SERVICIO DE ADMINISTRACIÓN TRIBUTARIA – SAT

RESOLUCIÓN DE GERENCIA GENERAL N.º 286-004-00000235

Lima, 13 de febrero de 2026.

CONSIDERANDO:

Que, mediante Edicto N.° 225 se crea el Servicio de Administración Tributaria - SAT, órgano desconcentrado especial de la Municipalidad Metropolitana de Lima, con personería jurídica de derecho público interno y con autonomía administrativa, económica, presupuestaria y financiera;

Que, mediante Decreto de Alcaldía N.° 015 publicado en el diario oficial El Peruano el 29 de septiembre de 2024 y vigente a partir del 1 de diciembre de 2024, se aprobó el Manual de Operaciones – MOP del SAT;

Que, de conformidad con lo dispuesto en el artículo 10 y el inciso c) del artículo 11 del Manual de Operaciones – MOP del SAT, la Gerencia General de la institución tiene como principal función representar y dirigir la administración, conducir y articular el planeamiento, organización, ejecución, evaluación y control de las acciones y actividades que se desarrollan en el SAT; así como la función específica de aprobar los planes y políticas institucionales que requieran de su suscripción por normatividad, en el marco de sus competencias;

Que, a través del artículo 1 de la Resolución Ministerial N.° 004-2016-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos. 2° Edición", en todas las entidades integrantes del Sistema Nacional de Informática;

Que, mediante el artículo 7 del Decreto Supremo N.° 043-2001-PCM, que aprueba el Reglamento de Organización y Funciones del INEI, se estipula que los Sistemas Nacionales de Estadística e Informática están conformados por los niveles central, departamental y local, encontrándose en este último los órganos de Estadística e Informática de las municipalidades y demás entidades públicas del ámbito local;

Que, de conformidad con el artículo 3 de la Resolución Ministerial N.° 166-2017-PCM, las entidades integrantes del Sistema Nacional de Informática deben asegurar la implementación del Sistema de Gestión de Seguridad de la Información en su institución;

Que, el numeral 109.1 del artículo 109 del Reglamento del Decreto Legislativo N.° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, aprobado mediante Decreto Supremo N.° 029-2021-PCM, indica que el Sistema de Gestión de Seguridad de la Información (SGSI) comprende el conjunto de políticas, lineamientos, procedimientos, recursos y actividades asociadas, que

gestiona una entidad con el propósito de proteger sus activos de información, de manera independiente del soporte en que estos se encuentren; asimismo contempla la gestión de riesgos e incidentes de seguridad de la información y seguridad digital, la implementación efectiva de medidas de ciberseguridad, y acciones de colaboración y cooperación;

Que, el numeral 1.1 del artículo 1 de la Resolución de Secretaría de Gobierno y Transformación Digital N.° 003-2023-PCM/SGTD, que establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas, detalla que la referida Norma Técnica Peruana NTP ISO/IEC 27001 vigente es de obligatorio uso para el análisis, diseño, implementación, operación, mantenimiento y mejora continua del SGSI;

Que, el numeral 4.1 del artículo 4 de la citada Resolución de Secretaría de Gobierno y Transformación Digital, establece que el titular de la entidad pública es responsable de la implementación del SGSI, para lo cual, como mínimo, debe aprobar las políticas y objetivos para implementar, operar, mantener y mejorar el SGSI;

Que, mediante Resolución Jefatural N.° 001-004-00004722, de fecha 23 de diciembre de 2021, se aprobó la Política General del Sistema de Gestión de Seguridad de la Información del SAT, sus objetivos y alcances;

Que, a través del Informe N.° D000001-2026-SAT-CT726 de fecha 05 de febrero de 2026, el Secretario Técnico del Comité de Gobierno Digital, hace de conocimiento la aprobación del Acta de Sesión del Comité de Gobierno Digital N.° 726-081-00000001 en reunión del 3 de febrero de 2026, la misma que contiene la propuesta de los siguientes documentos: Alcance y Límites del Sistema de Gestión de Seguridad de la Información (SGSI); Política y Objetivos Generales de Seguridad de la Información y Políticas Específicas de Seguridad de la Información del SAT. Cabe señalar que dicha propuesta subsume lo establecido en la Política General del Sistema de Gestión de Seguridad de la Información del SAT antes referida;

