Servicio de Impuestos Internos

SUBDIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
GE00343305

MATERIA: REORGANIZA LAS UNIDADES QUE CONFORMAN EL DEPARTAMENTO SUBDIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y ESTABLECE SUS ÁMBITOS DE COMPETENCIA. DEJA SIN EFECTO RESOLUCIÓN EX. N° 136, DE 2023.

SANTIAGO, 08 DE OCTUBRE DE 2025

RESOLUCIÓN EXENTA SII N°136.-

VISTOS: Las necesidades del Servicio de Impuestos Internos, en adelante, SII; lo dispuesto en el artículo 3° de la Ley Orgánica del SII, contenida en el Decreto con Fuerza de Ley N° 7, de Hacienda, de 1980 y en las letras c) y ñ) del artículo 7° del mismo texto legal; lo estatuido en la Ley N° 18.575 Orgánica Constitucional de Bases Generales de la Administración del Estado; el Decreto Exento (Por orden del Presidente de la República) RA N° 289/323/2024, de fecha 04/07/2024 del Ministerio de Hacienda, que nombra subrogante al cargo de Director del Servicio de Impuestos Internos a Carolina Saravia Morales; lo instruido en la Resolución N°36 de 2024, de la Contraloría General de la República; lo dispuesto en las Resoluciones N° 349 de 1984; N° 379 de 1991; Ex. N° 7.590 de 1999; Ex. N° 101 de 2019 y Ex. N°136 de 2023, todas del SII; y,

CONSIDERANDO:

1.- Que, de acuerdo con lo dispuesto en el artículo 3° de la Ley Orgánica del SII, la Dirección Nacional estará constituida por las Subdirecciones Fiscalización, Jurídica y Normativa y por las Subdirecciones y Departamentos que establezca el Director con sujeción a la planta de personal del Servicio;

2.- Que, de acuerdo con lo dispuesto en las letras c) y ñ) del artículo 7° de la Ley Orgánica del SII, a la Dirección le corresponde organizar, dirigir, planificar y coordinar el funcionamiento del Servicio, dictar las órdenes que estime necesarias o convenientes para la más expedita marcha del mismo, supervigilar el cumplimiento de las instrucciones que imparta y la estricta sujeción de los dictámenes y resoluciones a las instrucciones que sobre las leyes y reglamento emita la Dirección; pudiendo además fijar y modificar la organización interna de las unidades del Servicio, asignándoles el personal necesario, fijarles y modificarles sus sedes, jurisdicciones territoriales y sus dependencias, y sus atribuciones y obligaciones, sin que el ejercicio de esta facultad pueda originar modificaciones de la Planta y estructura del Servicio;

3.- Que, en la Resolución N° 349, de 1984, se fijaron las atribuciones y obligaciones de las unidades de la Dirección Nacional, y mediante Resolución N° 379, de 1991, y sus modificaciones, se establecieron las dependencias jerárquicas y las atribuciones de los departamentos que conforman el Departamento Subdirección de Informática;

4.- Que, en la Resolución Exenta N° 7.590, de 1999, se establecieron las funciones y atribuciones de los Departamentos Subdirecciones del SII existentes a esa fecha;

5.- Que, la Resolución Exenta SII N° 136, de 2023, reemplazó la denominación del “Departamento Subdirección de Informática” por la de “Departamento Subdirección de Tecnologías de la Información y reorganizó las unidades del Departamento Subdirección de Tecnologías de la Información, estableciendo los ámbitos de competencia y los ámbitos de acción de sus Departamentos, Oficinas y Áreas.

6.- Que, el rápido avance de las tecnologías de la información, los riesgos asociados y los desafíos que imponen los Ejes establecidos en la actualización del Plan Estratégico del SII, hacen necesario que dicho Departamento Subdirección ajuste su organización a fin de abordar con éxito y con el máximo de eficiencia las labores propias de aquella, potenciando la ciberseguridad, la calidad y los procesos productivos para asegurar la continuidad operacional de la administración tributaria;

RESUELVO:

PRIMERO: Reemplazase el número 5 de la letra A de la Resolución N° 379, de 04 de diciembre de 1991, por el siguiente:

"5.- Departamento Subdirección Tecnologías de la Información, en adelante, SDTI:

- Departamento Sistemas de Impuestos Directos e Indirectos.
- Departamento Sistemas Transversales.
- Departamento Sistemas de Asistencia al Contribuyente y Avaluaciones.
- Departamento Plataforma Operacional Tecnológica.
- Departamento Ciberseguridad.
- Oficina Aseguramiento de Estándares Tecnológicos.
- Oficina Ingeniería de Datos.
- Oficina Servicios de Producción.
- Oficina Gestión Tecnológica."

SEGUNDO: Sustitúyase el número 6 del dispositivo Primero de la Resolución N° 7.590 del 15 de noviembre de 1999, por el siguiente:

En la SDTI se establecen las siguientes atribuciones, responsabilidades y obligaciones de quien ejerza el cargo de Subdirector/a:

1) Definir y establecer las estrategias para el desarrollo, investigación, incorporación, aplicación y administración de las nuevas tecnologías de información y comunicaciones al quehacer del SII.
2) Velar por el uso adecuado de los recursos disponibles para la SDTI.
3) Desarrollar los sistemas de información necesarios para apoyar en la gestión del SII.
4) Proponer normas e instrucciones para el uso de dispositivos y sistemas de información relacionados con el cumplimiento de las obligaciones tributarias por parte de los contribuyentes, considerando las necesidades y requerimientos de las áreas de negocios.
5) Promover un adecuado funcionamiento de las aplicaciones informáticas en operación, administrar el diseño, uso y mantención de los sistemas de información, y gestionar los activos intangibles.
6) Controlar y gestionar los proyectos tecnológicos, apoyado de cada área responsable, con el fin de maximizar la vida útil de los sistemas computacionales, junto con asegurar la continuidad operacional.
7) Promover la gestión y fortalecimiento de los distintos procesos informáticos e institucionales, impulsando el desarrollo de competencias en el equipo y facilitando el trabajo colaborativo.
8) Otras funciones que la Dirección del SII estime de competencia o encomiende en forma particular a esta Subdirección, operando en acuerdo a la normativa vigente.

