TFJA

TRIBUNAL FEDERAL
DE JUSTICIA ADMINISTRATIVA

DOCUMENTO DE SEGURIDAD

19 DE SEPTIEMBRE DE 2019

Índice

I.	OBJETIVO DEL DOCUMENTO DE SEGURIDAD	2
II.	MARCO JURÍDICO	4
III.	DESARROLLO DEL DOCUMENTO DE SEGURIDAD	5
	A. SECRETARÍA OPERATIVA DE ADMINISTRACIÓN	5
	B. SECRETARÍA AUXILIAR DE LA JUNTA DE GOBIERNO Y ADMINISTRACIÓN UNIDAD DE PERITOS.	23
	C. SECRETARÍA OPERATIVA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	36
	D. CENTRO DE ESTUDIOS SUPERIORES EN MATERIA DE DERECHO FISCAL Y ADMINISTRATIVO	48
	E. UNIDAD DE ENLACE/TRANSPARENCIA	60
IV.	BIBLIOGRAFÍA	75

I. OBJETIVO

Cumplir con las disposiciones de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, relativas a la integración de un "Documento de Seguridad", como un instrumento que describa y de cuenta de manera general, sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por este Tribunal, para garantizar la protección de los datos que resguardan las áreas jurisdiccionales y unidades administrativas; de modo que se encuentren protegidos contra daño, pérdida, alteración, destrucción o su uso, acceso y tratamiento no autorizado, así como asegurar su confidencialidad, integridad y disponibilidad.

II. MARCO NORMATIVO

- Constitución Política de los Estados Unidos Mexicanos (artículos 6 y 16).
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Capítulo III De los Deberes, artículos 31 al 42).
- Ley Orgánica del Tribunal Federal de Justicia Administrativa.
- Reglamento Interior del Tribunal Federal de Justicia Administrativa.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público (Capítulo II De los Deberes, Deber de seguridad, artículo 55).

III. DESARROLLO DEL DOCUMENTO DE SEGURIDAD

A. SECRETARÍA OPERATIVA DE ADMINISTRACIÓN

1. Sistemas electrónicos de la Secretaría Operativa de Administración, en los que se recaban, tratan y reguardan datos personales:

a) Nombre del sistema
Sistema Integral de Administración Financiera WIN-SIAF
b) Tipo de soporte en que se encuentra.
Electrónico
c) Tipo de datos que recaban
Datos personales de identificación, ubicación, patrimoniales, laborales, autenticación, académicos, personales de naturaleza pública.
Datos personales sensibles de estado de salud.
d) Finalidad para la que son solicitados y resguardados
Registro y seguimiento de los asuntos concernientes a la Dirección General de Recursos Humanos, Dirección General de Recursos Materiales y Servicios Generales, así como a la Dirección General de Programación y Presupuesto.
e) Plazo de conservación
Indefinido. Los datos obran en el sistema, en tanto los titulares no soliciten su cancelación.

2. Servidores públicos que pueden ingresar al sistema, cargo que ocupan y funciones asignadas:

A modo de que pueda identificarse el número de servidores públicos que utilizan el sistema, a continuación se desglosa la información por puesto, conforme al área de adscripción a la que pertenecen en la Secretaría Operativa de Administración, las funciones que realizan y el nivel de acceso al sistema.

a) Dirección General de Recursos Humanos

Puesto	Número de servidores públicos	Funciones asignadas en materia de transparencia:	Nivel de acceso al sistema
Apoyo de servicios administrativos	10	Clasificar, Registrar, Actualizar, Verificar y Consultar datos laborales, académicos y personales de naturaleza pública	3 Operadores y Usuarios 1 Operador 6 Usuarios

Analista Administrativo	7	Clasificar, Registrar, Actualizar, Verificar y Consultar datos laborales, académicos, electrónicos y personales de naturaleza pública	2 Operadores y Usuarios 4 Operadores 1 Usuario
Secretaria de Secretario de Acuerdos	1	Clasificar, Registrar, Actualizar, Verificar y Consultar datos laborales, académicos, electrónicos y personales de naturaleza pública	Operador y Usuario
Técnico en Administración	4	Clasificar, Registrar, Actualizar, Verificar y Consultar datos laborales, académicos, electrónicos y personales de naturaleza pública	1 Operador 3 Usuarios
Secretaria particular	1	Consultar datos laborales, académicos, electrónicos y personales de naturaleza pública	Usuario
Jefe de Departamento	12	Clasificar, Registrar, Actualizar, Verificar y Consultar datos laborales, académicos, electrónicos y personales de naturaleza pública	4 Operadores y Usuarios 4 Operadores 4 Usuarios
Subdirector de área	9	Clasificar, Registrar, Actualizar, Verificar y Consultar datos laborales, académicos, electrónicos y personales de naturaleza pública	2 Operadores y Usuarios 5 Operadores 2 Usuarios
Director de Modernización Organizacional	1	Administrar, Verificar, Consultar y autorizar actualizaciones de datos laborales, electrónicos y personales de naturaleza pública	Administrador y Usuario
Director de Administración de Personal	1	Clasificar, Registrar, Verificar, Consultar y autorizar actualizaciones a datos laborales, académicos, electrónicos y personales de naturaleza pública	Operador
Director de Nóminas	1	Verificar y Consultar datos laborales, electrónicos y personales de naturaleza pública	Administrador y Usuario

Director General de Recursos Humanos	1	Verificar y Consultar datos laborales, académicos, electrónicos y personales de naturaleza pública	Usuario

b) Dirección General de Recursos Materiales y Servicios Generales:

Puesto	Número de servidores públicos	Funciones asignadas en materia de transparencia:	Nivel de acceso al sistema
Apoyo de servicios administrativos	1	Clasificar, Registrar, Actualizar, Verificar y Consultar datos laborales, electrónicos y personales de naturaleza pública	Operador y Usuario
Técnico en Administración	1	Clasificar, Registrar, Actualizar, Verificar y Consultar datos laborales, electrónicos y personales de naturaleza pública	Operador y Usuario
Analista Administrativo	4	Clasificar, Registrar, Actualizar, Verificar y Consultar datos laborales, electrónicos y personales de naturaleza pública	Operadores y Usuarios
Enlace	1	Clasificar, Registrar, Actualizar, Verificar y Consultar datos laborales, electrónicos y personales de naturaleza pública	Operador y Usuario
Jefe de Departamento	3	Clasificar, Registrar, Actualizar, Verificar y Consultar datos laborales, electrónicos y personales de naturaleza pública	Operadores y Usuarios
Subdirector de área	2	Clasificar, Registrar, Actualizar, Verificar y Consultar datos laborales, electrónicos y personales de naturaleza pública	Operadores y Usuarios
Director de Almacén e Inventario	1	Administrar, Verificar, Consultar y autorizar actualizaciones de datos	Administrador, Operador y Usuario

		laborales y personales de naturaleza pública	
Director General de Recursos Materiales y Servicios Generales	1	Administrar, Supervisar, Verificar, Consultar actualizaciones de datos laborales y personales de naturaleza pública	Usuario

c) Dirección General de Programación y Presupuesto:

Puesto	Número de servidores públicos	Funciones asignadas en materia de transparencia:	Nivel de acceso al sistema
Jefe de Departamento	1	Clasificar, Registrar, Actualizar, Verificar y Consultar datos identificativos, laborales, electrónicos y patrimoniales.	Operador
Jefe de Departamento	3	Revisión y Consultar datos identificativos y patrimoniales.	Usuarios
Subdirector de área	1	Clasificar, Registrar, Actualizar, Verificar y Consultar datos, identificativos laborales, electrónicos y patrimoniales.	Operador
Subdirector de área	1	Revisión y Consultar datos identificativos y patrimoniales.	Usuario
Director de Tesorería y Finanzas	1	Verificar y Consultar datos identificativos, laborales, electrónicos y patrimoniales.	Administrador
Director de Programación y Presupuesto	1	Consultar datos identificativos y patrimoniales.	Usuario
Director General de Programación y Presupuesto	1	Administrar Consultar y autorizar actualizaciones de datos identificativos, laborales, electrónicos y patrimoniales.	Administrador

3. Análisis de riesgo

A continuación se determina el riesgo de que los datos personales contenidos en el Sistema Integral de Administración Financiera WIN-SIAF, puedan sufrir una pérdida o daño, de modo que se identifique la información que por orden de prioridad requiere más protección.

Para ello, se utilizará como criterio orientador la ***Metodología BAA "Beneficio para el atacante, Accesibilidad para el atacante y Anonimidad del atacante"***[1], la cual posibilita medir el riesgo por el tipo de datos y el volumen de titulares que se tratan; por el tipo de acceso, esto es, el número de accesos potenciales a los datos; y, por el tipo de entorno desde el que se tiene acceso a los datos.

a) Riesgo por tipo de dato:

Tipo de dato	Nivel de riesgo inherente	Volumen de titulares	Nivel de riesgo por tipo de dato
Identificación	Bajo	<5K (datos de entre 501 hasta 5000 personas)	Nivel 1*
Ubicación	Medio		
Patrimoniales			
Laborales			
Autenticación			
Académicos	Alto		Nivel 2**
Estado de salud			

* Corresponde al tratamiento de datos de identificación con **riesgo inherente bajo**, por lo que no importa el número de personas titulares; además de los datos de ubicación, patrimoniales, jurídicos y de autenticación con **riesgo inherente medio**, de 501 hasta 5000 titulares de la información.

Corresponde al tratamiento de datos personales sensibles con **riesgo inherente alto, pues su utilización indebida puede dar origen a discriminación, o bien, poner en riesgo grave a los titulares de los datos; con un volumen de titulares de 501 hasta 5,000.

b) Riesgo por nivel de accesibilidad

Accesibilidad*
>20 -<200

* Cantidad de accesos a los datos personales

El número de personas que pueden acceder al Sistema Integral de Administración Financiera WIN-SIAF, a la fecha de la integración del presente documento, son 70 servidores públicos de la Secretaría Operativa de Administración, en las unidades administrativas que dirige,

[1] Disponible para consulta pública en: http://inicio.ifai.org.mx/DocumentosdeInteres/Metodologia_de_Riesgo_BAA_marzo2014.pdf. Fecha de consulta 08 de agosto de 2019.

distribuidos como sigue: Dirección General de Recursos Humanos (48), Dirección General de Recursos Materiales y Servicios Generales (13) y Dirección General de Programación y Presupuesto (9).

c) Riesgo por nivel de anonimidad

Entorno	Nivel de Anonimidad
Red Interna	2

El Sistema Integral de Administración Financiera WIN-SIAF tiene un **Nivel 2 de anonimidad**, ya que los datos permanecen en el sistema, al que únicamente puede accederse desde la red interna del Tribunal, mediante usuario y contraseña proporcionados por la Secretaría Operativa de Tecnologías de la Información y las Comunicaciones.

4. Identificación de Medidas de Seguridad

Al respecto, toda vez que el riesgo de pérdida o daño de los datos personales que se recaban y resguardan en el Sistema Integral de Administración Financiera WIN-SIAF, por el **tipo de dato es nivel 1 y 3, de accesibilidad de 20 a 200 personas y de anonimidad nivel 2**, ya que sólo se puede acceder a los datos a través de la red interna del Tribunal; se identifican las siguientes listas y patrones de control aplicables conforme a la Metodología BAA mencionada:

a) Patrón de control de medidas básicas (CB) aplicables en su totalidad

		Riesgo por tipo de dato 1			
Entornos de acceso	Internet	CB			
	Red terceros				
	WiFi				
	Red interna				
	Físico				
		≤ 20	≤ 200	≤ 2,000	> 2,000
		Cantidad de Accesos/Personas			

b) Listas de medidas administrativas para nivel de riesgo por tipo dato 3 (AD-3) y medidas básicas de seguridad para accesos desde la red interna (RI-3)

		Medidas administrativas aplicables: AD-3			
Entornos de acceso	Internet	RI-2 F-2 DMZ-3	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3
	Red terceros	RI-2 F-2 DMZ-3	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3
	WiFi	RI-2 F-2 DMZ-2	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3
	Red interna	RI-2 F-2	RI-3 F-2	RI-3 F-2	RI-3 F-2
	Físico	F 2	F 2	F 2	F 2
		≤ 20	≤ 200	≤ 2,000	> 2,000
		Cantidad de Accesos/Personas			

Cabe mencionar que a la fecha de la integración del presente documento de seguridad, **no se cuenta con registros de ataques u amenazas que hayan vulnerado las medidas de seguridad** que se tienen para la consulta y operación del Sistema Integral de Administración Financiera WIN-SIAF.

5. Análisis de brecha

Con base a los patrones y listados de medidas de seguridad mencionados, a continuación se enlistan las medidas con las que cuenta la Secretaría Operativa de Administración, para proteger los datos personales que obran en el Sistema Integral de Administración Financiera WIN-SIAF, así como aquellas que se encuentran en proceso de mejora o implementación.