Que, la citada Acta de Sesión del Comité de Gobierno Digital comunica también el inicio de la etapa de operación del SGSI, tras haberse cumplido con la emisión de la documentación correspondiente en el marco del Plan de Implementación del SGSI;

Que, mediante Proveído N.° D000207-2026-SAT-GGE, de fecha 6 de febrero de 2026, la Gerencia General dispone se proyecte la Resolución de Gerencia General que apruebe el documento técnico informativo y las políticas en mención;

Estando a lo dispuesto por el artículo 10° y los incisos c) y q) del artículo 11° del Manual de Operaciones - MOP del SAT, aprobado mediante Decreto de Alcaldía N.° 015;

SE RESUELVE:

Artículo 1°.- Aprobar la Política y Objetivos Generales de Seguridad de la Información del SAT, que como anexo forma parte integrante de la presente resolución.

Artículo 2°.- Aprobar las Políticas Específicas de Seguridad de la Información del SAT, que como anexo forma parte integrante de la presente resolución.

Artículo 3°.- Aprobar el documento técnico informativo "Alcance y Límites del Sistema de Gestión de Seguridad de la Información (SGSI) del SAT", que como anexo forma parte integrante de la presente resolución.

Artículo 4°.- Disponer el inicio de la etapa de operación del Sistema de Gestión de Seguridad de la Información del SAT.

Artículo 5°.- Dejar sin efecto la Resolución Jefatural N.° 001-004-00004722, de fecha 23 de diciembre de 2021, que aprobó la Política General del Sistema de Gestión de Seguridad de la Información del SAT, sus objetivos y alcances.

Artículo 6°.- Encargar al responsable del Portal de Transparencia del SAT la publicación de la presente resolución en la página web de la entidad: www.sat.gob.pe y en la Plataforma GOB.PE (cuyo dominio es www.gob.pe).

Regístrese, comuníquese y cúmplase.

María del Pilar Caballero Estella
Gerente General
Servicio de Administración Tributaria

POLÍTICA Y OBJETIVOS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

Política: GGEPO0005

Versión: 01

GERENCIA GENERAL DEL SAT

Elaborado por: Juan Martín Camino León **Cargo/Rol:** Oficial de Seguridad y Confianza Digital	**Firma:** SAT Firma Digital – SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por CAMINO LEON Juan Martin FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 16:40:39 -05:00
Revisado por: Beatriz del Carmen Aquino Fernandez **Cargo/Rol:** Jefe de la Oficina de Modernización	**Firma:** SAT Firma Digital – SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por AQUINO FERNANDEZ Beatriz Del Carmen FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 16:52:03 -05:00
Revisado por: Silvio Elisban Aiquipa Mendoza **Cargo/Rol:** Jefe de la Oficina General de Asesoría Jurídica	**Firma:** SAT Firma Digital – Servicio de Administración Tributaria de Lima Firmado digitalmente por AIQUIPA MENDOZA Silvio Elisban FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 17:51:50 -05:00
Revisado por: Juan Martín Yarleque More **Cargo/Rol:** Oficial de Gobierno de Datos	**Firma:** SAT Firma Digital – SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por YARLEQUE MORE Juan Martin FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 16:53:29 -05:00