TERCERO: Al **Departamento Sistemas de Impuestos Directos e Indirectos** le corresponde atender todos los desarrollos de sistemas relacionados con la facilitación de ingreso, cruce, fiscalización y gestión tributaria de los impuestos directos e indirectos, que apoyen las líneas de negocio del SII relacionadas.

Para hacer efectiva la implementación de sus funciones y de las que se le encomendarán en el resolutivo SEXTO, el Departamento Sistemas de Impuestos Directos e Indirectos estará constituido por las siguientes áreas:

- Área de Impuestos Directos.
- Área de Impuestos Indirectos.
- Área de Apoyo a la Gestión Tributaria.

CUARTO: Al **Departamento Sistemas Transversales** le corresponde atender todos los desarrollos de sistemas que presten servicios de carácter transversal a las soluciones de negocio que el SII ofrece a funcionarios/as y a la ciudadanía en general, específicamente aquellos que permiten gestionar los procesos jurídicos, normativos, administrativos, de gestión de las personas y de interoperabilidad. Además, debe promover el desarrollo e integración de los sistemas y/o componentes de uso transversal que faciliten el cumplimiento tributario.

Para hacer efectiva la implementación de estas funciones y las que se le encomendarán en el Resolutivo SEXTO, el Departamento Sistemas Transversales estará constituido por las siguientes Áreas:

- Área de Sistemas de Atención y Soporte a Personas.
- Área de Sistemas Transversales.
- Área de Sistemas de Interoperabilidad.

QUINTO: Al **Departamento Sistemas de Asistencia al Contribuyente y Avaluaciones**, sucesor del Departamento Sistemas de Avaluaciones y Asistencia al Contribuyente, le corresponde atender todos los desarrollos de sistemas relacionados con la plataforma de soluciones que soporta a los servicios de asistencia y ciclo de vida del contribuyente, la administración de documentos tributarios electrónicos y el impuesto territorial.

Para hacer efectiva la implementación de estas funciones y las que se le encomendarán en el Resolutivo SEXTO, el Departamento Sistemas de Asistencia al Contribuyente y Avaluaciones estará constituido por las siguientes Áreas:

- Área de Catastro de Contribuyentes.
- Área de Documentos Tributarios Electrónicos.
- Área de Gestión Territorial y Avalúos (sucesora del Área de Impuesto Territorial del mismo Departamento)

SEXTO: Además de las funciones ya señaladas en los resolutivos TERCERO, CUARTO y QUINTO, los Departamentos mencionados deberán cumplir las siguientes funciones transversales de análisis, diseño, desarrollo y mantención de software, dentro de la esfera de sus respectivas especialidades:

1) Atender los requerimientos de las áreas del SII que atienden, apoyándose en equipos multidisciplinarios.
2) Investigar soluciones computacionales y herramientas que puedan satisfacer a las nuevas necesidades, presentando diversas alternativas y propuestas.
3) Realizar el mantenimiento funcional y tecnológico a los sistemas a cargo del departamento, gestionar la obsolescencia, prevenir la materialización de riesgos en estos ámbitos y atender oportunamente el ciclo de vida de los sistemas desarrollados, así como atender los requerimientos derivados desde las áreas de producción.
4) Adoptar y fortalecer la aplicación de mejores prácticas de seguridad y protección de datos, integrándolas en el desarrollo y su mantención, además de potenciar uso de repositorios de datos que den soporte a la toma de decisiones, promoviendo su completitud, consistencia, integridad, trazabilidad, calidad y seguridad.
5) Velar por las mejoras en la eficiencia y eficacia del quehacer institucional, adhiriendo a la arquitectura tecnológica referencial vigente para los sistemas en uso por parte de la institución, velando por la continuidad operacional, su seguridad y estableciendo indicadores que permitan medir su gestión.

SÉPTIMO: Al **Departamento Plataforma Operacional Tecnológica** le corresponderá administrar, mantener, monitorear y gestionar toda la infraestructura tecnológica, incluyendo las estaciones de trabajo y soluciones relacionadas, con la finalidad de garantizar la continuidad operacional de los servicios prestados por el SII a los contribuyentes, funcionarios y entidades externas. Además, deberá identificar los riesgos, junto con proponer planes de acción y contar con indicadores que permitan medir su gestión. Sus funciones específicas son:

En el ámbito de la infraestructura tecnológica:

1) Administrar el inventario de todo el hardware y el sistema operativo del software, definición y aplicación de elementos de control y gestión para todas las componentes que lo sustentan, optimizando su utilización.
2) Gestionar eficazmente la plataforma tecnológica (hardware y servicios) que da soporte a las soluciones computacionales, según la normativa vigente, que incluye todas las componentes de la infraestructura tecnológica, considerando acciones preventivas y correctivas destinadas a minimizar o eliminar las interrupciones de los sistemas productivos.
3) Respecto del Data Center, deberá proporcionar y velar por todos los elementos necesarios para asegurar su correcto funcionamiento y la continuidad de sus servicios en forma ininterrumpida.
4) Administrar la red de SAN (*Storage Área Network*) que utilizan los servidores de datos.
5) Administrar eficientemente los recursos del Cloud público, optimizar la gestión presupuestaria y su rendimiento, a fin de potenciar la operación y fortalecer la continuidad operacional.
6) Evaluar y proponer nuevas soluciones que permitan optimizar y potenciar los servicios de infraestructura tecnológica del SII.
7) Definir estándares y políticas para la debida administración de los componentes que interactúan en la infraestructura tecnológica, además de verificar su correcto cumplimiento.

