ÍNDICE

Elaboró	Revisó	Aprobó
Oficial de Seguridad de la Información	**Comité de Seguridad de la información**	**Dueño del SGSI**

1. OBJETIVO

Definir el marco general para asegurar la seguridad de la información del Sistema de Gestión Integral de la Unidad de Prevalidación

2. ALCANCE

El Sistema de Gestión Integral contempla los activos que permiten la funcionalidad de los procesos que soportan a los servicios prestados por la Unidad de Prevalidación sobre el servicio de Prevalidación, así como la protección de los datos personales obtenidos para la prestación de los servicios de la Unidad de Prevalidación, así como para la contratación y gestión de los recursos humanos de la unidad de Prevalidación.

3. SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN

Dentro del SGI es fundamental capacitar y concientizar al personal de la Unidad de Prevalidación sobre los aspectos de Seguridad y Privacidad de la Información. El personal de la Unidad de Prevalidación debe involucrarse y asumir un rol protagónico y responsable como parte de un Sistema de Gestión Integral.

Deben existir políticas de formación clara, concisas y permanentes orientadas a formar a los colaboradores de la Unidad de Prevalidación sobre los siguientes aspectos:

- Entender los tipos de riesgos de seguridad de la Unidad de Prevalidación y su implicación en el desempeño de la misma.
- Lineamientos para realizar los respaldos de información.
- Buenas prácticas en el manejo y conservación de los sistemas.
- Políticas para el intercambio de información
- Principios de comportamiento ético profesional que guíen a los colaboradores en sus decisiones en el manejo y utilización de los recursos y sistemas de la Unidad de Prevalidación.

4. POLÍTICA DE SEGURIDAD DE INFORMACIÓN

El enfoque sobre el Sistema de Gestión de la Seguridad y Privacidad de Información que la Unidad de Prevalidación posee, consiste en la implementación de mejores prácticas de la industria para obtener un razonable, pero no absoluto, aseguramiento de que los procesos y activos de información están protegidos tomando en consideración los principios de confidencialidad, integridad y disponibilidad.

Apoyándose en diferentes técnicas y mecanismos, incluyendo, pero no limitándose a:

- Análisis de riesgos con base en mejores prácticas.
- Identificación de los niveles aceptables de riesgo aplicables a los sistemas y servicio de Prevalidación.
- Evaluación de alternativas para el tratamiento de riesgos.
- Monitoreo continuo de cambios en el ambiente de la Prevalidación, incluyendo regulaciones, nuevos requerimientos, ambiente de negocios, competencia, iniciativas, entre otros.

La Unidad de Prevalidación reconoce que está bajo su responsabilidad la protección del acceso o intercambio de información que se encuentre bajo su custodia con entidades externas, también reconoce que dichas entidades incrementan el riesgo de que la información pudiera ser vulnerada, por lo que tomará las medidas necesarias para proteger los activos de información propios, incluyendo pero no limitándose a prácticas de contratación, acuerdos de confidencialidad, acuerdos legales, evaluaciones independientes, entre otras.

La presente política es aplicable a todos los colaboradores de la Unidad de Prevalidación incluyendo personal con contrato permanente, eventual y terceros; para garantizar la confidencialidad, integridad, y disponibilidad de la información y recursos informáticos que sean de su propiedad o estén bajo su administración o custodia.

Política de Seguridad de Información

La Dirección General está comprometida con la seguridad de la información de los clientes internos / externos relacionada con el Servicio de Prevalidación, brindando los recursos necesarios para la implementación de un Sistema de Gestión de Seguridad de Información que cumpla con los requisitos aplicables, y con los objetivos de seguridad de la información, buscando en todo momento la mejora continua del Sistema de Gestión de Seguridad de la Información.

El Director establece que todo personal interno o externo que tenga relación con el servicio de Prevalidación, debe garantizar la confidencialidad, integridad y disponibilidad de la información; apegándose a las políticas, procesos, procedimientos y controles definidos e implementados dentro del SGSI.

Con ello, se permite proyectar a la Unidad de Prevalidación como un socio de negocio confiable en el manejo de información, requiriendo del compromiso de los colaboradores y usuarios del SGSI para adquirir los conocimientos necesarios para desarrollar una cultura de seguridad en el servicio de Prevalidación.

5. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN

El SGSI de la Unidad de Prevalidación tiene un alcance hacia el Servicio de Prevalidación, el cual incluye:

- La protección de la información procesada, almacenada por la Unidad de Prevalidación que incluye el Sistema de Prevalidación Electrónica de pedimentos, Soporte Técnico y Servicios Adicionales al Prevalidador. De acuerdo con la declaración de aplicabilidad del 01/08/2023.

  De conformidad con la regla 1.8.2 de las Reglas Generales de Comercio Exterior que deberán cumplir los personas que cuentan con la autorización para prestar los servicios de prevalidación electrónica de datos, contenidos en los pedimentos en términos del artículo 16-A de la Ley Aduanera y 13 de su reglamento, así como las personas interesadas en obtenerlas.