Revisado por: José Luis Rodriguez Alayo **Cargo/Rol:** Jefe de la Oficina de Recursos Humanos	**Firma:** SAT Firma Digital Firmado digitalmente por RODRIGUEZ ALAYO Jose Luis FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 17:35:00 -05:00
Revisado por: Wilfredo Jhon Calderon Valenzuela **Cargo/Rol:** Subgerente de Orientación y Registro	**Firma:** SAT Firma Digital SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por CALDERON VALENZUELA Wilfredo Jhon FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 17:32:12 -05:00
Revisado por: Jorge Alberto Ramirez Lopez **Cargo/Rol:** Jefe de la Oficina General de Planificación, Presupuesto y Modernización	**Firma:** SAT Firma Digital SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por RAMIREZ LOPEZ Jorge Alberto FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 16:56:02 -05:00
Revisado por: Alvaro Hernando Aquino Ingunza **Cargo/Rol:** Jefe de la Oficina General de Administración	**Firma:** SAT Firma Digital SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por AQUINO INGUNZA Alvaro Hernando FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 18:31:59 -05:00
Revisado por: Erik Ronald Soria Chuquillin **Cargo/Rol:** Gerente de Operaciones	**Firma:** SAT Firma Digital SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por SORIA CHUQUILIN Erik Ronald FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 17:31:30 -05:00
Revisado por: Sandro Ivan Rodriguez Romero **Cargo/Rol:** Jefe de la Oficina de Tecnologías de la Información	**Firma:** SAT Firma Digital SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por RODRIGUEZ ROMERO Sandro Ivan FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 17:38:34 -05:00
Revisado por: Ottoniel Waldir Tume Ledesma **Cargo/Rol:** Jefe de la Oficina General de Innovación y Desarrollo Tecnológico	**Firma:** SAT Firma Digital SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por TUME LEDESMA Ottoniel Waldir FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 17:24:03 -05:00
Aprobado por: Maria del Pilar Caballero Estella **Cargo/Rol:** Gerente General	**Firma:** SAT Firma Digital SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por CABALLERO ESTELLA Maria Del Pilar FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 18:58:30 -05:00

HOJA DE CONTROL DE VERSIONES

ÍTEM	MODIFICACIÓN	CÓDIGO - VERSIÓN	FECHA	RESPONSABLE
01	Elaboración Inicial del documento	GINPO001V01	31/12/2003	Gerencia de Informática
02	Elaboración de la segunda versión del documento	GINPO001V02	30/10/2006	
03	Elaboración de la tercera versión del documento	GINPO001V03	19/06/2012	
04	Documento Reestructurado	GINPO001V04	16/07/2014	
05	Documento Actualizado: • Se reestructuró la Introducción del documento. • Se incorporó el objetivo del documento. • Se reestructuró el alcance del documento. • Se retiró el subtítulo de objetivos de seguridad de la información en el SAT. • Se retiró subtitulo de términos y definiciones. • En el apartado 5.3, se reestructuró el Marco para el desarrollo de la Seguridad de la Información. • Se incorporó como subtítulo la Declaración de la Política y Objetivos Generales de Seguridad de la Información. • Se especificó los casos para la revisión y actualización del documento. • Se retiró el apartado de Responsabilidades.	JEFPO00401	29/08/2023	Gerencia de Informática
06	Documento actualizado: • Punto 2. Se actualizo la descripción. • Punto 4. Se agrego una resolución. • Punto 5, 5.1, 5.3, 6.1 y 6.2 Se actualizo la descripción.	JEFPO004V02	05/08/2024	Gerencia de Informática
07	Documento actualizado: • Se precisó el alcance. • Se incorporó el numeral 5 relacionado a los principios y se precisaron sus propiedades. • Se precisaron los objetivos generales.	GGEPO0005V01	14/11/2025	Oficial de Seguridad y Confianza Digital

ÍNDICE

1. INTRODUCCIÓN

En cumplimiento de los requisitos establecidos en la Norma Técnica Peruana NTP ISO/IEC 27001:2022. “Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 3ra Edición”, el Servicio de Administración Tributaria (SAT) de Lima, ha establecido su política y objetivos generales de seguridad de la información, como evidencia del liderazgo y compromiso ***que existe*** en la entidad con respecto al Sistema de Gestión de Seguridad de la Información.

2. OBJETIVO

Definir la postura institucional del Servicio de Administración Tributaria (SAT) ***de Lima,*** respecto a la seguridad de la información que genera, procesa ***y*** almacena, y establecer un marco general que permita lograr niveles de seguridad aceptables***,*** de conformidad con los requisitos establecidos en la Norma Técnica Peruana NTP ISO/IEC 27001:2022.