En el ámbito de la plataforma de datos y middleware:

8) Administrar el inventario de todo el software base de la plataforma tecnológica referido a base de datos y middleware.
9) Definir y aplicar los elementos de control a todas las componentes que lo sustentan, optimizando su utilización.
10) Entregar soporte técnico a las soluciones computacionales, procurando mantener los sistemas en funcionamiento ininterrumpidamente.
11) Evaluar y proponer nuevas soluciones que permitan optimizar y potenciar los servicios de datos del SII, las que deben ser coherentes con el ecosistema tecnológico en base a la arquitectura tecnológica referencial.
12) Aplicar acciones preventivas y correctivas vinculados a minimizar o eliminar las interrupciones de los sistemas productivos.
13) Promover la gestión de la obsolescencia, atendiendo de manera oportuna el ciclo de vida de las soluciones tecnológicas para asegurar la continuidad operacional.
14) Disponer de componentes que faciliten el monitoreo y trazabilidad de las transacciones de manera segura, además de contar con planes de contingencia en caso de fallas.

En el ámbito de las comunicaciones y redes:

15) Definir y ejecutar los proyectos de implementación de redes y comunicaciones tecnológicas, que aseguren la continua y correcta provisión del servicio de las redes informáticas y de telefonía para la institución.
16) Gestionar la interconectividad de las redes entre los Data Center, con soluciones Cloud públicas y conectividad de contribuyentes y funcionarios del SII, supervisando el correcto funcionamiento de los enlaces de navegación.
17) Gestionar los servicios de red estratégicos para asegurar la alta disponibilidad y el óptimo rendimiento de las aplicaciones y servicios del SII, además de la resolución de nombres y la distribución equitativa del tráfico para prevenir interrupciones del servicio.
18) Administrar la red LAN de funcionarios/as, y la red WAN, asegurando su correcto y continuo funcionamiento, en coordinación con las unidades regionales y proveedores correspondientes.
19) Gestionar las incidencias de comunicaciones tecnológicas, asegurando la continuidad operacional.

En el ámbito de la computación personal:

20) Administrar la infraestructura de computación personal (hardware y software) y su inventario, además de definir estándares y políticas para el manejo de la interacción de sus componentes.

21) Administrar y brindar un soporte técnico en el hardware y/o software básico estándar de la infraestructura de computación personal para asegurar su disponibilidad a los usuarios, además de proveerles un punto único de contacto para resolver y/o gestionar la resolución de los requerimientos e incidentes, facilitando un medio de atención vía mesa de ayuda o canal alternativo. En la misma línea, deberá administrar los servicios técnicos externos de mantención preventiva y correctiva.

22) Administrar y controlar oportunamente los contratos de proveedores de la infraestructura tecnológica a su cargo, de forma de no poner en riesgo la continuidad operacional.

23) Evaluar y proponer nuevas tecnologías que permitan mejorar la entrega de servicios y gestionar la adquisición de software base y/o aplicaciones que se instalan en la infraestructura de computación personal.

24) Supervisar y coordinar la gestión operativa del soporte técnico informático de las Direcciones Regionales.

25) Proveer de indicadores permanentes para medir la gestión de la Mesa de Ayuda y de las áreas resolutoras.

La gestión del Departamento deberá contar con procedimientos de respaldo y recuperación de información, junto con incorporar procedimientos periódicos de verificación de los medios de recuperación, velando por su confidencialidad, integridad y disponibilidad, apoyándose en procedimientos de contingencias para todas las soluciones que administra y gestiona, de tal forma de garantizar la continuidad operacional de los servicios aplicativos.

Paralelamente, debe coordinarse permanentemente con el Departamento de Ciberseguridad en materias de prevención, detección y respuesta a incidentes que afecten la continuidad operativa de toda la plataforma tecnológica.

Para hacer efectiva la implementación de estas funcionalidades, el Departamento Plataforma Operacional Tecnológica estará constituido por las siguientes Áreas:

- Área de Infraestructura Tecnológica.
- Área de Plataforma de Datos y Middleware (sucesora del Área de Servicios de Datos del mismo Departamento).
- Área de Comunicaciones y Redes (antes dependiente de la ex Oficina de Control y Comunicaciones Tecnológicas).
- Área de Computación Personal.

OCTAVO: Al **Departamento Ciberseguridad,** como sucesor del Departamento Aseguramiento de Estándares Tecnológicos, le corresponde gestionar proactivamente los riesgos de ciberseguridad, garantizar la protección de los activos tecnológicos de la información y los servicios críticos de la institución , mediante la implementación de un programa integral de prevención, detección, respuesta y recuperación de incidentes de seguridad, empleando planes de continuidad y de respuesta, además de asegurar el cumplimiento normativo, fomentar la cultura de ciberseguridad y mejorar continuamente las defensas apoyándose en pruebas rigurosas, simulaciones, estándares de industria, políticas y procedimientos que permitan dar certeza operacional a la continuidad, integridad y disponibilidad de los sistemas tecnológicos, visibilizando los eventos de seguridad.

