el borrado seguro de todos los equipos del cual se obtiene un certificado que cumple con estándares internacionales. Se realiza borrado seguro a terceros asignados a la institución cuando finaliza su asignación.

Capítulo IX
Programa general de capacitación

Con la finalidad de dar cumplimiento a lo establecido en la Ley General de Transparencia y Acceso a la Información Pública, relacionada con la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, el Comité de Transparencia del SAT durante el año 2017, capacitó en la modalidad presencial a los servidores públicos del SAT, con el curso denominado ***"Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados"***, *con* dicho curso se logró actualizar al personal encargado de atender las solicitudes de información, recursos de revisión, así como a aquellas personas interesadas en la materia de protección de datos personales.

En 2018, se brindó capacitación a los servidores públicos del SAT, en materia de Protección de Datos personales, en la modalidad en línea en el Centro Virtual de Capacitación en Acceso a la Información y Protección de Datos (CEVINAI) del INAI, de conformidad con lo establecido en el ***"Programa de Capacitación en Transparencia, Acceso a la Información, Protección de Datos Personales y Temas relacionados- 2018"***, formalizado cada año por parte de los miembros del Comité de Transparencia del Servicio de Administración Tributaria (SAT), el Enlace de Capacitación en Transparencia del SAT, ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

El documento de seguridad, se actualizará de conformidad con lo establecido en el artículo 36 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Capítulo X
Control de cambios

Versión No.	Fecha de elaboración	Descripción del cambio
1	10/09/2018	Emisión de Guía

Capítulo XI
Términos y acrónimos

Término	Descripción	Acrónimo
Administración General de Comunicaciones y Tecnologías de la Información.	Administración General del SAT encargada de despachar asuntos en materia de comunicaciones y tecnologías de la información	AGCTI
Confidencial	Referente a una propiedad o característica de los datos personales e información que se maneja en los sistemas del SAT.	C
Comité de Transparencia del SAT	Órgano colegiado del SAT, integrado por el responsable del área coordinadora de archivos o equivalente, el titular de la Unidad de Transparencia y el titular del Órgano Interno de Control de conformidad con lo establecido en la LFTAIP	CTSAT
Disponibilidad	Referente a una propiedad o característica de los datos personales e información que se maneja en los sistemas del SAT.	D
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	DP
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	DPS
Documento de Seguridad	Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el SAT,	DS

Término	Descripción	Acrónimo
	para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.	
Integridad	Referente a una propiedad o característica de los datos personales e información que se maneja en los sistemas del SAT.	I
Medidas de Seguridad	Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales	MS
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.	MSA
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 del SAT, sus instalaciones físicas, áreas críticas, recursos e información; b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas del SAT, recursos e información; c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir del SAT, y d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad	MSF
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;	MST

Término	Descripción	Acrónimo
	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;	
Servicio de Administración Tributaria	Órgano Administrativo Desconcentrado de la Secretaría de Hacienda y Crédito Público, el cual recauda los recursos tributarios y aduaneros que la ley prevé, dotando al contribuyente de las herramientas necesarias que faciliten el cumplimiento voluntario.	SAT
Seguridad de la Información	Es la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma.	SI
Sujeto Obligado	Cualquier autoridad, entidad, órganos autónomos, partidos políticos, fideicomisos y fondos público que tome decisión en cuanto al tratamiento de datos personales de acuerdo a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados	SO
Tecnologías de Información y Comunicaciones	Comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y videos	TIC
Unidad de Transparencia	Encargada de recabar y difundir información relativa a las obligaciones de transparencia, recibir y dar trámite las solicitudes de acceso a la información; así como proponer e implementar acciones conjuntas para asegurar una mayor eficiencia en los procesos de transparencia y protección de datos personales al interior del SAT	UT