3. ALCANCE

Lo contenido en el presente documento ***es aplicable a*** todas las personas vinculadas laboral o contractualmente con el SAT y que ***en el marco de sus funciones utilizan***, administran o acceden a activos de información de la entidad. ***Asimismo, aplica como marco de referencia para las partes interesadas externas que interactúan con el SAT en el tratamiento de información, incluyendo ciudadanos, proveedores y organismos reguladores, en la medida que corresponda.***

4. DOCUMENTOS DE REFERENCIA

Normativa Legal

- ***Decreto Legislativo n.º 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.***
- ***Decreto Supremo n.º 029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo n.º 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.***
- Resolución de Secretaria de Gobierno y Transformación Digital n.º 003-2023-PCM/SGTD. Establece la implementación ***y*** mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas.
- Norma Técnica Peruana NTP-ISO/IEC 27001:2022. Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 3ra Edición.
- ***Decreto de alcaldía n.º 15 “Aprueban el Manual de operaciones – MOP del Servicio de Administración Tributaria de la Municipalidad Metropolitana de Lima”.***

Las referidas normas incluyen sus respectivas disposiciones y normas modificatorias de ser el caso.

Documentos relacionados

- ***Política Específicas de Seguridad de la Información del SAT vigente.***
- ***Manual de Operaciones, vigente.***

5. PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACION EN EL SAT

5.1. Definición de la Seguridad de la Información en el SAT

En el SAT de Lima, la seguridad de la información se entiende como el estado deseado de preservar sus características fundamentales de confidencialidad, integridad y disponibilidad, así como otras propiedades asociadas cuando sean relevantes, independientemente del medio o formato en que se encuentre.

5.2. Propiedades fundamentales de la Información

En el SAT ***de Lima, se reconocen como propiedades fundamentales de la información a las siguientes:***

- **Confidencialidad**: ***la información no debe ponerse a disposición ni divulgarse a personas, entidades o procesos no autorizados.***
- **Integridad**: ***la información debe ser exacta, completa y no alterarse indebidamente desde su origen hasta su destino.***
- **Disponibilidad**: ***la información debe ser accesible y utilizable por una entidad autorizada en el momento que esta lo requiera.***

5.3. *Otras propiedades* relevantes *para* la Seguridad de la Información

En el SAT ***de Lima, también*** se consideran relevantes ***las*** siguientes ***propiedades asociadas a la información***:

- **Autenticidad**: ***propiedad que garantiza que la información proviene de una fuente legítima y verificada.***
- ***Responsabilidad****: asegura que las acciones sobre la información puedan ser atribuidas a una persona, sistema o proceso.*
- **No repudio**: ***propiedad que asegura que la ocurrencia de un evento o acción puede ser demostrada de manera confiable, de tal forma que la persona o entidad que la originó no pueda negar haberla realizado.***
- ***Fiabilidad: propiedad referida al grado en que la información y los sistemas de información son consistentes con el comportamiento previsto y los resultados esperados***

5.4. Marco para el desarrollo de la Seguridad de la Información

Para alcanzar niveles de protección adecuados y aceptables de ***la confidencialidad, integridad, disponibilidad y demás propiedades relevantes de la información en el Servicio de Administración Tributaria (SAT) de Lima,*** la ***Gerencia General*** y el Comité de Gobierno y Transformación Digital ***de la entidad*** han ***establecido que la seguridad de la información*** debe gestionarse mediante un proceso sistemático, documentado***, basado en un enfoque de riesgos*** y conocido por toda la organización.

En este contexto*,* se ha tomado la decisión estratégica de implementar, mantener, operar y orientar hacia una mejora continua, un Sistema de Gestión

de Seguridad de la Información (SGSI) basado en la ***Norma Técnica Peruana NTP*** ISO/IEC 27001:2022.

6. DECLARACIÓN DE LA POLÍTICA Y OBJETIVOS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

6.1. Política de Seguridad de la Información

En el Servicio de Administración Tributaria ***(SAT)*** de Lima, reconocemos que la información es un activo valioso que debe ser gestionado adecuadamente para desarrollar eficazmente nuestras funciones y alcanzar los objetivos estratégicos. ***Por esta*** razón, implementamos un Sistema de Gestión de Seguridad de la Información (SGSI), conforme a la normativa vigente, y asumimos los siguientes compromisos relacionados con la seguridad de la información:

- Fortalecer las medidas que aseguren la continuidad operativa y la ***protección*** de los sistemas de información de la entidad, a fin de brindar al ciudadano canales de atención permanentes, ***seguros*** y confiables.

- Implementar, ***mantener*** y mejorar continuamente mecanismos para preservar la confidencialidad, integridad y disponibilidad de la información que se recibe, procesa, comparte y almacena en el SAT, independientemente del medio que la contenga.