En el ámbito de CSIRT (Computer Security Incident Response Team)**:**[1][2]

1) Operar en conformidad con las directrices definidas por la Política de Seguridad de la Información, teniendo como objetivo contar con ambientes seguros y con una alta disponibilidad.

2) En el ámbito de la prevención deberá identificar eventos en brechas de seguridad, y proponer procedimientos y elementos necesarios para garantizar la continuidad de los servicios y la protección de los datos institucionales, incluyendo los controles físicos y lógicos, con

[1] https://www.enisa.europa.eu/publications/h ow-to-set-up-csirt-and-soc
[2] https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2-1

mecanismos internos o con empresas externas, implementando medidas para resguardar la infraestructura y mitigar los riesgos.

3) Monitorear, identificar amenazas y gestionar los incidentes de ciberseguridad que puedan afectar a la organización. Activar medidas de respuesta para contener, erradicar y recuperar los sistemas comprometidos.

4) Coordinar acciones de detección, análisis, contención, erradicación y recuperación de los servicios involucrados para asegurar la continuidad operativa; asegurar la participación de las especialidades que correspondan para dar tratamiento al incidente, y gestionar la comunicación interna y externa durante una crisis.

5) Crear y mantener indicadores de seguridad frente a manejo de vulnerabilidades, incidencias y acciones de mitigación que den la visibilidad necesaria para su correcta gestión.

6) Investigar y analizar los incidentes según su criticidad y riesgos, determinar su alcance y origen, realizar análisis forense de los incidentes para entender qué ocurrió, mecanismos utilizados e impacto, como también evaluar y documentar las lecciones aprendidas y reportar a las entidades pertinentes conforme a la normativa.

7) Promover acciones de concientización y capacitación a los usuarios y equipos técnicos en todo lo referente a la ciberseguridad, seguridad de sistemas y protección de datos.

8) Establecer relaciones de cooperación con organismos de ciberseguridad, compartiendo indicadores de compromiso y buenas prácticas.

<u>En el ámbito de estándares y control de seguridad:</u>

9) Asegurar el cumplimiento de las normas vigentes, ya sea mediante desarrollar, proponer o mantener actualizadas las políticas y/o procedimientos los que deben estar alineados a los estándares de la seguridad informática del SII instruidas por las entidades pertinentes, conforme a la normativa, para que sean integradas en todo el proceso de ciclo de vida de los sistemas, en la clasificación y protección de datos (etiquetado, manejo, cifrado y retención) y en el establecimiento de líneas base de configuración segura a nivel de sistema operativo, middleware, servicios en Cloud (público y privado), base de datos y dispositivos de trabajo.

10) Apoyar en el diseño y planificar la arquitectura de ciberseguridad que permita proteger los activos digitales de la organización frente a las amenazas internas y externas.

11) Apoyar en el diseño y planificar la arquitectura la implementación de manera segura de proyectos tecnológicos, incluyendo revisiones de arquitectura de seguridad y las distintas configuraciones de la infraestructura tecnológica.

12) Realizar de manera continua una gestión de vulnerabilidades, tanto a nivel perimetral como al interior de la plataforma computacional, así como también a nivel de desarrollo de software y de intercambio de información con terceros por parte de la institución.

13) Contar con un marco de controles y gobernar su aplicación, apoyado en un catálogo de los activos tecnológicos, mapa de riesgos, u otras herramientas de gestión. Verificar la eficacia de dichos controles mediante la implementación de autoevaluaciones, auditorías técnicas y monitoreos permanentes.

14) Gestionar los riesgos asociados a la cadena de proveedores tecnológicos, en base al cumplimiento de requisitos de seguridad y asegurando el cumplimiento de normativas aplicables.

15) Definir, medir y reportar con indicadores de seguridad a la SDTI y a la alta dirección en forma periódica, en las distintas instancias requeridas.

16) Coordinar con el Área CSIRT para incorporar lecciones aprendidas en base a las huellas de actividades maliciosas: adecuar las políticas, los controles y conducir la mejora continua, promoviendo planes de trabajo evolutivos.

17) Promover el cumplimiento de las normas técnicas en el ámbito de ciberseguridad y protección de los datos, manteniendo trazabilidad y evidencias de conformidad.

En el ámbito de detección y evaluación:

18) Planificar y realizar ejercicios colaborativos con las áreas técnicas, enfocada en acciones preventivas (ámbito de seguridad ofensiva y defensiva), identificar las vulnerabilidades, evaluar los controles de seguridad con objetivos medibles, visibilizar permanentemente su efectividad y las capacidades de detección del Área CSIRT.

19) Emular escenarios funcionales y no funcionales para las soluciones tecnológicas, diseñar planes de prueba realistas que incluyan ejercicios de intrusión e ingeniería social, realizar detección y medir el impacto de las brechas de seguridad, emular amenazas de conocimiento global, comprender su origen y proponer soluciones.

20) Realizar pruebas de penetración y simulación de ataques éticos para evaluar la efectividad de los controles de seguridad y descubrir los puntos débiles para generar una solución técnica.
21) Realizar pruebas físicas a sitios, dispositivos, cableado y estaciones de trabajo.