Es necesario mencionar que únicamente se consideraron los controles y medidas que guardan relación con las actividades que lleva a cabo esta Secretaría.

Control/Medida	Parámetro	Estatus
Documentación de política de seguridad de la información	Políticas de seguridad del Tribunal, para la protección de la información que se	HECHO

	resguarda en los diferentes sistemas.	
Revisión de la política de seguridad de la información.	Revisión anual o cuando exista una modificación a las medidas de procesos de seguridad, o a las condiciones de riesgo.	HECHO (*Gap Analysis)*
Acuerdos de confidencialidad: Los requisitos para los acuerdos de confidencialidad o de no revelación deben reflejar las necesidades de protección de información de la organización y deben ser revisados periódicamente.	Revisión anual o por evento.	HECHO
Registro de las actividades que impliquen el tratamiento de datos personales (Bitácora de actividades).	El sistema permite identificar cada uno de los procesos que lleva a cabo el área administrativa, de inicio a fin, y los datos personales que se recaban.	HECHO
Roles y responsabilidades de los servidores públicos, definidos y documentados en concordancia con la política de seguridad de la información.	Manuales de organización y Manuales de procedimiento de la Dirección General de Recursos Humanos, Dirección General de Recursos Materiales y Servicios Generales, Dirección General de Programación y Presupuesto.	HECHO
Términos y condiciones de acceso al sistema: los usuarios, operadores y administradores conocen la responsabilidad del cargo que desempeñan y la seguridad de la información que tratan.	Acuse con la firma del servidor público, respecto de la recepción y conocimiento del Código de Ética del Tribunal Federal de Justicia Administrativa.	HECHO

Concienciación, educación y entrenamiento de seguridad de la información.	Cursos de capacitación en materia de protección de datos personales, enfocados en el tratamiento y conservación de los datos, así como en medidas de seguridad.	HECHO
Administración de medios removibles: discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.	Asignación de discos duros y unidades de almacenamiento USB de manera controlada (Formato de Asignación de Servicios de Cómputo y Comunicaciones)	HECHO
Acuerdos de intercambio de información con instituciones pública externas.	Seguir las disposiciones de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, relativas a la transferencia de datos personales, en aquellos casos en los que no se requiere del consentimiento de los titulares. Aviso de privacidad.	HECHO
Uso de sistema de monitoreo: procedimiento para monitorear el uso de la información y del sistema.	Actualización de la bitácora de transacciones realizadas por los servidores públicos.	HECHO
Registro de usuarios	Existe un procedimiento formal para registrar usuarios, así como para revocar el acceso.	HECHO
Verificación del cumplimiento técnico.	Verificar anualmente los sistemas de información para el cumplimiento de los estándares de seguridad, con base en los resultados del análisis de brecha (*Gap Analysis)* efectuado por la Secretaría Operativa de	HECHO

	Tecnologías de la Información y las Comunicaciones.	
Eliminación o reutilización segura del equipo. Los equipos que contengan medios de almacenamiento deberán revisarse para asegurar la remoción o sobre-escritura apropiada de cualquier información sensible y "software" de autor antes de su eliminación.	Respaldos de información almacenada en los equipos de cómputo de los servidores públicos que sean dados de baja, previo a la reasignación de usuario y contraseña.	HECHO
Controles de código malicioso que prevean la detección, prevención y recuperación de la infraestructura.	Políticas de seguridad informática.	HECHO
Controles de red: las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Políticas de seguridad informática.	HECHO
Registro de auditorías, relacionados con las actividades de los usuarios y eventos de seguridad.	Registrar fecha de acceso, usuario y cambios que, en su caso, realizó.	HECHO
Administración de privilegios. Deberá	Políticas de seguridad informática para la	HECHO

restringirse y controlarse la asignación y uso de privilegios.	asignación de privilegios de accesibilidad.	
Uso de contraseñas	Los usuarios tienen asignada una contraseña para ingresar al Sistema.	HECHO
Equipos desatendidos	El sistema solicita el ingreso de usuario y contraseña a los 10 minutos de inactividad del operador y usuario.	HECHO
Eliminación de los derechos de acceso al sistema.	Baja de usuarios y contraseñas al Sistema Integral de Administración Financiera WIN-SIAF.	HECHO
Controles de acceso a los equipos que resguardan la información.	Usuario y contraseña, esta última que pueda cambiarse constantemente.	HECHO
Eliminación de los datos personales que obran en el Sistema Integral de Administración Financiera WIN-SIAF.	Establecer periodos de conservación de la información resguardada en el Sistema, teniendo como base las disposiciones de la Ley General de Archivo, así como las emitidas por el Tribunal.	HECHO **Acuerdo E/JGA/16/2016 mediante el cual se autorizan los instrumentos de control y consulta archivística del Tribunal Federal de Justicia Fiscal y Administrativa**
Control de vulnerabilidades técnicas del Sistema	Probabilidad de que se ocurran vulnerabilidades y medidas apropiadas para enfrentarlas, con base en el resultado del análisis de brecha (*Gap Analysis)* efectuado por la Secretaría Operativa de Tecnologías de la Información y las Comunicaciones.	HECHO
Respaldo de información	Respaldo de los datos personales e información que se encuentra cargada en el	HECHO

	Sistema, así como la base de datos.	

6. Plan de trabajo para implementar los patrones de control y medidas de seguridad nuevas

De conformidad con el análisis de brecha efectuado, la Secretaría Operativa de Administración identificó un control/medida de seguridad para reforzar la protección de los datos que se encuentran resguardados en el Sistema Integral de Administración Financiera WIN-SIAF, a saber:

a. Periodo de conservación y procedimiento de eliminación de los datos personales que obran en el Sistema Integral de Administración Financiera WIN-SIAF.

A continuación se detallan las acciones que se llevarán a cabo para implementar la medida de seguridad, el objetivo que se persigue y la fecha de avance:

Medida de seguridad	Objetivo	Actividades	Fecha de avance
Periodo de conservación y procedimiento de eliminación de los datos personales que obran en el Sistema Integral de Administración Financiera WIN-SIAF.	Establecer periodos de conservación de la información resguardada en el Sistema, teniendo como base las disposiciones de la Ley General de Archivo, así como las emitidas por el Tribunal.	- Verificar con la Dirección General de Archivos del Tribunal, el periodo de conservación indicado para información electrónica, sobre todo cuando se trata de datos personales. - Establecer, en conjunto con la Secretaría Operativa de Tecnologías de la Información y las Comunicaciones, periodos de respaldo de la información contenida en el Sistema y la eliminación correspondiente.	Enero 2020

7. Señalar los mecanismos de monitoreo y supervisión periódica de las medidas de seguridad, a saber:

Control/Medida	Parámetro	Mecanismos de monitoreo y supervisión
Documentación de política de seguridad de la información	Políticas de seguridad del Tribunal, para la protección de la información que se resguarda en los diferentes sistemas.	Resultados del análisis de brecha (*Gap Analysis)* efectuado por la Secretaría Operativa de Tecnologías de la Información y las Comunicaciones.
Revisión de la política de seguridad de la información.	Revisión anual o cuando exista una modificación a las medidas de procesos de seguridad, o a las condiciones de riesgo.	Resultados del análisis de brecha (*Gap Analysis)* efectuado por la Secretaría Operativa de Tecnologías de la Información y las Comunicaciones.
Acuerdos de confidencialidad: Los requisitos para los acuerdos de confidencialidad o de no revelación deben reflejar las necesidades de protección de información de la organización y deben ser revisados periódicamente.	Revisión anual o por evento.	Documentos firmados con terceros que incluyan el acuerdo de confidencialidad.
Registro de las actividades que impliquen el tratamiento de datos personales (Bitácora de actividades).	El sistema permite identificar cada uno de los procesos que lleva a cabo el área administrativa, de inicio a fin, y los datos personales que se recaban.	Número de modificaciones que se realizan a los registros de actividades del sistema.
Roles y responsabilidades de los servidores públicos, definidos y documentados en concordancia con la política de seguridad de la información.	Manuales de organización y Manuales de procedimiento de la Dirección General de Recursos Humanos, Dirección General de Recursos Materiales y Servicios Generales, Dirección General de	Número de ajustes realizados a los Manuales de organización y Manuales de procedimientos de la Dirección General de Recursos Humanos, Dirección General de Recursos Materiales y

	Programación y Presupuesto.	Servicios Generales, y la Dirección General de Programación y Presupuesto, por año.
Términos y condiciones de acceso al sistema: los usuarios, operadores y administradores conocen la responsabilidad del cargo que desempeñan y la seguridad de la información que tratan.	Acuse con la firma del servidor público, respecto de la recepción y conocimiento del Código de Ética del Tribunal Federal de Justicia Administrativa.	No aplica.
Concienciación, educación y entrenamiento de seguridad de la información.	Cursos de capacitación en materia de protección de datos personales, enfocados en el tratamiento y conservación de los datos, así como en medidas de seguridad.	Número de personas capacitadas anualmente.
Administración de medios removibles: discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.	Asignación de discos duros y unidades de almacenamiento USB de manera controlada (Formato de Asignación de Servicios de Cómputo y Comunicaciones)	Identificación de los servidores públicos que almacenan datos en medios removibles y justificación.
Acuerdos de intercambio de información con instituciones pública externas.	Seguir las disposiciones de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, relativas a la transferencia de datos personales, en aquellos casos en los que no se requiere del consentimiento de los titulares. Aviso de privacidad.	Número de solicitudes realizadas por instituciones externas para acceder o transferir los datos personales que obran en el Sistema Integral de Administración Financiera WIN-SIAF.
Uso de sistema de monitoreo: procedimiento para monitorear el uso de la información y del sistema.	Actualización de la bitácora de transacciones realizadas por los servidores públicos.	Número de actualizaciones realizadas en el año, o bien, cuando se requiera.

Registro de usuarios	Existe un procedimiento formal para registrar usuarios, así como para revocar el acceso.	Actualización de la base de datos.
Verificación del cumplimiento técnico.	Verificar anualmente los sistemas de información para el cumplimiento de los estándares de seguridad, con base en los resultados del análisis de brecha (*Gap Analysis)* efectuado por la Secretaría Operativa de Tecnologías de la Información y las Comunicaciones.	Resultados del análisis de brecha (*Gap Analysis)* efectuado por la Secretaría Operativa de Tecnologías de la Información y las Comunicaciones.
Eliminación o reutilización segura del equipo. Los equipos que contengan medios de almacenamiento deberán revisarse para asegurar la remoción o sobre-escritura apropiada de cualquier información sensible y "software" de autor antes de su eliminación.	Respaldos de información almacenada en los equipos de cómputo de los servidores públicos que sean dados de baja, previo a la reasignación de usuario y contraseña.	Número de usuarios y contraseñas que han sido dadas de baja, para acceder a un equipo.
Controles de código malicioso que prevean la detección, prevención y recuperación de la infraestructura.	Políticas de seguridad informática.	Revisión periódica de los componentes *Firewall*, códigos fuente de la aplicación y pruebas de denegación del servicio.
Controles de red: las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Políticas de seguridad informática.	Revisión periódica de los componentes *Firewall*, códigos fuente de la aplicación y pruebas de denegación del servicio.

Registro de auditorías, relacionados con las actividades de los usuarios y eventos de seguridad.	Registrar fecha de acceso, usuario y cambios que, en su caso, realizó.	No aplica.
Administración de privilegios. Deberá restringirse y controlarse la asignación y uso de privilegios.	Políticas de seguridad informática para la asignación de privilegios de accesibilidad.	Número y cargo de servidores públicos que cuentan con privilegios para acceder al sistema con el carácter de administrador.
Uso de contraseñas	Los usuarios tienen asignada una contraseña para ingresar al Sistema.	Revisar los ingresos con las contraseñas asignadas a los usuarios
Equipos desatendidos	El sistema solicita el ingreso de usuario y contraseña a los 10 minutos de inactividad del operador y usuario.	No aplica.
Eliminación de los derechos de acceso al sistema.	Baja de usuarios y contraseñas al Sistema Integral de Administración Financiera WIN-SIAF.	Registrar en la base de datos, la fecha en que se elimina el usuario y contraseña de algún servidor público.
Controles de acceso a los equipos que resguardan la información.	Usuario y contraseña, esta última que pueda cambiarse constantemente.	Número de veces que se ha cambiado la contraseña en un equipo de cómputo.
Control de vulnerabilidades técnicas del Sistema	Probabilidad de que se ocurran vulnerabilidades y medidas apropiadas para enfrentarlas, con base en el resultado del análisis de brecha (*Gap Analysis)* efectuado por la Secretaría Operativa de Tecnologías de la Información y las Comunicaciones.	Resultados del análisis de brecha (Gap Analysis) efectuado por la Secretaría Operativa de Tecnologías de la Información y las Comunicaciones.
Respaldo de información	Respaldo de los datos personales e información que se encuentra cargada en el Sistema, así como la base de datos.	Periodo en que se realiza el respaldo y número de registros que se respaldan.