6. OBJETIVO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN (SGSI)

Los objetivos de SGSI de la Unidad de Prevalidación son expresados mediante la misión y visión establecidos por index; y el objetivo específico del servicio de prevalidación, los cuales se mencionan a continuación:

Misión de index

Representar con eficiencia y profesionalismo a la Industria Maquiladora y Manufacturera de Exportación, mediante acciones y servicios de calidad, para lograr que en México sea líder en competitividad en un entorno global.

Visión de index

Ser por excelencia el organismo de vanguardia en representación de la Industria Maquiladora y Manufacturera de Exportación en México.

Objetivo del Servicio de Prevalidación

Otorgar un servicio diferenciador a los usuarios de Comercio y con elementos de Valor Agregado, ser una alternativa eficiente, con calidad, atención personalizada, especializada, permitiendo agregarle valor al desarrollo de sus operaciones de Comercio Exterior.

Objetivos del SGSI

Garantizar que el servicio de prevalidación cubra los requerimientos de seguridad de la información acordados con sus clientes y con requerimientos regulatorios aplicables a la Prevalidación, de acuerdo con los servicios proporcionados por la Unidad de Prevalidación conforme a los principios de confidencialidad, integridad y disponibilidad de la información, mediante una adecuada administración de controles de seguridad, a través de:

1) Establecer un sistema de gestión de seguridad de la información con apego a los "*Lineamientos que deben de observar quienes cuenten con la autorización para prestar los servicios de Prevalidación electrónica de datos contenidos en los pedimentos y los interesados en obtenerla"* y a la norma "*ISO 27001*".
2) Establecer los controles de seguridad de la información, justificando cada uno sobre la afectación positiva o negativa al servicio.
3) Evitar penalizaciones debido a daños o perjuicios que por impericia o incumplimiento de la normatividad aplicable a aquellas personas morales que cuenten con la autorización de mérito, se ocasione al Fisco Federal o a un tercero.
4) Monitorear el cumplimiento de los niveles de servicio establecidos signados con nuestros proveedores y en caso de incumplimiento hacer efectivo las penalizaciones establecidas en los contratos.
5) Fomentar una cultura en la Unidad de Prevalidación hacia los principios de seguridad de la información.

Ver, Programa de logro de objetivos.

7. COMPROMISO DE LA ALTA DIRECCIÓN

La Dirección General proporcionara los recursos humanos y materiales requeridos para implementar los controles de seguridad y procesos que se determine necesarios con base en los procesos de administración de riesgos de la Unidad de Prevalidación, verificando el cumplimiento con las regulaciones aplicables.

La Dirección General verifica a través de la Revisión por la Dirección anual la efectividad del Sistema de Gestión de Seguridad de la Información y la presente Política para asegurar que los mismos se apegan a las necesidades de la Prevalidación y de su entorno.

8. ROLES DE SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN (SGSI)

Para la implantación y operación de procesos de SGSI, se han establecido los roles para el SGSI en el documento **PO-PR-29 "Autoridades y responsabilidades de Seguridad de la Información".**

9. ADMINISTRACIÓN DEL RIESGO E INCIDENTES DE SEGURIDAD

La administración del riesgo contempla los siguientes aspectos:

- Análisis del riesgo
- Tratamiento del riesgo
- Aceptación del riesgo
- Monitoreo del riesgo
- Difusión del riesgo

Estos aspectos son contemplados dentro del documento denominado **"PD-PR-24 Procedimiento de Análisis y Administración de riesgos"**.

Se cuenta con el documento **PD-PR-14 "Procedimiento para reportar incidentes de seguridad de la Información"** el cual establece los lineamentos generales para asegurar y proteger los recursos humanos, físicos y lógicos para el tratamiento de los Incidentes de Seguridad que se presenten dentro y fuera de las instalaciones de index y que pudieran presentar un riesgo para el Servicio de Prevalidación.

En caso de un incidente que pongan en riesgo la confidencialidad, disponibilidad e integridad de la información de los contribuyentes, este se reportará al SAT en los siguientes 5 días hábiles después del suceso, acorde en lo establecido en el **PD-PR-14 "Procedimiento para reportar incidentes de seguridad de la Información"**

10. LINEAMIENTOS A SEGUIR DE PROVEEDORES Y/O PERSONAL AJENO A LA UNIDAD DE PREVALIDACIÓN

Todo aquel proveedor o personal ajeno a la unidad de prevalidación debe seguir las políticas de seguridad definidas por la Unidad de prevalidación y que le sean de aplicabilidad, así como apegarse a los acuerdos contenidos dentro del convenio de confidencialidad y el contrato; en caso de no cumplir con estas políticas serán sancionados de acuerdo con lo estipulado en el contrato.