22) Sugerir soluciones a las brechas detectadas, planes de mejora y evidenciar la comprobación de la solución. Priorizar las soluciones y repetir las pruebas hasta cerrar las brechas detectadas, elevando la postura de seguridad y la resiliencia.

23) Facilitar el intercambio de información con los equipos técnicos, retroalimentando las mejores prácticas en el ámbito del desarrollo de software y gestión de la plataforma tecnológica.

24) Implementar, mantener y monitorear las tecnologías de ciberseguridad, aplicando controles y técnicas que permitan proteger la plataforma tecnológica del SII.

Además, el Departamento deberá realizar una correcta gestión de proveedores y contratos que presten servicios al SII en el ámbito de ciberseguridad y específicamente en las temáticas del área, así como mantener una permanente actualización de las mejores prácticas del mercado, estándares y vanguardia tecnológica en el ámbito de ciberseguridad, con el fin de proponer proyectos que contribuyan a mejorar las condiciones de seguridad de la plataforma tecnológica

Para hacer efectiva la implementación de estas funcionalidades, el Departamento Ciberseguridad estará constituido por las siguientes Áreas:

- Área de CSIRT (sucesora del Área Seguridad de Sistemas dependiente de la ex Oficina de Control y Comunicaciones Tecnológicas).
- Área de Estándares y Control de Seguridad.
- Área de Detección y Evaluación.

NOVENO: A la **Oficina Aseguramiento de Estándares Tecnológicos**, como sucesora de la Oficina Control y Comunicaciones Tecnológicas, le corresponde definir, gobernar y controlar el correcto uso de las arquitecturas referenciales aplicativas y las normas técnicas que garanticen la calidad del software en el proceso de desarrollo, mantención, operación y baja de las soluciones tecnológicas implementadas en la SDTI.

En el ámbito de la arquitectura de software:

1) Investigar, definir, modelar, mantener y promover la arquitectura referencial para las aplicaciones de los sistemas computacionales desarrollados por la SDTI y para la plataforma tecnológica del SII, facilitando el desarrollo de una hoja de ruta evolutiva en el tiempo y un ciclo de vida, que considere tanto los lineamientos institucionales como el apoyo a las otras áreas del SII, con el fin de prevenir la materialización de riesgos operacionales y optimizar el cumplimiento tributario.

2) Interpretar y aplicar la normativa técnica de la arquitectura referencial para adaptarse a las nuevas tecnologías, incorporar mejoras, adoptar buenas prácticas y gestionar la obsolescencia tecnológica.

3) Asegurar la disponibilidad centralizada, asequible, actualizada y vigente de la documentación de la arquitectura referencial.

4) Establecer un plan de apoyo a los especialistas técnicos de la SDTI para facilitar la adopción de los lineamientos en las aplicaciones.

5) Contar con indicadores que permitan mostrar la evolución en el uso de nuevas tecnologías y los eventos que generan riesgos en la operación de los sistemas.

En el ámbito de aseguramiento de calidad:

6) Definir y promover políticas, estrategias, procedimientos y mejores prácticas para fortalecer la calidad de los sistemas computacionales, considerando aspectos funcionales, no funcionales, y los lineamientos técnicos proporcionados por los equipos técnicos relacionados con Plataforma Tecnológica, Ciberseguridad, Ingeniería de Datos, Producción y Arquitectura de Software.

7) Gestionar los ambientes y datos de prueba (funcionales, diseñados por expertos de negocio, con requisitos y criterios de aceptación; y no funcionales, de rendimiento, carga, condiciones de estrés, estabilidad, confiabilidad, compatibilidad, accesibilidad y usabilidad de los sistemas). Velar por su correcta realización, homologación funcional, seguridad y protección de los datos, los criterios utilizados y los riesgos operacionales detectados, considerando un reporte final de evaluación de resultados y la trazabilidad de los hallazgos.

8) Promover y validar que los desarrollos de software incorporen la realización de pruebas unitarias.

9) Evaluar herramientas y automatizar los procesos de pruebas por medio de modelos, procedimientos y herramientas que faciliten la determinación de los niveles de calidad de un sistema y/o componentes del software.

10) Promover una visión de mejora continua en el desarrollo de sistemas (evidenciar la calidad de las pruebas, generar indicadores, retroalimentar a los distintos procesos del área tecnológica) y capacitar a los equipos.

11) Manejar la documentación y normas, de manera única y de fácil acceso, con el fin de fomentar la estandarización y buenas prácticas de calidad de los sistemas tecnológicos.

Para hacer efectiva la implementación de estas funcionalidades, la Oficina estará constituida por las siguientes Áreas:

- Área de Arquitectura de Software (sucesora del Área de Arquitectura e Innovación Tecnológica dependiente del ex Departamento de Aseguramiento de Estándares Tecnológicos).
- Área de Aseguramiento de Calidad (sucesora del Área de Calidad de Sistemas dependiente del ex Departamento de Aseguramiento de Estándares Tecnológicos).

DÉCIMO: A la **Oficina Ingeniería de Datos**, sucesora de la Oficina Sistemas de Inteligencia de Negocios, le corresponderá diseñar, gobernar y operar la arquitectura de datos, gestionar y controlar técnicamente todas las integraciones y procesamiento masivo de los datos y brindar apoyo técnico y herramientas de análisis, aplicando normas de seguridad que den cumplimiento a las normas, con el fin de responder a la demanda interna y externa de los datos, garantizando su confiabilidad, oportunidad, y trazabilidad para soportar la operación y la toma de decisiones en los niveles estratégicos, tácticos y operacionales del SII.