8. Programa de capacitación a los servidores públicos que administran, operan o usan los sistemas que concentran datos personales en el área responsable.

El programa de capacitación se ajusta al calendario de cursos presenciales y a distancia impartidos por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, conforme a la cédula de detección de necesidades de capacitación que realiza la Unidad de Enlace/Transparencia del Tribunal Federal de Justicia Administrativa.

Al respecto, para el ejercicio 2019 se solicitaron los siguientes cursos:

Acciones de capacitación en Línea (CEVINAI)	Número de personas a capacitar						
	Comité de Transparencia	Unidad de Transparencia	Áreas de Archivo	Mandos Superiores	Mandos Medios	Técnico operativo	TOTALES
Reforma Constitucional (3 horas)		1					1
Introducción a la Ley General de Transparencia y Acceso a la Información Pública (6 horas)		1					1
Introducción a la Ley Federal de Transparencia y Acceso a la Información Pública (6 horas)		1					1
Introducción a la Ley General de Protección de Datos en Posesión de Sujetos Obligados (6 horas)	1	1					2
Clasificación de la Información (3 horas)	3	1					4
Ley General de Archivos	3	1					4
Lineamientos para la organización y conservación de archivos emitidos por el SNT	3	1					4
Metodología para el diseño y formulación de sistemas de clasificación y ordenación archivística (3 horas)		1					1
Descripción archivística (3 horas)		1					1
Metodología para la valoración y disposición documental (3 horas)		1					1
TOTAL	10	10	0	0	0	0	20

B. SECRETARÍA AUXILIAR DE LA JUNTA DE GOBIERNO Y ADMINISTRACIÓN UNIDAD DE PERITOS.

1. Sistemas de Tratamiento y Almacenamiento de Datos Personales

a) Nombre del sistema: Registro Electrónico Nacional de Peritos Terceros del Tribunal Federal de Justicia Administrativa	
b) Tipo de soporte en que se encuentra: Estructura y descripción del Registro Electrónico Nacional de Peritos Terceros del Tribunal Federal de Justicia Administrativa	
Tipo de soporte:	Soportes Físicos e Informáticos
Características del lugar de resguardo:	Oficinas que ocupa la Unidad de Peritos citas en Edificio Torre"O" Insurgentes Sur 881. Col. Nápoles, Alcaldía Benito Juárez, C.P. 03810 Ciudad de México
Programas en que se utilizan los D.P.	Sistema de Control y Seguimiento de Juicios, versión 4.0.20.
Resguardo de los soportes físicos y/o electrónicos en que se encuentran los datos personales	
Físicos	Archivero de gavetas inventario 3238209 Archivero de gavetas inventario 3237680 Archivero de gavetas inventario 3237684 Archivero de gavetas inventario 3237688 Archivero de gavetas inventario 3237722 Archivero de gavetas inventario 3237739 Resguardante: Lic. Carolina Fayad Contreras, Titular de la Unidad.
Electrónicos	Resguardante: Lic. Carolina Fayad Contreras, Titular de la Unidad. [redacted] SERIE [redacted] inventario [redacted] Software: [redacted]. Resguardante: Ana María López Anta [redacted] Software: [redacted]

c) Tipo de datos personales que se recaban: Registro Electrónico Nacional de Peritos Terceros del Tribunal Federal de Justicia Administrativa. Datos Personales.	
Inventario:	• Personales • Curriculares • Ubicación • Académicos • Fiscales • Identificación
Bases de datos	• Asignar Peritos Terceros en las diversas Salas Regionales a nivel Nacional a solicitud de los Magistrados • Mantener actualizadas las fichas técnicas de los especialistas en el sistema • Realizar movimientos dentro del sistema tales como: ingresos e inactivos por diversos motivos (suspensión temporal, suspensión por procedimiento, baja por defunción, baja por petición)
No. De titulares	656
d) Finalidad de los Datos	
Registro Interno para Auxiliar a los Magistrados Instructores que integran las Salas Regionales Ordinarias, Auxiliares, Especializadas y Mixtas del Tribunal Federal de Justicia Administrativa, a proponer los peritos terceros que intervendrán en los procedimientos contenciosos administrativos que conozcan por razón de turno, mediante la asignación aleatoria de dichos profesionistas, y su posterior designación en términos de los preceptos legales aplicables, a efecto de garantizar la equidad y transparencia en dicho proceso.	
e) Plazo de conservación	
N/D	

2. **Funciones y Obligaciones de los Servidores Públicos que llevan a cabo el tratamiento de datos personales.**

Registro Electrónico Nacional de Peritos Terceros del Tribunal Federal de Justicia Administrativa			
Administrador	**Carolina Fayad Contreras**	**Nivel de autorización**	**ALTA (Registrar, Actualizar Visualizar**

			y Transferir)
Cargo:	**Titular de la Unidad de Peritos**		
Área	**Unidad de Peritos**		
Funciones y obligaciones	**Las señaladas en los artículos 74 y 88 del reglamento Interior del Tribunal Federal de Justicia Administrativa.**		
Personal autorizado para tratamiento (Incluir a las personas que formar parte del sistema al tratar datos personales)			
Jefe de Departamento	**Ana María López Anta**	**Calidad**	**Operador**
Funciones y obligaciones:	Atender de forma personalizada a los peritos y al personal jurisdiccional del Tribunal. Supervisar, organizar y mantener actualizado el archivo con que cuenta la Jefatura de Departamento. Supervisar la administración y la actualización del Registro Electrónico Nacional de Peritos Terceros del Tribunal Federal de Justicia Administrativa en el Sistema de Control y Seguimiento de Juicios. Coordinar y Supervisar el seguimiento a las solicitudes de los Magistrados Presidentes y/o Instructores de las Salas que integran este Tribunal, respecto de aquellos peritos cuyas materias no estén consideradas en el Registro de Peritos. Coordinar y supervisar la incorporación en el Registro de aquellos profesionistas cuyas materias estén siendo requeridas por las diversas Salas que integran este Tribunal y que no se encuentren incluidas en el catálogo o Región de que se trate. Supervisar la actualización de las fichas curriculares de los peritos terceros, a efecto de que se refleje de manera inmediata en el Sistema de Control y Seguimiento de Juicios para su consulta por las Salas y Unidades Administrativas del Tribunal que así lo requieran. Apoyar a los Magistrados Instructores, los Secretarios de Acuerdos y los Actuarios, en cualquier duda relacionada con el		

	funcionamiento y manejo del Registro Electrónico Nacional de Peritos. Proponer previa solicitud del Magistrado Instructor, la designación de aquellos especialistas que integren el Registro y que pertenezcan a otra Región distinta a su jurisdicción. Solicitar apoyo a instituciones públicas o privadas, a fin de incorporar especialistas al Registro Electrónico Nacional de Peritos. Desahogar las solicitudes de los Magistrados Instructores, respecto de las solicitudes de los requerimientos de propuestas de peritos terceros que formen parte del Registro, a efecto de que éstos coadyuven con la Sala respectiva o Unidades Administrativas de este Tribunal. Coordinar y supervisar el seguimiento constante, apoyándose de los reportes que genere el Sistema y los requerimientos de los Magistrados Presidentes o Instructores de las Salas que integran este Tribunal, a efecto de elaborar los informes en los que se asienten las profesiones, oficios, ciencias, artes o técnicas de las materias o áreas de conocimiento con mayor demanda, o aquellas que no estén consideradas en el Registro Electrónico, con la finalidad de que se tomen las medidas conducentes para allegarse de los especialistas necesarios. Proponer y presentar a la Titular de la Unidad, los acuerdos para la suspensión temporal y/o baja de peritos en el Registro. Supervisar y acordar con la Titular de la Unidad los acuerdos de Baja del Registro por defunción o solicitud del perito tercero. Supervisar que se administre y se mantenga actualizado el registro de los peritos terceros que hayan incumplido las obligaciones que sean consideradas graves y no graves. Supervisar que se lleve a cabo el registro de los peritos terceros que por algún motivo hayan sido suspendidos o causado baja del Registro. Las demás que le instruya la Titular de la Unidad.

Personal autorizado para visualizar el Sistema.			
59	Salas Regionales	**Calidad**	**Usuario**
Funciones y obligaciones:	Las señaladas en la Ley Orgánica, Reglamento Interior del Tribunal Federal de Justicia Administrativa, y demás normatividad aplicable.		

3. Análisis de riesgo.

a. Riesgo por tipo de dato:

Tipo de dato	Nivel de Riesgo Inherente	Volumen de Titulares	Riesgo Inherente
Autenticación	MEDIO	<5k	1
Ubicación	MEDIO	<5k	1
Personales	BAJO	<5k	1

b. Riesgo por nivel de accesibilidad:

Accesibilidad (Cantidad de accesos a los datos personales)
≤ 20
>20 ≤ 200
>200 ≤ 2,000
>2,000

c. Riesgo nivel de anonimidad

Entorno	Nivel de Anonimidad
Físico	1
Red Interna	2
Red Inalámbrica	3
Red de Terceros	4
Internet	5

4. Identificación de medidas de seguridad

Una vez obtenidos cada factor de riesgo se determina que el nivel de riesgo por tipo de dato, de conformidad los niveles contenidos en el documento denominado "Metodología de Análisis

de Riesgo BAA" del INAI, se ubica en nivel 1, es decir, bajo a lo que le correspondería aplicar las medidas de seguridad (CB), consideradas por el citado documento.

		Riesgo por tipo de dato 1			
Entornos de acceso	Internet	CB			
	Red terceros				
	WiFi				
	Red interna				
	Físico				
		≤ 20	≤ 200	≤ 2,000	> 2,000
		Cantidad de Accesos/Personas			

Tabla de control 1. Riesgo por tipo de dato 1

De acuerdo con el nivel de riesgo por tipo de dato, identificar la tabla que le corresponde. Si se obtuvo riesgo por tipo de dato igual a 1, independientemente del entorno de acceso y el número de accesos que se tengan, le corresponde implementar el patrón de control de medidas básicas de seguridad.

Patrones de control:

CB: Patrón de control de medidas de seguridad básicas. Es aplicable para aquellos particulares cuyo nivel de riesgo por tipo de dato es igual a 1.

a) Posibles ataques o amenazas.

- Pérdida o destrucción no autorizada o por caso fortuito o fuerza mayor.
- Robo, extravío o copia no autorizada.
- Uso, acceso, o tratamiento no autorizado.
- Daño, alteración o modificación no autorizada.

b) Si han ocurrido ataques o amenazas.

No aplica.

5. Análisis de Brecha

PATRÓN DE CONTROL CB		
CONTROL	**PARÁMETRO**	**INSTALADO**
Documentación de la política de seguridad de la información: La política de seguridad de la información debe ser aprobada por la alta gerencia, publicada y comunicada a todos los empleados y terceras partes relevantes.	Considerar la lista de controles como política de seguridad.	SI
Revisión de la Política de seguridad de la información: La política de seguridad de la información debe ser revisada en intervalos planeados o si ocurren cambios significativos, para asegurar su continua aplicabilidad, adecuación y efectividad.	Revisión anual o cuando exista una modificación a las medidas o procesos de seguridad, o las condiciones de riesgo.	SI
Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas.	Ninguno.	SI
Acuerdos de confidencialidad: Los requisitos para los acuerdos de confidencialidad o de no revelación deben reflejar las necesidades de protección de información de la organización y deben ser revisados periódicamente.	Revisión anual.	SI
Revisión independiente de la seguridad de la información: El enfoque de la organización hacia el manejo de la seguridad de la información y su implementación (por ejemplo, objetivos de control, controles, políticas, procesos y procedimientos para seguridad) debe ser revisado de manera independiente en intervalos planeados, o cuando ocurran cambios significativos en la implementación de la seguridad.	Revisión anual del documento de autoevaluación o el Contrato de Adhesión (CDA).	SI

Abordar la seguridad en los acuerdos de terceros: Los acuerdos con terceros deben cubrir todos los requisitos de seguridad pertinentes, cuando estén relacionados con el acceso, tratamiento, comunicación o gestión de la información o de las instalaciones de procesamiento de información de la organización, o la adición de productos o servicios a las instalaciones de procesamiento de la información.	Los terceros que accedan a los datos deben firmar la lista de accesos de personal autorizado, indicando la actividad a realizar, fecha o rango de fechas en las que tendrán acceso y aceptar el conocimiento de las medidas de seguridad necesarias para la protección de los datos personales.	SI
Inventario de activos: Todos los activos deben ser claramente identificados y un inventario de los activos más importantes deber ser elaborado y mantenido.	Considerar dentro del inventario cualquier activo físico o lógico que almacene o procese datos personales o sensibles.	SI
Uso aceptable de los activos: Deben identificarse, documentarse e implementarse reglas para el uso aceptable de la información y los activos relacionados con las instalaciones de procesamiento de información.	Evitar cualquier actividad que comprometa los datos personales para protegerlos de divulgación o uso no autorizado.	SI
Roles y responsabilidades: Los roles y responsabilidades de seguridad de los empleados, contratistas y usuarios de terceras partes, deben estar definidos y documentados en concordancia con la política de seguridad de la información de la organización.	Agregar roles y responsabilidades de protección de datos dentro de todo contrato vinculante. Estos contratos deben ser firmados por los empleados, contratistas y usuarios de terceros.	SI