- Fomentar y promover el compromiso con la seguridad de la información entre el personal de la entidad con el fin de asegurar un uso adecuado y seguro de los activos de información y el cumplimiento de la legislación y normas aplicables.

6.2. Objetivos Generales de la Seguridad de la Información

Los objetivos generales de seguridad de la información que el SAT persigue con la implementación del SGSI, se han definido tomando ***como referencia*** lo establecido en el artículo 1 de la RSGTD N°003-2023-PCM/SGTD, y son:

- ***Garantizar la disponibilidad y continuidad de los servicios y sistemas de información del SAT.***

- ***Preservar la confidencialidad, integridad y disponibilidad de la información institucional.***

- ***Gestionar los riesgos de seguridad de la información, manteniéndolos en niveles aceptables para la entidad.***

- ***Proteger la información y activos asociados frente a eventos e incidentes de seguridad.***

- ***Fortalecer la cultura de seguridad de la información en los servidores y colaboradores del SAT.***

- ***Asegurar la difusión, atención y el cumplimiento de la normativa aplicable en materia de seguridad de la información y confianza digital.***

7. REVISIÓN Y ACTUALIZACIÓN

La política y objetivos generales de seguridad de la información, serán revisados por lo menos una vez al año o cuando resulte necesario debido a cambios en el marco normativo aplicable o del enfoque de riegos de la entidad. La revisión debe ser realizada por el Oficial de Seguridad y Confianza Digital quien deberá proponer la actualización correspondiente.

SAT
SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA

POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Política: GGEPO0004

Versión 01

GERENCIA GENERAL DEL SAT

Elaborado por: Juan Martín Camino León **Cargo/Rol:** Oficial de Seguridad y Confianza Digital	**Firma:** SAT Firma Digital SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por CAMINO LEON Juan Martin FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 16:41:17 -05:00
Revisado por: Beatriz del Carmen Aquino Fernandez **Cargo/Rol:** Jefe de la Oficina de Modernización	**Firma:** SAT Firma Digital SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por AQUINO FERNANDEZ Beatriz Del Carmen FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 16:50:46 -05:00
Revisado por: Silvio Elisban Aiquipa Mendoza **Cargo/Rol:** Jefe de la Oficina General de Asesoría Jurídica	**Firma:** SAT Firma Digital Servicio de Administración Tributaria de Lima Firmado digitalmente por AIQUIPA MENDOZA Silvio Elisban FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 17:49:42 -05:00
Revisado por: Juan Martín Yarleque More **Cargo/Rol:** Oficial de Gobierno de Datos	**Firma:** SAT Firma Digital SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por YARLEQUE MORE Juan Martin FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 16:52:41 -05:00

Revisado por: José Luis Rodriguez Alayo **Cargo/Rol:** Jefe de la Oficina de Recursos Humanos	**Firma:** SAT Firma Digital Servicio de Administración Tributaria de Lima Firmado digitalmente por RODRIGUEZ ALAYO Jose Luis FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 17:34:26 -05:00
Revisado por: Wilfredo Jhon Calderon Valenzuela **Cargo/Rol:** Subgerente de Orientación y Registro	**Firma:** SAT Firma Digital SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por CALDERON VALENZUELA Wilfredo Jhon FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 17:31:08 -05:00
Revisado por: Jorge Alberto Ramirez Lopez **Cargo/Rol:** Jefe de la Oficina General de Planificación, Presupuesto y Modernización	**Firma:** SAT Firma Digital SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por RAMIREZ LOPEZ Jorge Alberto FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 16:54:43 -05:00
Revisado por: Alvaro Hernando Aquino Ingunza **Cargo/Rol:** Jefe de la Oficina General de Administración	**Firma:** SAT Firma Digital SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por AQUINO INGUNZA Alvaro Hernando FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 18:41:11 -05:00
Revisado por: Erik Ronald Soria Chuquillin **Cargo/Rol:** Gerente de Operaciones	**Firma:** SAT Firma Digital SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por SORIA CHUQUILIN Erik Ronald FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 17:33:34 -05:00
Revisado por: Sandro Ivan Rodriguez Romero **Cargo/Rol:** Jefe de la Oficina de Tecnologías de la Información	**Firma:** SAT Firma Digital SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por RODRIGUEZ ROMERO Sandro Ivan FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 17:37:53 -05:00
Revisado por: Ottoniel Waldir Tume Ledesma **Cargo/Rol:** Jefe de la Oficina General de Innovación y Desarrollo Tecnológico	**Firma:** SAT Firma Digital SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por TUME LEDESMA Ottoniel Waldir FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 17:23:08 -05:00
Aprobado por: Maria del Pilar Caballero Estella **Cargo/Rol:** Gerente General	**Firma:** SAT Firma Digital SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por CABALLERO ESTELLA Maria Del Pilar FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 18:54:26 -05:00