En el ámbito de la exploración y análisis de datos:

1) Proponer y elaborar componentes tecnológicas que mejoren la eficiencia y eficacia del análisis de los datos acumulados para apoyar el conocimiento que genera valor y contribuye a mejorar la gestión interna del SII.

2) Brindar un soporte transversal a las áreas de negocio para implementar soluciones integrales que faciliten el apoyo a los procesos de negocios, servicios de datos, sistemas de producción y a los funcionarios/as a cumplir con los objetivos institucionales, empleando herramientas y sistemas analíticos (análisis en línea, múltiples fuentes, generando indicadores, etc.).

3) Desarrollar e implementar mecanismos de control automatizados del cumplimiento tributario, tanto selectivos como masivos, utilizando las soluciones adecuadas a cada situación

4) Fomentar y participar en el desarrollo de capacidades analíticas al interior del SII a través de actividades de transferencia de conocimiento y capacitación.

5) Administrar el contenido de los repositorios de datos analíticos.

En el ámbito del procesamiento distribuido de datos masivos:

6) Brindar un soporte transversal a todas las áreas de negocio, implementando soluciones de procesamiento distribuido de datos masivos para ser ejecutados de manera periódica y automática, aportando en la eficiencia del uso de los recursos y en la entrega oportuna de resultados a los procesos operacionales.

7) Administrar el contenido de los repositorios de datos masivos que darán soporte a la toma de decisiones de los usuarios de esta Oficina, asegurando la completitud, consistencia, integridad y calidad de los datos.

8) Proponer y desarrollar iniciativas que permitan avanzar en los procesos analíticos, explorando acciones de ciencia de datos, apoyando a las áreas de negocio a encontrar un mejor valor y oportunidad de los datos.

9) Promover iniciativas que empleen técnicas actualizadas para la gestión y exploración de la información tributaria, empleando técnicas de aprendizaje automático u otros algoritmos más desarrollados.

10) Investigar el uso de tecnologías de vanguardia en procesos de negocio que generan y utilizan datos, desarrollando soluciones que puedan integrarse con aplicaciones operacionales.

En el ámbito de arquitectura de datos:

11) Proponer estrategia y gobierno para los modelos de datos, basado en principios y dominios de negocio, responsables y alcance de los datos.

12) Definir estándares y lineamientos para la gestión de datos, incluyendo datos maestros y metadatos, considerando modelos, clasificación, calidad, interoperabilidad, administración de versiones, niveles de protección, controles de acceso, cifrado, enmascaramiento y retención, y velar por su cumplimiento.

13) Definir métodos y arquitectura de datos, con foco en los procesos, mensajería, comunicación entre sistemas y estándares de interoperabilidad, con su plan de actualización y dependencias, para el desarrollo analítico en los ámbitos semánticos, plataforma centralizada, gobernanza de modelos y aprendizaje automático, en relación con las definiciones estratégicas para abordar las técnicas analíticas.

14) Proponer y controlar la implementación de modelos de datos que sustenten el ciclo de vida de los datos.

15) Proponer criterios y métodos de control de seguridad y calidad de datos a las áreas técnicas responsables.

La Oficina debe contar con un registro de trazabilidad de accesos a todas las fuentes de datos que administra, junto con disponer de un reporte de utilización de estos.

Para hacer efectiva la implementación de estas funcionalidades, la Oficina Ingeniería de Datos estará constituida por las siguientes Áreas:

- Área de Sistemas de Exploración y Análisis.
- Área de Sistemas de Procesamiento Distribuido de Datos.
- Área de Arquitectura de Datos (sucesora del Área de Gobierno de Datos, dependiente del ex Departamento de Aseguramiento de Estándares Tecnológicos).

DÉCIMOPRIMERO: La **Oficina Servicios de Producción**, como sucesora de la Oficina Sistemas Productivos, es responsable de potenciar e independizar la administración, explotación, control y monitoreo de los sistemas, así como la gestión de los servicios en ambiente de producción. Para el cumplimiento de sus funciones, deberá aplicar metodologías, supervisar procesos y asegurar el cumplimiento de la normativa vigente. Las funciones principales son:

En el ámbito de gestión de servicios:

1) Definir, coordinar, controlar y mejorar la entrega y soporte de los servicios productivos, conforme a las mejores prácticas establecidas para la gestión de servicios en el ámbito de la producción.

2) Actualizar, controlar y gestionar el catálogo de servicios de productivos (componentes, cadenas de dependencias, trazabilidad de los elementos críticos, su capacidad y proyecciones de crecimiento), generar reportes periódicos con estadísticas de tasas de uso de los servicios de datos, flujo transaccional, capacidad de respuesta y rendimiento, cobertura e impacto ante fallas, promover iniciativas de mejora continua, gestionar el ciclo de vida operativo resguardando su disponibilidad, confidencialidad e integridad en todas las prestaciones y asegurando el cumplimiento de los estándares productivos.

3) Coordinar con los equipos técnicos de ciberseguridad y aseguramiento de calidad la implementación de controles y seguimientos sobre los servicios productivos, con el propósito de garantizar la protección de los datos, la continuidad operacional y gestionar su disponibilidad mediante planes de contingencia y pruebas de resiliencia.

4) Velar por la continuidad operacional de los servicios, dar seguimiento y alertar sobre el incumplimiento de los Acuerdos de Nivel de Servicios por eventos de inestabilidad e interrupciones. Gestionar las incidencias y resolver problemas, proporcionando visibilidad periódica del estado de los requerimientos, señalando su criticidad, tiempos de resolución y áreas responsables.