Concienciación, educación y entrenamiento de seguridad de la información: Todos los empleados de la organización y, cuando sea relevante, contratistas y usuarios de terceras partes, deben recibir concienciación. Asimismo debe darse entrenamiento de forma periódica en las políticas y procedimientos organizacionales, conforme a la importancia de su función en el trabajo.	Sólo considerar campañas anuales de concienciación.	SI
Proceso disciplinario: Debe existir un proceso disciplinario formal para aquellos empleados que han cometido una brecha de seguridad.	Ninguno	SI
Eliminación de los derechos de acceso: Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	Cotejar contra inventario los accesos y cuentas entregadas al empleado, contratista o tercero.	SI
Controles físicos de entrada: Las áreas seguras deben estar protegidas con controles de entrada para asegurar que únicamente personal autorizado tenga permitido el acceso.	Restringir el acceso a la información en soporte físico a través de mecanismos de acceso como candados y llaves en archiveros y habitaciones que resguarden datos personales.	SI
Protección del equipo: El equipo debe estar situado y protegido para reducir los riesgos de amenazas y peligros ambientales, y oportunidades de acceso no autorizado.	Ninguno.	SI

Seguridad de los equipos en el exterior: La seguridad debe ser aplicada en equipos en el exterior tomando en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.	Actuar conscientemente para prevenir el posible robo o acceso no autorizado a los equipos.	SI
Controles contra código malicioso: Se deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos. Se deberán implementar procedimientos de concienciación adecuados.	Ninguno.	SI
Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Considerar contraseñas para los dispositivos de red diferentes a las provistas por defecto. WIFI: establecer contraseña.	SI
Eliminación y entrega de los medios de almacenamiento: Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales.	Cuando el tratamiento de la información ya no sea necesario. Garantizar la destrucción de los medios físicos que contengan datos personales y sensibles de tal forma que no sea posible reconstruirlos.	PROCESO
Acuerdos de intercambio de información: Deberán establecerse acuerdos para el intercambio de información y aplicaciones entre la organización y entidades externas.	Considerar los acuerdos de intercambio de información dentro del aviso de privacidad de la organización y los contratos vinculantes con el receptor de la información, de acuerdo a lo establecido en la	PROCESO

	LFPDPPP y su Reglamento.	
Medios físicos de almacenamiento en tránsito: Cualquier medio que contenga información deberá ser protegido contra acceso no autorizado, mal uso o corrupción durante su transporte más allá de los límites de la organización.	Ninguno.	SI
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Registrar las personas con acceso autorizado a los datos personales incluyendo fecha de acceso (o rango de acceso permitido) y firma.	PROCESO
Registro de usuarios: Deberá existir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.	Validar, y documentar las altas de accesos. Garantizar la revocación de accesos inmediatamente después a una baja. Generar inventario que considere todos los accesos entregados a toda persona.	PROCESO
Uso de contraseñas: Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas.	Contraseña.	SI
Equipos desatendidos: Los usuarios deberán asegurar que los equipos atendidos cuenten con protección adecuada.	Considerar bloqueo automático del equipo a los 5 minutos con solicitud de contraseña para desbloquear.	SI

Política de escritorios y pantallas limpias: Se deberá implementar una política de escritorio limpio de papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.	Ninguno.	SI
Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	Instalación de actualizaciones semestralmente.	ACTUALIZACIÓN CONSTANTE
Verificación del cumplimiento técnico: Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad.	Revisiones anuales, considerando como estándares de seguridad los controles de esta lista.	SI

6. Plan de Trabajo:

ACCIONES A IMPLEMENTAR	FECHA
Administración de medios removibles: Deberán documentarse e implementarse procedimientos para la gestión de medios removibles.	N/D
Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	N/D
Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas.	EN PROCESO
Elaboración del Plan de Contingencia.	N/D
Actualización de la normatividad aplicable.	EN PROCESO
Coordinación periódica entre Justicia en Línea y Unidad de Peritos, para establecer actualizaciones esquemas de seguridad, funcionalidad y cierre de brechas de seguridad	6 MESES

Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	N/D
Programa de disociación de información para disminuir los riegos vulnerabilidad.	N/D
Establecer programa de capacitación de personal de las Salas, en materia de protección de datos y seguridad informática.	N/D

7. Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad:

- Establecer un registro electrónico de accesos, donde se guarden lo datos de quién accede a los datos, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida.
- Llevar un registro de incidentes de vulnerabilidad, que permitan establecer puntos de oportunidad y mejora en seguridad.
- Realizar un Analisis de Riesgo y Analisis de Brecha periodicamente.
- Revisión constante de la normatividad para su continua actualización y mejora.
- Reuniones permanentes con la Dirección de Justicia en Línea con el fin de establecer mecanismos actualizados de trabajo en seguridad y mejoras en el desempeño del sistema.

8. Programa General de Capacitación:

NIVELES DE RESPONSABILIDAD	TEMÁTICAS	PERIODICIDAD
Unidad de Peritos	LGTAI, LFTAI, LGPDPPSO, Criterios del INAI, Seguridad de DP	6 meses
Justicia en Línea	LGTAI, LFTAI, LGPDPPSO, Criterios del INAI, Seguridad de DP	6 meses
Personal de Salas	LGTAI, LFTAI, LGPDPPSO, Criterios del INAI, Seguridad de DP	6 meses

1. SECRETARÍA OPERATIVA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

1. Sistemas electrónicos de la Secretaría Operativa de Tecnologías de las Información y las Comunicaciones, en los que se recaban, tratan y reguardan datos personales:

a) Nombre de los sistemas

- Sistema de Justicia en Línea (SJL).
- Sistema de Control y Seguimiento de Juicios (SICSEJ).
- Comunidad de Control y Vigilancia Jurisdiccional (COCOVIJ)

b) Inventario de datos personales.

SJL	SICSEJ	COCOVIJ
• Nombre Completo • Huella dactilar • Domicilio • Información Académica • CURP • RFC • Estado Civil • Copias de identificación oficial • En algunos casos cartas poder	• Nombre Completo • Huella dactilar • Domicilio • Información Académica • CURP • RFC • Estado Civil • Copias de identificación oficial • En algunos casos cartas poder	• Nombre Completo • Huella dactilar • Domicilio • Información Académica • CURP • RFC • Estado Civil • Copias de identificación oficial • En algunos casos cartas poder

Tipo de datos que son tratados por las áreas administrativas y jurisdiccionales del Tribunal (datos personales/datos personales sensibles)

SJL	SICSEJ	COCOVIJ
Las áreas administrativas manejan: • Datos personales • Datos personales sensibles	Las áreas administrativas manejan: • Datos personales • Datos personales sensibles	Las áreas administrativas manejan: • Datos personales • Datos personales sensibles

c) Finalidad para la que son solicitados y resguardados.

- SJL – Administrar y notificar el procedimiento contencioso administrativo que se sustancie ante el Tribunal.

- SICSEJ – Administrar y notificar el procedimiento contencioso administrativo que se sustancie ante el Tribunal.
- COCOVIJ – Para que los Magistrados visitadores de la junta de gobierno y administración puedan dar seguimiento a la función jurisdiccional de las salas regionales especializadas y auxiliares

2. Funciones y obligaciones de los servidores públicos que llevan a cabo el tratamiento de datos personales.

SJL

Rol	Usuarios	
	Dados de Alta	Activos
Actuario	334	261
Administradores	12	3
Administrador de Componente	3	3
Archivista	303	217
Auxiliar de Actuario	34	33
Auxiliar de Secretario de Acuerdos	145	126
Encargado de Modulo de Registro	102	75
End-User Administrator	5	3
Magistrado	302	152
Mantenimiento	1	1
Mesa de Control de Engroses	1	1
Mesa de programación de sesiones	1	1
	10	4

SICSEJ

Rol	Usuarios	
	Dados de Alta	Activos
Magistrado	211	211
Secretario	669	669
Actuaria Jurídica	170	170
Actuario	60	60
Archivistas Históricos	73	73
Archivista	235	235
Oficial De Partes	137	137
Actuario De Calle	54	54
Total	1609	1609

COCOVIJ

Tipos de Grupo	Grupos Totales
Administrativos	6
Magistrados Visitadores	7
Salas Regionales	63

SJL			SICSEJ	COCOVIJ
Mesa de Tramite	2	2		
Mesa de Versiones	158	118		
Oficial de Partes	1164	824		
Oficial Jurisdiccional	16	8		
Personal Jurisdiccional	955	551		
Secretario de Acuerdos	10	2		
Secretario General de Acuerdos	206	144		
Secretario Particular	6	2		
Unidad de Compilacion y Sistematizacion de Tesis	8	4		
Unidad de Peritos				
Total	3778	2535		

SJL	SICSEJ	COCOVIJ
• Magistrado • Secretario de Acuerdos • Actuario • Administradores • Administrador de Componente • Archivista • Auxiliar de Actuario	• Magistrado • Secretario • Actuaria Jurídica • Actuario • Archivistas • Históricos • Archivista • Oficial De Partes • Actuario De Calle	El sistema COCOVIJ lleva a cabo el tratamiento de datos por medio de grupos: • Administrativos • Magistrados Visitadores • Salas Regionales

SJL	SICSEJ	COCOVIJ
• Auxiliar de Secretario de Acuerdos • Encargado de Modulo de Registro • End-User Administrator • Mantenimiento • Mesa de Control de Engroses • Mesa de programación de sesiones • Mesa de Tramite • Mesa de Versiones • Oficial de Partes • Oficial Jurisdiccional • Personal Jurisdiccional • Secretario General de Acuerdos • Secretario Particular • Unidad de Compilación y Sistematización de Tesis • Unidad de Peritos		

- ***Funciones Jurisdiccionales o Funciones Administrativas***

Para el tratamiento de los datos jurisdiccionales del procedimiento contencioso administrativo en lo que refiere a las funciones y obligaciones de los servidores públicos se pueden consultar en la "LEY ORGÁNICA DEL TRIBUNAL FEDERAL DE JUSTICIA ADMINISTRATIVA".

- ***Servidores públicos pueden acceder a los datos personales***

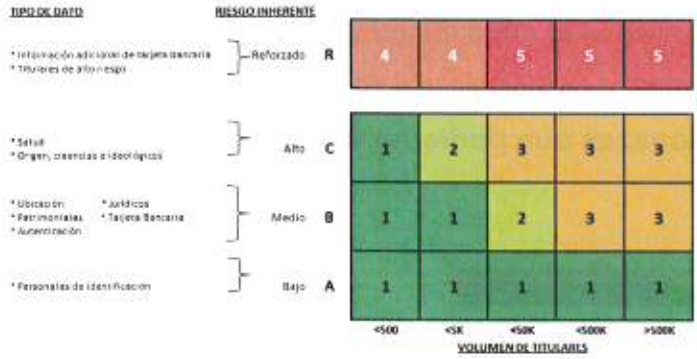
SJL	SICSEJ	COCOVIJ
• Subdirectores de Dirección de Procesos Jurisdiccionales – Administrador de Base de Datos • Jefes de departamento de Dirección de Sistemas Jurisdiccionales – Administrador de Componentes	• Magistrados – Usuario Jurisdiccional • Secretarios de Acuerdos - Usuario Jurisdiccional • Oficiales Jurisdiccionales - Usuario Jurisdiccional • Delegados – Administradores • Directores de área de la Dirección de Justicia en Línea – Administradores de Base de datos • Subdirectores de área de la Dirección de Justicia en Línea - Administradores de Base de datos • Jefes de departamento de la Dirección de Justicia en Línea - Administradores de Base de datos	El sistema COCOVIJ lleva a cabo el tratamiento de datos por medio de grupos: • Administrativos • Magistrados Visitadores • Salas Regionales

- ***¿Cuántos pueden transferir, modificar o cancelar los datos personales?***

SJL	SICSEJ	COCOVIJ
Subdirectores de Dirección de Procesos Jurisdiccionales – Administrador de Base de Datos Jefes de departamento de Dirección de Sistemas Jurisdiccionales – Administrador de Componentes	Magistrados – Usuario Jurisdiccional Secretarios de Acuerdos - Usuario Jurisdiccional Oficiales Jurisdiccionales - Usuario Jurisdiccional Delegados – Administradores Directores de área de la Dirección de Justicia en Línea – Administradores de Base de datos Subdirectores de área de la Dirección de Justicia en Línea - Administradores de Base de datos Jefes de departamento de la Dirección de Justicia en Línea - Administradores de Base de datos	Ninguno – Dentro de la COCOVIJ no existen datos personales sin embargo existen aplicaciones donde se pueden consultar mas no ingresar, modificar o borrar datos personales

3. Análisis de riesgos

a) Riesgo por tipo de dato



- SICSEJ y SJL se encuentran en un Nivel de Riesgo Medio, y contamos con un Volumen de más de 50 mil Titulares, pero menor a 500 mil Titulares.