11. TRANSFERENCIA DE INFORMACIÓN

Transferencia de información a proveedores o clientes
En la medida de lo posible evitar el envío de información sensible o crítica a personal externo de la organización.

Cuando se envíe información sensible o critica a personal externo a la organización se deberá firma de un convenio de confidencialidad y acuerdo de transferencia de la información uso interno.

Transferencia de información Digital o electrónica
Entregar de manera personal la transferencia de información sensible o critica, validar la autorización e identidad de la persona quién recibirá la información.

Transferencia de información utilizando mecanismos de autenticación y protocolos de cifrado o seguros previa autorización

Proporcionar la información secreta de autenticación por separado.

Transferencia de información Física
Enviar la información de uso interno por los mecanismos autorizados por la organización: mensajería, chofer, responsable de área.

Proteger la información utilizando un sobre cerrado, sin referencias sobre su contenido.

12. DECLARACIÓN DE APLICABILIDAD

La selección de objetivos de control y controles de tratamiento como resultado del previo análisis de los riesgos se encuentran reflejados en el documento **“FO-PR-09 Declaración de Aplicabilidad”.**

13. GENERALES

- El Administrador de TI-SI debe asegurar que existan campañas de concientización para asegurar que los usuarios entienden y aceptan su responsabilidad relacionada con la Política de Seguridad de la Información de la Unidad de Prevalidación, por lo menos una vez por año.
- El Administrador de TI-SGSI debe realizar una revisión por lo menos una vez al año para verificar su cumplimiento.
- El responsable de esta política debe mantener actualizados los registros que genere la presente política y notificar de manera inmediata cualquier cambio en los mismos al Dueño del SGSI.
- De ser identificado el incumplimiento a las políticas antes descritas, el colaborador debe ser sancionado según los lineamientos descritos por el PD-PR-14 Procedimiento para reportar incidentes de Seguridad de la Información y/o Código de ética, y en su caso conforme a lo previsto en la regulación aplicable en la CDMX.

14. CONTROL DE CAMBIOS

Control de Cambios		
Revisión afectada	**Descripción del cambio**	**Fecha de emisión**
1	Creación del documento	29-09-2017
2	Se anexa punto 9 “lineamientos de proveedores y/o personal ajeno a la unidad de prevalidación” Se anexa en punto 14: Contratos vigentes de clientes y proveedores Ley Federal de Protección de Datos Personales en Posesión de los Particulares	01-12-2017
3	Se incluye el punto 5 “Alcance del sistema de gestión de seguridad de la información”	29-01-2018
4	Se anexa en el punto 8 – 3 los integrantes del comité de seguridad	17-04-2018
5	Se modifica el nombre del oficial de seguridad, se amplía el alcance del sistema y se corrigen error de redacción.	22-04-2019
6	Cambio en el cuadro de aprobación, modificación de anexos acorde a formatos generados a partir del documento, adecuación acorde a los cambios en procesos, estructura organizacional y métodos de trabajo.	01-02-2021
7	Adecuación del documento resultado de la revisión posterior a Auditoria de Certificación ET1.	03-08-2021
8	Adecuación De documento referencia ISO IEC 27001:2022	01/08/2023
9	Adecuación de documento referencia ISO 9001:2015, ISO IEC 27001:2022, LFPDPPP	31/01/2024

15. ANEXOS

- FO-PR-09 Declaración de Aplicabilidad
- FO-PR-42 Matriz de requisitos legales y regulatorios

16. NORMATIVIDAD, LEGISLACIÓN Y MARCO DE REFERENCIA

- Contratos vigentes de clientes y proveedores
- Convenios de Confidencialidad vigentes de clientes y proveedores
- Ley Aduanera
- Reglamento de la ley aduanera
- Reglas generales de comercio exterior
- Código fiscal
- Ley de comercio exterior
- Ley general de impuestos de importación y exportación

- Requisitos Tecnológicos para Prevalidadores
- Reglamento de la Ley Federal de protección de datos Personales en Posesión de Particulares
- Ley federal de Derechos
- Lineamientos que deben observar quienes tengan la autorización para prestar los servicios de Prevalidación electrónica de datos, contenidos en los pedimentos y 1os interesados en obtenerla
- Guía de operación para conexión con Entidades Externas o Terceros al SAT
- ISO IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad —Sistemas de gestión de la seguridad de la información — Requisitos
- NMX-CC-9001-IMNC-2015, Sistemas de gestión de la calidad – Requisitos (ISO 9001:2015)
- LFPDPPP- Ley Federal De Protección De Datos Personales En Posesión De Los Particulares

17. DEFINICIONES

- **Información.** Conjunto de datos, este conjunto tiene coherencia y permite su uso para alguna tarea.
- **Seguridad de la Información.** Es el conjunto de medidas preventivas y reactiva de la organización y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.
  Ver, fundamentos y vocabularios.