5) Establecer indicadores de recuperabilidad de los servicios, asegurar la existencia de sistemas respaldados y ambientes de contingencias resilientes.

<u>En el ámbito de la administración y configuración de sistemas:</u>

6) Administrar las aplicaciones y sistemas en ambiente de producción, procurando un uso eficiente de los recursos, la correcta ejecución de los procesos involucrados y el resguardo de la seguridad que garantice la continuidad operacional.

7) Coordinar, preparar y realizar el Comité Control de Cambios de la SDTI, participar activamente en los procesos de modificación de la infraestructura tecnológica y colaborar con las áreas responsables del desarrollo y mantención de sistemas para el cumplimiento de las normas e instrucciones internas de la SDTI.

8) Resguardar las versiones vigentes de los programas fuentes de los sistemas, aplicaciones y/o procesos que están en los ambientes productivos y documentar procedimientos, configuraciones y flujos operativos asociados a los servicios productivos.

9) Coordinar y atender oportunamente las alertas y contingencias que afecten a los sistemas, aplicaciones y/o procesos de producción, garantizando una respuesta eficaz que minimice el impacto en la continuidad de los servicios.

<u>En el ámbito de la explotación de sistemas en producción:</u>

10) Planificar, ejecutar y controlar la operación y explotación general de las aplicaciones y sistemas en ambiente de producción, considerando la ejecución de programas, la distribución de resultados y el mantenimiento diario de los sistemas.

11) Coordinar y atender oportunamente las alertas y contingencias que afecten a los sistemas, aplicaciones y/o procesos de producción, garantizando una respuesta eficaz que minimice el impacto en la continuidad de los servicios.

12) Administrar y gestionar el intercambio de información con los distintos organismos, tanto internos (Subdirecciones y Direcciones Regionales) como externos (Instituciones Públicas, Financieras y Organismos Internacionales), asegurando la integridad, oportunidad y seguridad de los datos compartidos.

<u>En el ámbito del monitoreo:</u>

13) Velar por la continuidad operativa de la plataforma tecnológica del SII, monitoreando permanentemente el estado y la actividad de los sistemas aplicativos y toda la infraestructura tecnológica (incluido Datacenter), con el propósito de identificar y alertar oportunamente sobre situaciones o eventos que puedan comprometer su continuidad operacional, disponibilidad, estabilidad y desempeño conforme a los estándares definidos, incluyendo aquellos relacionados con soluciones de seguridad. Además, deberá proporcionar un primer punto de contacto en el servicio de atención técnica, a fin de resolver incidentes básicos y rutinarios mediante procedimientos.

14) Incorporar elementos de monitoreo automático en los flujos transaccionales de los servicios productivos, con el fin de identificar, al menos, el número de transacciones, tiempo de respuesta, principales fuentes de consumo transaccional y los periodos de mayor actividad (fechas y horarios).

15) Generar estadísticas y proveer visibilidad sobre los datos derivados de la operación del área, con el objetivo de entregar información relevante sobre el comportamiento de sus componentes y apoyar la toma de decisiones.

La Oficina debe promover el uso eficiente de los sistemas computacionales, identificando y relevando situaciones que afecten la disponibilidad de los servicios, gestionando su normalización y estabilidad operacional.

Para hacer efectiva la implementación de estas funcionalidades, la Oficina Sistemas Productivos estará constituida por las siguientes Áreas:

- Área de Gestión de Servicios (sucesora del Área Gestión de Procesos y Servicios de la ex Oficina Gestión de Servicios Tecnológicos).
- Área de Administración y Configuración de Sistemas.
- Área de Explotación de Sistemas Productivos.
- Área de Monitoreo (sucesora del Área de Monitoreo y Operaciones de la ex Oficina Control y Comunicaciones Tecnológicas).

DÉCIMOSEGUNDO: A la **Oficina Gestión Tecnológica**, como sucesora de la Oficina Gestión de Servicios Tecnológicos, le corresponderá supervisar, controlar y dar visibilidad completa de todas las iniciativas, proyectos, presupuestos y contratos tecnológicos, proporcionando los antecedentes necesarios para facilitar la toma de decisiones y la mejora continua de la plataforma tecnológica. Además, a la Oficina le corresponderá la administración y gestión de la cartera de proyectos tecnológicos a fin de dar seguimiento y visibilidad de los avances y atrasos, relevando los beneficios y riesgos operativos, de ser necesario, para lo cual deberá contar con indicadores que permitan medir su gestión. Asimismo, le corresponderá:

<u>En el ámbito de la gestión de proyectos y procesos tecnológicos:</u>

1) Gobernar, administrar y gestionar la cartera de proyectos tecnológicos, alineada con la estrategia institucional, midiendo su desempeño y realizando las acciones necesarias para lograr una mayor eficiencia en el cumplimiento de los plazos, en el control de costos y en el alcance establecido.

2) Reportar permanentemente el avance de los proyectos, mediante informes que consideren estados y riesgos, entre otros elementos, para la gestión proactiva de las potenciales desviaciones, promoviendo la autogestión de los equipos a través de la entrega de información, herramientas y apoyo que faciliten alcanzar los objetivos de cada uno de ellos.

3) Priorizar el orden de atención de las necesidades de acuerdo con las capacidades disponibles, los lineamientos institucionales, los riesgos y el valor agregado de los servicios.

4) Velar por la correcta identificación y evaluación de los beneficios de los proyectos, mediante la vinculación de sus beneficios con el costo de los componentes requeridos.