- COCOVIJ se encuentra en un Riesgo Medio, y con un Volumen de más de 5 mil Titulares, pero menor a 50 mil Titulares.

b) Nivel de Accesibilidad de los sistemas SICSEJ, SJL, COCOVIJ

Accesibilidad (Cantidad de accesos a los datos personales)
≤ 20
> 20 ≤ 200
> 200 ≤ 2,000
> 2,000

Con base en la gráfica de Nivel de Accesibilidad anexada, los 3 sistemas cuentan con el nivel de accesibilidad más alto ya que la cantidad de usuarios que puede acceder a los sistemas en un lapso de tiempo es ilimitada.

c) Nivel de Anonimidad de los sistemas SICSEJ, SJL, COCOVIJ

Entorno	Nivel de Anonimidad
Físico	1
Red interna	2
Red inalámbrica	3
Red de terceros	4
Internet	5

Con base en la gráfica de Nivel de Anonimidad anexada se estipula que los Sistemas SICSEJ y COCOVIJ tienen el nivel 2 de anonimidad ya que solo se puede acceder a ellos por una red interna, mientras que SJL tiene un nivel 5 de anonimidad ya que se puede acceder a él desde Internet.

4. Posibles ataques y amenazas que pudieran vulnerar los datos personales que resguardamos

[redacted]

5. Análisis de brecha

a) Medidas de seguridad tiene el Tribunal para prever los posibles ataques y amenazas a las que se encuentran expuestas los datos

El Tribunal Federal de Justicia Administrativa para finales del 2019 realizará un *Gap Analysis* (del inglés, análisis de brecha) para identificar la brecha existente entre las prácticas de seguridad actuales y las mejores prácticas existentes en la industria, para que todo esto se materialice en el 2020 con la implementación del [redacted].

Actualmente se tienen implementados [redacted], así como también las siguientes medidas de Seguridad Informática para la protección de los siguientes Sistemas:

- ***Sistema de Justicia en Línea (SJL).***
  - Este sistema se encuentra alojado en una [redacted].
- ***Sistema de Control y Seguimiento de Juicios (SICSEJ).***
  - Este sistema se encuentra alojado en [redacted].
- ***Comunidad de Control y Vigilancia Jurisdiccional (COCOVIJ)***
  - Este sistema se encuentra alojado en [redacted].

b) Medidas de seguridad quedan pendientes de implementarse para mejorar la protección de los datos

Posteriormente a que sea realizado el *Gap Analysis* (del inglés, análisis de brecha) y una vez que se tengan identificadas las brechas existentes entre las prácticas de seguridad actuales y las mejores prácticas en la industria, se comenzará con el desarrollo del Documento de Seguridad para implementar en el primer trimestre del 2020.

Derivado del *Gap Analysis* (del inglés, análisis de brecha) las brechas que sean detectadas que no cuenten con medidas de seguridad implementadas, estás deberán implementarse durante el primer semestre del 2020.

6. Plan de trabajo

Probabilidad de que sucedan los ataques y amenazas a los datos que se resguardan?

- Hacer una predicción de probabilidad de un ataque es muy complejo, pero observando el comportamiento de estos en los últimos años podemos estar seguros que la "seguridad informática" está en constante crecimiento y el Tribunal está empleando nuevas tecnologías y parches de seguridad que permitan resguardar los datos de la mejor manera posible.

En caso de riesgo, el nivel de impacto en el ámbito privado de las personas que son titulares en los datos sería el siguiente:

- *Tomando en cuenta la siguiente tabla para la identificación de los niveles de impacto.*

Rango valores nivel de impacto

	Bajo			Medio			Alto		
Nivel de Impacto	1	2	3	4	5	6	7	8	9

Podemos estimar que el nivel de impacto en el ámbito privado de las personas que son titulares en los datos es (7) Alto. Ya que la mayor parte de la información seria de un Juicio Contencioso Administrativo Federal y se podría identificar datos sensibles, sin embargo, es por esta razón que el Tribunal implementa día a día mejores medidas de seguridad.

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

- Realizar un análisis de riesgos y poniendo que ponga a prueba los mecanismos de seguridad existentes como, pruebas de denegación de servicio, configuración de Routers y Firewalls, revisión de código fuente de la aplicación de manera periódica que permita aplicar actualizaciones de seguridad, etc.

- Con base a los datos obtenidos en un análisis de riesgo y las pruebas realizadas a las herramientas de seguridad del Tribunal, se determina en un cuadro de control de riesgo donde se escriben aquellas vulnerabilidades a mitigar, así como que políticas que se deben aplicar. Sin embargo, el Tribunal cuenta con un área de administra la parte de Seguridad Informática.

8. Programa General de Capacitación

Cursos de capacitación se proporcionan a los servidores públicos que acceden, transfieren, modifican o cancelan datos personales

- SICSEJ cuenta con un plan de capacitación denominado como "Programa de Capacitación para el Sistema de Control y Seguimiento de Juicios" para enseñar el uso del sistema.
- SJL cuenta con un plan de capacitación denominado como "Programa de Capacitación para el Sistema de Justicia en Línea" para enseñar el uso del sistema.

El objetivo principal de la capacitación para el usuario final es enseñar a los funcionarios del Tribunal de Justicia Fiscal y Administrativa la funcionalidad del nuevo entorno del Sistema de Justicia en Línea, particularmente el Subsistema Juicio en Línea.

Conforme a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el área de Enlace y Transparencia de este Tribunal cuenta con las facultades para impartir cursos de capacitación orientados a la protección de datos personales por lo que se podría solicitar a esta área el apoyo para impartir un curso a los servidores públicos de esta Secretaría Operativa.

Plan de capacitación de SICSEJ

MÓDULO	TEMAS
Secretarios de Acuerdos y Magistrados	Recepción de expedientes, promociones y exhortos Envío de expedientes, promociones y exhortos Validar expedientes, promociones y exhortos Validar carpetas de amparo directo, amparo indirecto, revisión y queja Generación de plantillas (acuerdos, sentencias y oficios) Personalizar plantillas (acuerdos, sentencias y oficios) Incluir (acuerdos, sentencias y oficios) Modificar documentos incluidos (acuerdos, sentencias y oficios) Certificar sentencias (interlocutoria y definitivas) Cancelación de envíos Asignación y Consulta de peritos Consulta de testimonios, autorizados y autoridades Generación de otros oficios Consulta general Reportes Agenda

Plan de capacitación de SJL

PROCESOS	TEMAS
1. Validación de demanda inicial.	a) Campos obligatorios. b) Búsqueda de autoridades. c) Vinculación de promociones a documentos. d) Modificación de datos de la promoción. e) Búsqueda por filtros. f) Invalidación de promociones.
2. Elaboración de documentos de instructor.	a) Plantillas. (indicar que no se deben modificar el espacio para código de barras, ni los campos para insertar firma digital, extensión .docx) b) Cierre de sesión.
3. Elaboración de documentos de Sala.	a) Elaboración. b) Validación. c) Permisos. d) Explicar lo que ocurre cuando hay suplencias.
4. Elaboración de Sentencia de Instructor y Sala.	a) Elaboración. b) Sentido.
5. Certificación de documentos desde consulta de expediente y validación de promoción.	ión de documentos desde consulta de te y validación de promoción
6. Consulta de promociones pendientes de acordar.	a) Consulta de promociones pendientes de acordar.
7. Amparo y revisión	a) Elaboración de acuerdo y oficio, indicando que el tipo de oficio debe ser genérico para que el sistema no habilite la remisión.
8. Consulta de expediente	a) Consulta de expediente. b) Actualización de expediente. c) Vinculación de usuario externo al expediente.
9. Presentación de Acumulación.	a) Breve explicación de la operación del Sistema cuando se presenta el escenario de acumulación de juicios.
10. Elaboración de documento	a) Tipos y subtipos. b) Generación de carpeta accesoria.

11. Elaboración de documento Cambio de vía	a) Tipo y Subtipo. b) Señalar procedencia.

Frecuencia de las acciones de capacitación: se aplica al personal de nuevo ingreso, reingreso y quien ejerza nuevas funciones.

2. CENTRO DE ESTUDIOS SUPERIORES EN MATERIA DE DERECHO FISCAL Y ADMINISTRATIVO

1. Sistemas electrónicos del Centro de Estudios Superiores en Materia de Derecho Fiscal Y Administrativo, en los que se recaban, tratan y resguardan datos personales:

a) Nombre de los sistemas:

Dirección Académica

- Sistema de gestión electrónica de Control Escolar de Estudios de Posgrados,
- Sistema de capacitación en materia Jurisdiccional,
- Sistema de Gestión de Aprendizaje en Línea TEMIS y
- Sistema de Control docente.

Dirección de Difusión

No se cuenta con sistema específico, toda la documentación es remitida a través de correo institucional y/o memoria USB.

Coordinación Biblioteca

Sistema de gestión electrónica de Biblioteca

b) Tipo de soporte en que se encuentra:

- Dirección Académica: **Electrónico y físico**
- Dirección de Difusión: **Electrónico y físico**
- Coordinación Biblioteca: **Electrónico y físico**.

c) C) Tipo de datos que recaba este Centro de Estudios

En todos los casos son datos personales, **datos con riesgo inherente bajo.**

Dirección Académica

- Nombre,
- Fecha de nacimiento,
- Acta de nacimiento,
- Dirección,
- Comprobante de domicilio,
- Cédula Fiscal,
- Estado de cuenta bancario con clabe,
- Género,
- CURP,
- Reseña curricular,

- Teléfono fijo,
- Teléfono celular,
- Correo electrónico,
- Título,
- Cédula profesional,
- Universidad de procedencia,
- Modalidad de titulación,
- Promedio de egreso,
- Otros estudios,
- Área de adscripción,
- Extensión,
- Fecha de ingreso laboral y
- Puesto que desempeña

Dirección de Difusión

- Nombre,
- Domicilio,
- Teléfono,
- Semblanza curricular y
- Correo electrónico

Coordinación de Biblioteca

- Nombre del usuario
- Área de adscripción en el Tribunal
- Extensión Telefónica

d) Finalidad para la que son solicitados y resguardados.

- En el caso de los cursos de actualización para Identificación del participante, control de asistencia, emisión de documentos de participación y estadísticos.
- Para los cursos de capacitación (Posgrados), Identificación de alumnos, registro y control escolar, asistencia, y como parte del plan de estudios para la acreditación de los cursos, emisión de documentos oficiales certificados y estadísticos.
- Los que emite la Comisión para la Igualdad de Género: control de asistencia y estadísticos.
- Los interesados en publicar sus artículos en la "Praxis de la Justicia Fiscal y Administrativa", reseña curricular y estadística.
- Todas las tesis, precedentes, criterios y jurisprudencias publicadas en la Revista del Tribunal no maneja datos personales, ya que toda la información que es remitida para su publicación por la Secretaría General de Acuerdos, es

minuciosamente revisada y testada por personal de la misma Secretaría, remitiendo versiones públicas para publicación.

- Los usuarios del servicio en la biblioteca central, se les solicita los datos personales para brindar los préstamos del acervo bibliotecario con la finalidad de conocer los temas y materias de mayor interés, formar directorio de usuarios, control de préstamos y estadísticos, en resguardo a cargo de la titular de esta área y el personal designado.

e) Plazo de conservación

Área a responsable	Plazo de conservación	Causa baja
Dirección Académica	Permanente	No aplica
Dirección de Difusión	El tiempo que el titular de los Derechos Patrimoniales autorice	A solicitud del Titular, en el momento que así lo considere.
Coordinación de biblioteca	Mientras el trabajador o usuario esté activo.	Cuando causa baja el trabajador y se notifica por oficio.

2. Servidores públicos que pueden ingresar al sistema, cargo que ocupan y funciones asignadas:

Dirección Académica.

a) Para visualizar el contenido del sistema, usuarios y operadores.

Servidor Publico	Cargo	Funciones
Lucia Juárez Ortega	Directora Académica	Dirigir y administrar los cursos de actualización, de estudios superiores en las materias autorizadas por el Tribunal con reconocimiento de validez oficial.
Lina Berenice Chávez Islas	Subdirectora de Área	Supervisión y coordinación de los eventos académicos
Alejandro Ortiz López	Jefe de Departamento	Administración del Sistema de Gestión de Aprendizaje en Línea TEMIS.
Altamara Flor Tazón Sierra	Jefe de Departamento	Control de asistencia y emisión de constancias de participación en cursos Jurisdiccionales y de la Comisión de Igualdad de Género y otros.

Ernesto Carlos Gutiérrez Félix	Jefe de Departamento	Control de asistencia y emisión de constancias de participación en cursos Jurisdiccionales y de la Comisión de Igualdad de Género y otros.
Consuelo Molina Avilés	Jefe de Departamento	Control de asistencia y emisión de constancias de participación en cursos Jurisdiccionales y de la Comisión de Igualdad de Género y otros.
Laura Márquez Galindo	Departamento de control escolar	Recabar documentación, registro y control de cursos de especialidad y posgrado de expedientes de los titulares de los datos.
Leticia Palma Rosas	Jefa de Departamento	Coadyuva con el control y registro académica de alumnos, Proporciona información a los titulares de los expedientes.
María Genoveva Néquiz Castro	Apoyo de Servicios Administrativos	Apoyo en recabar la información de los titulares y Control de expedientes docentes

Dirección de Difusión

a) Para visualizar el contenido del sistema, usuarios y operadores.

Servidor Publico	Cargo	Funciones
Mauricio Estrada Avilés	Director de Difusión	Dirige y coordina la comunicar editorial del Tribunal, y coadyuva con otras áreas en diversos temas.
Dulce Ma. Castro Robelo	Subdirectora de Diseño	Diagramar la maqueta editorial para su publicación conforme a lineamientos editoriales.
Alejandra Abril Mondragón Contreras	Jefa e Departamento	Compila y proyecta los contenidos de publicaciones a cargo de la Dirección de Difusión y apoya en proyectos específicos solicitados.

b) Para transferir, modificar o cancelar los datos, Administradores

Servidor Publico	Cargo	Funciones
Mauricio Estrada Avilés	Director de Difusión	Dirige y coordina la comunicar editorial del Tribunal, y coadyuva con otras áreas en diversos temas.

Coordinación de Biblioteca

a) Para visualizar el contenido del sistema, usuarios y operadores.

Servidor Público	Cargo	Funciones
Maricruz Moreno Villaseñor	Subdirectora de Área	Supervisión de los servicios bibliotecarios
Ismael Zúñiga Sánchez	Técnico en administración	Proporcionar el servicio de préstamo interno y externo en turno matutino
Martha Carolina Escobedo Maravillas	Apoyo de Servicios administrativos	Proporcionar el servicio de préstamo interno y externo en turno vespertino

b) Para transferir, modificar o cancelar los datos, Administradores

Servidor Público	Cargo	Funciones
Maricruz Moreno Villaseñor	Subdirectora de Área	Dirige y supervisa los servicios bibliotecarios
María del Rocío García García	Apoyo de Servicios Administrativos	Registro y control de usuarios en sistema

3. Análisis de riesgo.

Área	Tipo de Datos	Nivel de Riesgo	Volumen de Titulares
Dirección Académica	Datos personales de identificación	Bajo	1500
Dirección de Difusión	Datos personales de identificación	Bajo	20
Coordinación de Biblioteca	Datos personales de identificación	Bajo	50

4. Identificación de las Medidas de Seguridad

Dirección Académica

Control	Parámetro	Carácter
Perímetro de seguridad físico, el espacio que resguarda la documentación se encuentra con puerta y chapa de seguridad, se mantiene cerrado y solo con	Acceso restringido solo el personal del área con autorización del titular de la misma.	Necesario

acceso permitido por el responsable del área.		
Los sistemas mantienen la seguridad con clave y contraseña de acceso de los titulares para consulta de materiales de carácter académicos.	Acceso restringido solo el personal del titular y responsable del área con autorización del titular de académico.	Necesario
Se entrega folio de registro para control de asistencia, ya sea en formato impreso o por correo electrónico.	Acceso del Titular y el personal del área autorizado para verificar asistencia en cursos de actualización.	Necesario
Los sistemas se encuentran en los servidores del Tribunal asignando a los servidores públicos claves y contraseñas de seguridad	Acceso restringido solo el personal registrado cuenta con claves de acceso.	Necesario

Dirección de Difusión

Control	Parámetro	Carácter
Los datos y materiales de los titulares se mantienen en resguardo en los equipos en los servidores que trabaja la información y datos personales hasta la difusión de los artículos, comentarios, reseñas y obras.	Acceso restringido de los responsables del área que reciben, maquetan y difunden con autorización del titular.	Necesario

Coordinación de Biblioteca

Control	Parámetro	Carácter
La papeleta de préstamo se resguarda en espacios físicos, en gaveta de manera cronológica	Acceso restringido solo el titular y responsables del área.	Necesario
En los sistemas se establecen contraseñas de acceso, adicional a las claves de los equipos y usuarios.	Acceso restringido para modificar o cancelar, requiere documento de autorización o baja del servidor público	Necesario

No se tiene registro de vulnerabilidad de corrupción, ataques o amenazas, toda vez que el tribunal a Través de sus Direcciones Generales de la Secretaría Operativa de Tecnologías de la Información y las Comunicaciones se establecen los controles y medidas de seguridad de los equipos, a través de clave de acceso o contraseñas y limitan los acceso a Internet y redes sociales para no vulnerar la seguridad y resguardo de los datos personales e institucionales, se cuida la seguridad.

5. Análisis de Brecha

Dirección Académica

a) Los posibles ataques o amenazas a los que se encuentran

- Probablemente en los reactivos de exámenes de selección para especialidades

b) Las medidas de seguridad faltantes, y

- No exponer los archivos con accesos sencillos, tener claves que solo el usuario entienda y sepa sus contenidos, así como no permitir el acceso a los equipos ni hacer uso de sitios de Internet mal intencionados

c) La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

- Probablemente establecer un catálogo de claves para los archivos más vulnerables y del cual solamente conozcan los servidores públicos responsables del área.

Dirección Difusión y la Coordinación de Biblioteca

a) Los posibles ataques o amenazas a los que se encuentran

- No existen hasta hoy un indicador de amenaza a los datos personales, es probable que la Dirección General de Tecnologías de la información conozca y sea el área más indicada de informar sobre el particular.

b) Las medidas de seguridad faltantes, y

- Las Direcciones que conforman a la Secretaría Operativa de Tecnologías de la Información y las Comunicaciones establecen las medidas de control en todo el Tribunal siendo a esta que se reporten todos los correos mal intencionados, fallas en los equipos para su intervención y solución por el área especializada para detectar ol origen y la vulnerabilidad sufrida.

c) La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

- Por el momento cambiar las contraseñas de los equipos con mayor frecuencia quizás de 6 meses reducirla a tres meses , por otro lado se estará atento a cualquier medida necesaria a implementar.

6. Plan de Trabajo

Definir acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.

Área de adscripción	Medidas de seguridad faltantes	Actividad por desarrollar
Dirección Académica	Implementación de un sistema de inicio de sesión único	Desarrollo de un portal institucional con servicios para los usuarios internos. Vinculación del Sistema de Administración de Formación Institucional "TEMIS", como un servicio del portal
	Validar y documentar las altas de accesos	Elaborar las políticas que definan los casos en que se puede modificar la información sobre los alumnos, contenida en la base de datos y en los expedientes físicos
Dirección de Difusión	No señala	No señala
Coordinación de Biblioteca	Validar y documentar las altas y accesos	Realizar inventarios de los servidores públicos autorizados para el ingreso al sistema. Elaborar las políticas para el uso adecuado del sistema
	Protección del equipo	El equipo en el que se opera el sistema se da acceso a los interesados para visualizar el catálogo electrónico del acervo bibliotecario, se propone proteger el equipo para no modificar en la consulta del sistema.

7. Señalar los mecanismos de monitoreo y supervisión periódica de las medidas de seguridad:

Área	Medidas de Seguridad	Mecanismos de Monitoreo
Dirección Académica	Monitoreo del archivo físico y electrónico Inventario de los servidores públicos y sus respectivas claves y	La Secretaría Operativa de Tecnologías de la Información y las comunicaciones el respaldo en los servidores del Tribunal de los archivos que contienes información de los titulares debidamente cifrados para su seguridad, con el apoyo de las áreas especializadas.

	contraseñas de sus equipos.	
	Acceso controlado al área de servidores	La Secretaría Operativa de Tecnologías de la Información y las comunicaciones brindará copia de bitácora de acceso
	Interacción con servidores, aplicaciones y sistemas	Registro de acciones de Administradores y usuarios
	Políticas de Acceso y modificación de datos	Revisar cuando menos una vez al año.
Dirección de Difusión	Cambio de contraseñas de los equipos en donde se resguardan los datos personales y respaldo de la información.	Trimestralmente realizar el cambio de contraseñas de los equipos y semestralmente depurar los respaldos de información, conservando lo estrictamente indispensable.
Coordinación de Biblioteca	Verificar e inventariar a los servidores públicos que tienen acceso al sistema de Gestión electrónica de la Biblioteca	Revisión semestral del registro de los responsables con acceso y permisos otorgados.
	Establecer políticas de acceso y modificación de datos.	Revisión anual de las políticas de acceso y modificación o validación de las mismas.

8. Programa General de Capacitación

ACTUALIZACIÓN PARA LAS ÁREAS JURISDICCIONALES	
Nombre del evento	Frecuencia
Conferencia: Nuevas tasas del IVA en la Región Fronteriza Norte y la Eliminación de la Compensación Universal	Única vez
Presentación de la Obra: Manual de Derecho Tributario	Única vez
Conferencia: Las Reformas a la Ley Aduanera	Única vez
Análisis Económico del Derecho	Única vez
Seminario en Contratación Pública Cámara de Comercio Internacional	Única vez
Curso: Ética Judicial	Única vez
Presentación de la Obra: Las Sanciones Disciplinarias en el Sistema Anticorrupción Mexicano	Única vez
Responsabilidad Administrativa de Funcionarios Públicos (Secretaría de la Función Pública)	Única vez
Curso de Argumentación Jurídica	Única vez

Formas en que se Puede Presentar la Corrupción entre Funcionarios (Auditoría Superior de la Federación)	Única vez
Valoración de Pruebas	Única vez
Créditos Fiscales Determinados, Multas Federales no Fiscales y Pensiones Civiles	Única vez

CAPACITACIÓN PARA LAS ÁREAS JURISDICCIONALES POSGRADOS	
Nombre del evento	frecuencia
Especialidad en Justicia Administrativa 2018-2019 7a Generación	Anual año lectivo
Maestría en Justicia Administrativa 2018-2019 4a Generación	Anual año lectivo
Especialidad en Derechos Humanos y Justicia Administrativa 2018-2019 2a Generación	Anual año lectivo
Especialidad en Responsabilidades Administrativas y Sistema Nacional Anticorrupción 2018-2019 1a Generación	Anual año lectivo
Especialidad en Justicia Administrativa en Línea 2018-2019 1a Generación	Anual año lectivo
Especialidad en Justicia Administrativa 2019-2020 8a Generación	Anual año lectivo
Maestría en Justicia Administrativa 2019-2020 5a Generación	Anual año lectivo
Especialidad en Derechos Humanos y Justicia Administrativa 2019-2020 3a Generación	Anual año lectivo
Especialidad en Responsabilidades Administrativas y Sistema Nacional Anticorrupción 2018-2019 1a Generación	Anual año lectivo
Especialidad en Justicia Administrativa en Línea 2019-2020 2a Generación	Anual año lectivo
Especialidad en Justicia Administrativa en Línea 2019-2020 3a Generación	Anual año lectivo
Maestría en Justicia Administrativa en Línea 2019-2020 1a Generación	Anual año lectivo

CAPACITACIÓN PARA LAS ÁREAS JURISDICCIONALES Y ADMINISTRATIVAS	
COMISIÓN PARA LA IGUALDAD DE GENERO Nombre del evento	Frecuencia
Taller DEMAC "Para perderle el miedo a la escritura"	Una vez

Clínica para la prevención, atención y sanción del hostigamiento sexual y acoso sexual con el INMUJERES	Una vez al año
Conferencia "Las sentencias de derechos humanos nos juzgan a todxs"	Una vez al año
Paneles de análisis de sentencias de Tribunales Multilaterales y extranjeros emitidas con perspectivas Derechos Humanos y de género	Una vez al año
Conferencia obligatoria sobre la comunicación inclusiva	Una vez al año
Taller sobre la prevención de la violencia de género y la resolución pacífica de conflictos	Una vez al año
Conferencia "Protocolo para la prevención, atención y sanción del Hostigamiento sexual y Acoso sexual en la Administración Pública Federal"	Una vez al año
Conferencia "Masculinidades positivas"	Una vez al año
Curso El ABC de la accesibilidad web	Una vez al año
Curso Prevención social de las violencias con enfoque antidiscriminatorio (VIO)	Una vez al año
Curso Medidas para la igualdad en el marco de la Ley Federal para Prevenir y Eliminar la Discriminación (MED)	Una vez al año
Curso Claves para la atención pública sin discriminación (CLA)	Única vez
Curso El ABC de la igualdad y la No Discriminación (ABC)	Varias veces durante el año
Curso Migración y Xenofobia (MYX)	Varias veces durante el año
Curso Derechos Humanos y Control de Convencionalidad	Una vez al año
Taller "Incorporación de la perspectiva de género en la justicia administrativa"	Anualmente
Taller sobre la metodología prevista en el "Protocolo para juzgar con perspectiva de género" publicado por la SCJN	Anualmente
Conferencias para prevenir la violencia laboral: acoso laboral y acoso y hostigamiento sexual	Una vez al año
Conferencias de las Magistradas ganadoras del concurso de sentencias dictadas con perspectivas de derechos humanos y perspectiva de género 2018	Una vez al año
Taller "Prevención de rumores y violencia de género"	Única vez

La finalidad del programa anual de capacitación es mantener actualizado a todos los servidores públicos interesados, participando en los cursos, talleres y eventos que se realizan durante el año; asimismo se capacitan a través de posgrados de especialidad en las materias de interés del Tribunal Federal de Justicia administrativa.