5) Apoyar la gestión de los procesos tecnológicos, con el propósito de detectar, evaluar los riesgos y mitigar aquellos que pudieran impedir el logro de los objetivos propuestos o, en su defecto, administrar el impacto de la materialización de éstos.

6) Apoyar en la definición, implementar, medir y evaluar los procesos bajo la responsabilidad de la SDTI, velando por el cumplimiento de los compromisos establecidos en el SII.

En el ámbito de la gestión de contratos y presupuesto tecnológico:

7) Garantizar la correcta ejecución presupuestaria y el uso eficiente de los recursos fiscales.

8) Gestionar la provisión de los bienes y servicios requeridos para asegurar la continuidad operacional y el desarrollo de proyectos requeridos por el SII en coordinación con la Subdirección de Administración.

9) Administrar y gestionar los contratos que permitan la adquisición de los bienes y servicios requeridos, manteniendo un seguimiento y control continuo de evidencie su recepción y el cumplimiento de las obligaciones estipuladas a nivel de cada partida.

10) Elaborar reportes en forma oportuna para la toma de decisiones e implementación de los ajustes si son requeridos, además de asegurar el cumplimiento de los plazos y procedimientos, optimizando el desempeño financiero y la transparencia en la gestión.

11) Disponer de información sobre el estado de ejecución y avance de las adquisiciones, planificadas y emergentes, los contratos y sus presupuestos asociados, identificando y proponiendo las mejoras en cada una de las etapas del ciclo de satisfacción de necesidades.

Para hacer efectiva la implementación de estas funcionalidades, la Oficina Gestión Tecnológica estará constituida por las siguientes Áreas:

- Área de Gestión de Proyectos y Procesos Tecnológicos (sucesora del Área Gestión de Proyectos Tecnológicos de la misma Oficina).
- Área de Gestión de Contratos y Presupuesto Tecnológico.

DÉCIMOTERCERO: A todos los Departamentos y Oficinas de la SDTI les corresponderá, además:

- Administrar y controlar los contratos con proveedores de servicios orientados a potenciar y fortalecer las capacidades internas del Departamento u Oficina, actuando en conjunto con las áreas responsables de los procesos de adquisiciones y colaborando con aquella a cargo de gestionar los contratos, velando por el resguardo de los intereses del SII y apoyando el proceso de selección, evaluación, adquisición, desarrollo, mantención y soporte de nuevas tecnologías, en lo referente a su ámbito de competencia.
- Promover la gestión y fortalecimiento de los distintos procesos tecnológicos e institucionales, impulsando el desarrollo de competencias en el equipo y facilitando el trabajo colaborativo.
- Implementar indicadores que permitan evaluar su gestión.
- Promover la automatización de actividades y facilitando la mejora continua de los procesos.
- Investigar y proponer soluciones computacionales y herramientas que puedan satisfacer a las nuevas necesidades, presentando diversas alternativas de mejoras a los sistemas de producción de las áreas que le corresponde atender y a sus procesos de negocios.
- Y ejecutar otras funciones que determine quien ejerza el cargo de Subdirector/a.

DÉCIMOCUARTO: Corresponderá a quien ejerza el cargo de Subdirector/a implementar las medidas que procedan tendientes a organizar la SDTI, de acuerdo con las atribuciones, obligaciones, responsabilidades y funciones que esta Resolución otorga a los Departamentos y Oficinas bajo su dependencia.

DÉCIMOQUINTO: La creación de las nuevas Áreas al interior de esta Subdirección no implica cambios en su dotación.

DÉCIMOSEXTO: Cualquier mención, asignación de funciones, delegación de facultades u otras contenidas en resoluciones o instrucciones de este Servicio que aludan a alguno de los Departamentos, Oficinas o Áreas mencionados en la Resolución Exenta SII N°136, de 2023, se entenderán referidas a las unidades organizativas sucesoras en la Subdirección de Tecnologías de la Información. Asimismo, las jefaturas en actual ejercicio de los Departamentos, Oficinas o Áreas que cambian de dependencia y/o cambian su denominación mantendrán su vigencia hasta completar su período de nombramiento.

DÉCIMOSEPTIMO: La asignación de supervisión asociada al ejercicio del cargo, tanto para las jefaturas vigentes como para las jefaturas de Áreas que se crean, se otorgarán sólo y mientras se cumplan los requisitos de dotación para percibirla, así como los demás requisitos definidos en la Resolución Exenta SII N°2.519, de junio de 2016.

DÉCIMOCTAVO: A contar de la fecha de vigencia de la presente resolución, las instrucciones que en ella se contienen priman sobre toda norma que pugne con sus disposiciones.

DÉCIMONOVENO: La presente resolución regirá a contar de su publicación, en extracto, en el Diario Oficial y a partir de esa fecha quedan sin efecto las disposiciones de la Resolución Ex. SII N° 136, de 2023.

ANÓTESE, COMUNÍQUESE Y PUBLÍQUESE EN EXTRACTO EN EL DIARIO OFICIAL.

CAROLINA FABIOLA SARAVIA MORALES

Firmado digitalmente por CAROLINA FABIOLA SARAVIA MORALES
Fecha: 2025.10.08 21:06:16 -03'00'

DIRECTORA (S)

CDR
EMF
Distribución:

- Internet.
- Diario Oficial en extracto.

ERICK MARINKOVIC FEBRE

Firmado digitalmente por ERICK MARINKOVIC FEBRE
Fecha: 2025.10.08 16:35:12 -03'00'