Tomando acciones como la integración y diseño del Plan y Programa de Estudios tanto a nivel especialidad como de nivel Maestría en las modalidades, presencial y en línea para obtener el Registro de Validación Oficial ante la Secretaría de Educación Pública con la finalidad que los participantes en las especialidades den continuidad en su formación académica.

Transmitiendo simultáneamente a las Salas Regionales con sede distinta a la Ciudad de México todos los eventos de actualización y de la Comisión de Igualdad de Género.

En relación a los cursos que coordina la Comisión para la Igualdad de Género tienen el propósito de incorporar los derechos humanos y la perspectiva de género para su aplicación en los juicios competencia de este Tribunal.

3. UNIDAD DE ENLACE/TRANSPARENCIA

1. Sistemas electrónicos de la Unidad de Enlace/Transparencia, en los que se recaban, tratan y reguardan datos personales:

a) Nombre del sistema
Gestión Interna de Solicitudes de Información (SISITUR)
b) Tipo de soporte en que se encuentra.
Electrónico
c) Tipo de datos que recaban
Datos personales de identificación, ubicación, patrimoniales, jurídicos y autenticación
d) Finalidad para la que son solicitados y resguardados
Trámite y respuesta de solicitudes de acceso a la información y solicitudes para el ejercicio de los Derechos ARCO (acceso, rectificación, cancelación y oposición de la publicación de información).
e) Plazo de conservación
Indefinido. Los datos obran en el sistema, en tanto los titulares no soliciten su cancelación.

2. Servidores públicos que pueden ingresar al sistema, cargo que ocupan y funciones asignadas:

a) 4 Servidores públicos adscritos a la Unidad de Enlace/Transparencia

Puesto del servidor público	Funciones asignadas	Nivel de acceso al sistema
Titular de la Unidad de Enlace/Transparencia	- Asegurar que el personal adscrito a la Unidad, lleve a cabo las actividades relacionadas con la recepción y trámite interno de las solicitudes de acceso a la información, de modo que se cumpla con los procedimientos establecidos en la normativa vigente. - Supervisar que el personal de la Unidad auxilie y oriente a los titulares de datos personales, en el ejercicio de sus derechos de acceso, rectificación, oposición y cancelación (ARCO).	Administrador

	- Vigilar la gestión de las solicitudes de datos personales en coordinación con las áreas responsables de la información, de modo que se garantice el ejercicio de los derechos ARCO.	
Subdirección de Seguimiento y verificación de procedimientos	- Supervisar las actividades encomendadas por el titular de la Unidad de Enlace/Transparencia, respecto a la recepción, tramitación y respuesta de las solicitudes de acceso a la información y protección de datos personales. - Colaborar con el registro de las solicitudes de información y protección de datos personales, en el que se dé seguimiento al estado procesal en el que se encuentran y la fecha de vencimiento, para dar respuesta en el término de ley. - Evaluar que las respuestas de las unidades administrativas y jurisdiccionales del Tribunal, se ajusten a las disposiciones, términos y plazos previstos en la normatividad vigente, para la atención de las solicitudes de información y de protección de datos.	Operador
Subdirección de Clasificación de Información	- Verificar el contenido de las solicitudes de acceso a la información y de protección de datos personales, para que pueda iniciarse el procedimiento previsto en las leyes vigentes. - Procesar las solicitudes de información y protección de datos personales, para que las áreas del Tribunal se pronuncien sobre el acceso a los documentos requeridos, o bien, respecto de los datos.	Operador

	- Colaborar con el registro de las solicitudes de información y protección de datos personales, en el que se dé seguimiento al estado procesal en el que se encuentran y la fecha de vencimiento, para dar respuesta en el término de ley	
Departamento de Procedimientos y Medios de Impugnación	- Informar a las personas respecto a la elaboración de las solicitudes de acceso a la información y de protección de datos personales, para que pueda iniciarse el procedimiento previsto en las leyes vigentes. - Enviar a las áreas del Tribunal las solicitudes de información y protección de datos personales, para que se pronuncien sobre el acceso a los documentos requeridos, o bien, respecto de los datos. - Comprobar que la respuesta de las unidades administrativas y jurisdiccionales, sea congruente con los puntos de información de la solicitud, para que pueda notificarse a los particulares, dentro del plazo previsto en la normativa vigente.	Operador

b) 188 Servidores públicos habilitados[2] para dar seguimiento a las solicitudes de información:

Puesto del servidor público	Funciones asignadas en materia de transparencia:	Nivel de acceso al sistema
Secretario de Acuerdos	Dar respuesta a las solicitudes de acceso a la información y de derechos ARCO	Operador
Oficial Administrativo	Dar respuesta a las solicitudes de acceso a la información y de derechos ARCO	Operador
Director de área	Dar respuesta a las solicitudes de acceso a la información y de derechos ARCO	Operador
Subdirector de área	Dar respuesta a las solicitudes de acceso a la información y de derechos ARCO	Operador

2

Secretaria particular	Dar respuesta a las solicitudes de acceso a la información y de derechos ARCO	Operador
Actuario	Dar respuesta a las solicitudes de acceso a la información y de derechos ARCO	Operador

3. Análisis de riesgo

A continuación se determina el riesgo de que los datos personales contenidos en el Sistema de Gestión Interna de Solicitudes de Información (SISITUR), puedan sufrir una pérdida o daño, de modo que se identifique la información que por orden de prioridad requiere más protección.

Para ello, se utilizará como criterio orientador la ***Metodología BAA "Beneficio para el atacante, Accesibilidad para el atacante y Anonimidad del atacante"***[3], la cual posibilita medir el riesgo por el tipo de datos y el volumen de titulares que se tratan; por el tipo de acceso, esto es, el número de accesos potenciales a los datos; y, por el tipo de entorno desde el que se tiene acceso a los datos.

a) Riesgo por tipo de dato:

Tipo de dato	Nivel de riesgo inherente	Volumen de titulares	Nivel de riesgo por tipo de dato
Identificación	Bajo	<5K (datos de entre 501 hasta 5000 personas)	Nivel 1*
Ubicación	Medio		
Patrimoniales			
Jurídicos			
Autenticación			

* Corresponde al tratamiento de datos de identificación con riesgo inherente bajo, por lo que no importa el número de personas titulares; además de los datos de ubicación, patrimoniales, jurídicos y de autenticación con riesgo inherente medio, de 501 hasta 5000 titulares de la información.

b) Riesgo por nivel de accesibilidad

Accesibilidad*
>20 -<200

* Cantidad de accesos a los datos personales

[3] Disponible para consulta pública en: http://inicio.ifai.org.mx/DocumentosdeInteres/Metodologia_de_Riesgo_BAA_marzo2014.pdf. Fecha de consulta 08 de agosto de 2019.

El número de personas que pueden acceder al Sistema de Gestión Interna de Solicitudes de Información (SISITUR), a la fecha de la integración del presente documento, son 4 servidores públicos adscritos a la Unidad de Enlace/Transparencia y 188 servidores públicos habilitados adscritos a la Sala Superior, Junta de Gobierno y Administración, Salas Regionales Metropolitanas, Salas Regionales Foráneas, Salas Regionales Especializadas y Auxiliares, así como a las Unidades Administrativas del Tribunal.

c) Riego por nivel de anonimidad

Entorno	Nivel de Anonimidad
Físico	1
Red Interna	2

El Sistema de Gestión Interna de Solicitudes de Información (SISITUR) tiene un **Nivel 2 de anonimidad**, ya que si bien las solicitudes de acceso a la información y las relativas al ejercicio de los derechos ARCO, se imprimen y se agregan a un expediente físico que se reguarda en el archivo de la Unidad de Enlace/Transparencia, por lo que es posible controlar su consulta; lo cierto es que dichos datos permanecen en el sistema, esto es, en la red interna del Tribunal, a la cual se ingresa mediante usuario y contraseña proporcionados por la Dirección General del Sistema de Justicia en Línea.

4. Identificación de Medidas de Seguridad

Al respecto, toda vez que el riesgo de pérdida o daño de los datos personales que se recaban y resguardan en el Sistema de Gestión Interna de Solicitudes de Información (SISITUR) es nivel 1 por el tipo de dato, nivel de accesibilidad de 20 a 200 personas y nivel 2 de anonimidad, ya que no sólo se puede acceder a los datos de manera física, sino a través de la red interna del Tribunal; conforme a la Metodología BAA mencionada, se identifican las siguientes listas y patrones de control aplicables:

c) Patrón de control de medidas básicas (CB) aplicables en su totalidad

		Riesgo por tipo de dato 1			
Entornos de acceso	Internet	CB			
	Red terceros				
	WiFi				
	Red interna				
	Físico				
		≤ 20	≤ 200	≤ 2,000	> 2,000
		Cantidad de Accesos/Personas			

d) Listas de medidas administrativas para nivel de riesgo por tipo dato 2 (AD-2) y medidas básicas de seguridad para accesos desde la red interna (R1)

		Riesgo por tipo de dato 2			
		Medidas administrativas aplicables: AD-2			
Entornos de acceso	Internet	RI-1 F-1 DMZ-2	RI-1 F-1 DMZ-3	RI-2 F-2 DMZ-3	RI-2 F-2 DMZ-3
	Red terceros	RI-1 F-1 DMZ-2	RI-1 F-1 DMZ-3	RI-2 F-2 DMZ-3	RI-2 F-2 DMZ-3
	WiFi	RI-1 F-1 DMZ-2	RI-1 F-1 DMZ-3	RI-2 F-2 DMZ-3	RI-2 F-2 DMZ-3
	Red interna	RI-1 F-1	RI-1 F-1	RI-2 F-2	RI-2 F-2
	Físico	F-1	F-1	F 2	F 2
		≤ 20	≤ 200	≤ 2,000	> 2,000
		Cantidad de Accesos/Personas			

Cabe mencionar que a la fecha de la integración del presente documento de seguridad, **no se cuenta con registros de ataques u amenazas que hayan vulnerado las medidas de seguridad** que se tienen para la consulta y operación del Sistema de Gestión Interna de Solicitudes de Información (SISITUR).

5. Análisis de brecha

Con base a los patrones y listados de medidas de seguridad mencionados, a continuación se enlistan las medidas con las que cuenta la Unidad de Enlace/Transparencia, para proteger los datos personales que obran en el Sistema de Gestión Interna de Solicitudes de Información (SISITUR), así como aquellas que se encuentran en proceso de mejora o implementación.

Es necesario mencionar que únicamente se consideraron los controles y medidas que guardan relación con las actividades que lleva a cabo esta Unidad; de modo que se incluyen los patrones de control y las medidas de seguridad administrativas adicionales.

Control/Medida	Parámetro	Estatus
Documentación de política de seguridad de la información	Políticas de seguridad del Tribunal, para la protección de la información que se resguarda en los diferentes sistemas.	HECHO
Revisión de la política de seguridad de la información.	Revisión anual o cuando exista una modificación a las medidas de procesos de seguridad, o a las condiciones de riesgo.	HECHO (*Gap Analysis)*
Registro de auditorías, relacionados con las actividades de los usuarios y eventos de seguridad.	Registrar fecha de acceso, usuario y cambios que, en su caso, realizó.	HECHO
Registro de solicitudes	Todas las solicitudes deben ser registradas en una base de datos, en la que se identifique cuales se relacionan con datos personales; misma que será accesible únicamente al personal de la Unidad de Enlace/Transparencia.	HECHO
Roles y responsabilidades de los servidores públicos, definidos y documentados en concordancia con la política de seguridad de la información.	Manual de organización y Manual de procedimiento de la Unidad de Enlace/Transparencia.	HECHO
Concienciación, educación y entrenamiento de seguridad de la información.	Cursos de capacitación en materia de archivos, entre ellos, el manejo y conservación de los expedientes de las solicitudes.	NUEVA
	Cursos de capacitación en materia de protección de datos personales, enfocados en el tratamiento y conservación de los datos, así como en medidas de seguridad.	HECHO
Eliminación de los derechos de acceso al sistema.	Baja de usuarios y contraseñas al Sistema de Gestión Interna de Solicitudes.	HECHO

Controles de acceso a los equipos que resguardan la información de las solicitudes.	Usuario y contraseña, esta última que pueda cambiarse constantemente.	HECHO
Controles contra código malicioso que prevean la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos.	Revisión constante de políticas de seguridad informática.	HECHO
Controles de red: las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Revisión constante de políticas de seguridad informática.	HECHO
Eliminación de los datos personales que obran en el Sistema de Gestión Interna de Solicitudes de Información	Establecer periodos de conservación de la información resguardada en el Sistema, teniendo como base las disposiciones de la Ley General de Archivo, así como las emitidas por el Tribunal.	NUEVA
Acuerdos de intercambio de información con instituciones pública externas.	Seguir las disposiciones de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, relativas a la transferencia de datos personales, en aquellos casos en los que no se requiere del consentimiento de los titulares. Aviso de privacidad.	HECHO
Registro de usuarios	Existe un procedimiento formal para registrar usuarios, así como para revocar el acceso.	HECHO
Uso de contraseñas	Los usuarios tienen asignada una contraseña para ingresar al Sistema.	HECHO
Equipos desatendidos	El sistema solicita el ingreso de usuario y contraseña a los 10	HECHO

	minutos de inactividad del operador y usuario.	
Control de vulnerabilidades técnicas del Sistema	Probabilidad de que se ocurran vulnerabilidades y medidas apropiadas para enfrentarlas, con base en el resultado del análisis de brecha (*Gap Analysis)* efectuado por la Secretaría Operativa de Tecnologías de la Información y las Comunicaciones.	HECHO
Respaldo de información	Respaldo de los datos personales e información que se encuentra cargada en el Sistema, así como la base de datos.	HECHO

6. Plan de trabajo para implementar los patrones de control y medidas de seguridad nuevas

De conformidad con el análisis de brecha efectuado, la Unidad de Enlace/Transparencia identificó dos controles/medidas de seguridad para reforzar la protección de los datos que se encuentran resguardados en el Sistema de Gestión Interna de las Solicitudes del Tribunal, las cuales son:

a. La concienciación, educación y entrenamiento de seguridad de la información.
b. La Eliminación de los datos personales que obran en el Sistema de Gestión Interna de Solicitudes de Información

A continuación se detallan las acciones que se llevarán a cabo para implementar dichas medidas de seguridad, el objetivo que se persigue y la fecha de avance:

Medida de seguridad	Objetivo	Actividades	Fecha de avance
Concienciación, educación y entrenamiento de seguridad de la información	Capacitar a los servidores públicos de la Unidad de Enlace/Transparencia, así como a los servidores públicos habilitados, en materia de archivos, especialmente en el	- Solicitar a la Dirección General de Archivos del Tribunal la impartición de cursos en esa materia. - Incluir en la identificación de necesidades de capacitación, la cual es	Por definir

	manejo y conservación de los datos.	solicitada anualmente por el INAI, las relativas a la materia de archivos.	
Eliminación de los datos personales que obran en el Sistema de Gestión Interna de Solicitudes de Información	Establecer periodos de conservación de la información resguardada en el Sistema, teniendo como base las disposiciones de la Ley General de Archivo, así como las emitidas por el Tribunal.	- Verificar con la Dirección General de Archivos del Tribunal, el periodo de conservación indicado para información electrónica, sobre todo cuando se trata de datos personales. - Establecer, en conjunto con la Secretaría Operativa de Tecnologías de la Información y las Comunicaciones, periodos de respaldo de la información contenida en el Sistema y la eliminación correspondiente.	Por definir

7. Mecanismos de monitoreo y supervisión periódica de las medidas de seguridad:

Control/Medida	Parámetro	Mecanismos de monitoreo y supervisión
Documentación de política de seguridad de la información	Políticas de seguridad del Tribunal, para la protección de la información que se resguarda en los diferentes sistemas.	Resultados del análisis de brecha (*Gap Analysis)* efectuado por la Secretaría Operativa de Tecnologías de la Información y las Comunicaciones.
Revisión de la política de seguridad de la información.	Revisión anual o cuando exista una modificación a las medidas de procesos de seguridad, o a las condiciones de riesgo.	Resultados del análisis de brecha (*Gap Analysis)* efectuado por la Secretaría Operativa de Tecnologías de la Información y las Comunicaciones.
Registro de solicitudes	Todas las solicitudes deben ser registradas en una base de datos, en la que se	Indicador del número de solicitudes ingresadas y el

	identifique cuales se relacionan con datos personales; misma que será accesible únicamente al personal de la Unidad de Enlace/Transparencia.	número de solicitudes atendidas.
Roles y responsabilidades de los servidores públicos, definidos y documentados en concordancia con la política de seguridad de la información.	Políticas de organización y de procedimientos de la Unidad de Enlace/Transparencia.	Revisar periódicamente el Manual de organización y Manual de procedimiento de la Unidad de Enlace/Transparencia
Eliminación de los derechos de acceso al sistema.	Baja de usuarios y contraseñas al Sistema de Gestión Interna de Solicitudes.	Registrar en la base de datos de servidores públicos habilitados, la fecha en que se da de baja un usuario y contraseña.
Controles de acceso a los equipos que resguardan la información de las solicitudes.	Usuario y contraseña, esta última que pueda cambiarse constantemente.	No aplica.
Controles contra código malicioso que prevean la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos.	Políticas de seguridad informática.	Revisión periódica de los componentes *Firewall*, códigos fuente de la aplicación y pruebas de denegación del servicio.
Controles de red: las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Políticas de seguridad informática.	Revisión periódica de los componentes *Firewall*, códigos fuente de la aplicación y pruebas de denegación del servicio.

Acuerdos de intercambio de información con instituciones pública externas.	Seguir las disposiciones de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, relativas a la transferencia de datos personales, en aquellos casos en los que no se requiere del consentimiento de los titulares. Aviso de privacidad.	Número de solicitudes realizadas por instituciones externas para acceder o transferir datos personales.
Registro de usuarios	Existe un procedimiento formal para registrar usuarios, así como para revocar el acceso.	Actualización de la base de datos, cuando lo requiera el titular de la unidad jurisdiccional y administrativa.
Uso de contraseñas	Los usuarios tienen asignada una contraseña para ingresar al Sistema.	No aplica.
Equipos desatendidos	El sistema solicita el ingreso de usuario y contraseña a los 10 minutos de inactividad del operador y usuario.	No aplica
Control de vulnerabilidades técnicas del Sistema	Probabilidad de que se ocurran vulnerabilidades y medidas apropiadas para enfrentarlas, con base en el resultado del análisis de brecha (Gap Analysis) efectuado por la Secretaría Operativa de Tecnologías de la Información y las Comunicaciones.	Resultados del análisis de brecha (Gap Analysis) efectuado por la Secretaría Operativa de Tecnologías de la Información y las Comunicaciones.
Respaldo de información	Respaldo de los datos personales e información que se encuentra cargada en el Sistema, así como la base de datos.	Periodo en que se realiza el respaldo y número de registros que se respaldan.

8. Programa de capacitación a los servidores públicos que administran, operan o usan los sistemas que concentran datos personales la Unidad de Enlace/Transparencia.

El programa de capacitación se ajusta al calendario de cursos presenciales y a distancia impartidos por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, conforme a la cédula de detección de necesidades de capacitación que realiza esta Unidad de Enlace/Transparencia.

Al respecto, para el ejercicio 2019 se solicitaron los siguientes cursos:

Acciones de capacitación Presencial	Número de personas a capacitar					
	Comité de Transparencia	Unidad de Transparencia	Mandos Superiores	Mandos Medios	Técnico Operativo	TOTALES
Ética Pública (6 horas)		1				1
Sensibilización para la Transparencia y la Rendición de Cuentas (5 horas)		1				1
Introducción a la Administración Pública Mexicana (6 horas)		1				1
TOTAL	0	3	0	0	0	3

Acciones de capacitación en Linea (CEVINAI)	Número de personas a capacitar					
	Comité de Transparencia	Unidad de Transparencia	Mandos Superiores	Mandos Medios	Técnico operativo	TOTALES
Ética Pública (5 horas)	3	1				4
Sensibilización para la Transparencia y la Rendición de Cuentas (5 horas)		1				1
Introducción a la Administración Pública Mexicana (5 horas)		1				1
TOTAL	3	3	0	0	0	6

Acciones de capacitación Presencial	Número de personas a capacitar					
	Comité de Transparencia	Unidad de Transparencia	Mandos Superiores	Mandos Medios	Técnico operativo	TOTALES
Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y sus lineamientos		1				1
Introducción a la Ley Federal de Transparencia y Acceso a la Información Pública (6 horas)		1				1
Gestión de Documentos y Administración de Archivos		1				1
Formación de Instructores en las Leyes que el INAI tutela.		1				1
TOTAL	0	4	0	0	0	4

Acciones de capacitación en Línea (CEVINAI)	Número de personas a capacitar						
	Comité de Transparencia	Unidad de Transparencia	Áreas de Archivo	Mandos Superiores	Mandos Medios	Técnico operativo	TOTALES
Reforma Constitucional (3 horas)		1					1
Introducción a la Ley General de Transparencia y Acceso a la Información Pública (6 horas)		1					1
Introducción a la Ley Federal de Transparencia y Acceso a la Información Pública (6 horas)		1					1
Introducción a la Ley General de Protección de Datos en Posesión de Sujetos Obligados (6 horas)	1	1					2
Clasificación de la Información (3 horas)	3	1					4
Ley General de Archivos	3	1					4
Lineamientos para la organización y conservación de archivos emitidos por el SNT	3	1					4
Metodología para el diseño y formulación de sistemas de clasificación y ordenación archivística (3 horas)		1					1
Descripción archivística (3 horas)		1					1
Metodología para la valoración y disposición documental (3 horas)		1					1
TOTAL	10	10	0	0	0	0	20

Acciones de capacitación especializada en Línea (CEVINAI)	Número de personas a capacitar						
	Comité de Transparencia	Unidad de Transparencia	Áreas de Archivo	Mandos Superiores	Mandos Medios	Técnico operativo	TOTALES
Procedimiento de impugnación y criterios del pleno		1					1
Sistema de Portales de Obligaciones de Transparencia (SIPOT)		1					1
Gobierno Abierto y Transparencia Proactiva		1					1
TOTAL	0	3	0	0	0	0	3

IV. BIBLIOGRAFÍA

1. Instituto Nacional de Transparencia, A. a. (Junio de 2018). Instituto Nacional de Transparencia, Acceso a la Información. Recuperado el 03 de 08 de 18, de Recomendaciones para el manejo de incidentes de seguridad de datos personales: http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf

2. Pública, I. F. (Marzo de 2014). Son tus datos. Recuperado el 13 de Julio de 2018, de https://sontusdatos.org/wp-content/uploads/2013/04/ifai-metodologia-de-Riesgo-BAA_2014.pdf

"De conformidad con lo dispuesto por los artículos 113, fracción I de la Ley General de Transparencia y Acceso a la Información Pública; 110, fracción I de la Ley Federal de Transparencia y Acceso a la información Pública; y Décimo Octavo, primer párrafo, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas; indica que fueron suprimidos de la versión pública del presente documento de seguridad, lo relativo a las medidas con las que cuenta el Tribunal Federal de Justicia Administrativa para proteger y asegurar los sistemas que utiliza para el desempeño de sus actividades, así como los números de serie y características particulares de los equipos de cómputo, ya que ***la divulgación de esa información representaría un perjuicio significativo, real, demostrable e identificable al interés público****, pues su difusión vulneraría, no solo la seguridad informática de la institución, sino la seguridad pública del Estado mexicano, ya que se generaría la expectativa razonable de que ocurra un ataque intrusivo o cibernético que pudiera inhabilitar el uso y funcionamiento de los servicios tecnológicos y de comunicaciones, poniendo en peligro las actividades administrativas y de los órganos jurisdiccionales; esto es, se afectarían funciones primordiales de la Federación, como es la impartición de justicia, la garantía de ese derecho y el desempeño de las áreas administrativas que se le relacionan; asimismo,* ***el riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda****, lo cual se acredita, si se parte de la base de que el correcto funcionamiento de los órganos federales encargados de impartir justicia y de aquellas unidades administrativas que garantizan la autonomía, independencia e imparcialidad de los operadores judiciales, son del mayor interés público, por lo que es claro que la divulgación de cualquier información que menoscabe ese interés constituiría un perjuicio desproporcionado sobre quien desea ejercer el derecho de acceso a la información; y que* ***la limitación es proporcional y representa el medio menos restrictivo disponible para evitar el perjuicio****, pues es posible realizar una versión pública, en la cual se proteja la información reservada, pero que permita conocer aquella que es de interés general y, por tanto, de carácter público."*

El presente Documento de Seguridad fue aprobado por el Comité de Transparencia del Tribunal Federal de Justicia Administrativa, en la Vigésima Séptima Sesión Ordinaria celebrada el 20 de septiembre de 2019, cuya acta puede ser consultada en la siguiente liga: http://transparencia.tfja.gob.mx/utransp/01/fraccxxxix/acta/27extra19.pdf.