Nro.	MODIFICACIÓN	CÓDIGO VERSIÓN	FECHA	RESPONSABLE
01	Elaboración Inicial del Documento	GGEPO0004V01	18/08/2025	Oficial de Seguridad y Confianza Digital

INDICE

1. INTRODUCCION

En el marco de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) del Servicio de Administración Tributaria (SAT), se establece el presente documento de Políticas Específicas de Seguridad de la Información, cuyo propósito es complementar la Política y Objetivos Generales de Seguridad de la Información mediante lineamientos específicos que fortalezcan la protección de la información y de los activos asociados.

Ambas políticas deben ser formalmente documentadas, comunicadas y adoptadas por todo el personal de la entidad, así como por terceros y contratistas vinculados con el SAT, constituyéndose en un marco de referencia obligatorio para garantizar la gestión segura y responsable de la información.

2. OBJETIVO

Establecer lineamientos específicos que complementen la Política y Objetivos Generales de Seguridad de la Información del SAT y orienten la implementación de controles alineados con la NTP ISO/IEC 27002, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información institucional y asegurar el cumplimiento de los objetivos de seguridad definidos por la entidad.

3. ALCANCE

Este documento cubre lineamientos aplicables a la gestión y uso seguro de la información y sus activos asociados, incluyendo sistemas, aplicaciones, infraestructuras tecnológicas y servicios relacionados.

Su aplicación está alineada con los compromisos establecidos en la Política y Objetivos Generales de Seguridad de la Información, la normativa legal vigente y los requerimientos de seguridad de las partes interesadas relevantes.

El cumplimiento es obligatorio para todas las unidades orgánicas y el personal del SAT, así como para terceros y contratistas que, en el marco de sus actividades vinculadas con la entidad, accedan, procesen, transmitan o almacenen información institucional.

4. DOCUMENTOS DE REFERENCIA

Normativa Legal

- Decreto Legislativo n.º 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Decreto Supremo n.º 029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo n.º 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
- Resolución de Secretaria de Gobierno y Transformación Digital n.º 003-2023-PCM/SGTD. Establece la implementación, mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas.
- Norma Técnica Peruana NTP ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos.
- Norma Técnica Peruana NTP ISO/IEC 27002:2022. Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información.
- Resolución de Gerencia General n.º 286-004-00000109, que aprueba la actualización del Plan de Continuidad Operativa del Servicio de Administración Tributaria de Lima,

Las referidas normas incluyen sus respectivas disposiciones ampliatorias, modificatorias, complementarias y conexas, de ser el caso.

Documentos relacionados

- Política y Objetivos Generales de Seguridad de la Información del SAT vigente.
- Plan de Continuidad Operativa del Servicio de Administración Tributaria de Lima vigente.

5. DEFINICIONES

Para efectos del presente documento, se consideran las siguientes definiciones:

a. **Activo de información**: Cualquier recurso que soporte la gestión, procesamiento, transmisión o almacenamiento de información institucional y que tenga valor para la entidad (ej. datos, aplicaciones, infraestructura, documentación, conocimiento).

b. **Amenaza:** Causa potencial de un incidente no deseado que puede provocar un daño a los activos de información, a los procesos de negocio o a la organización en su conjunto. Una amenaza puede ser de origen natural, humano o tecnológico, intencional o accidental.

c. **Ciclo de vida del activo:** Conjunto de etapas por las que transita un activo de información desde su creación o adquisición hasta su disposición final. Generalmente incluye las fases de identificación, clasificación, uso, mantenimiento, almacenamiento, transferencia, respaldo y eliminación o destrucción segura.

d. **Confidencialidad**: Propiedad que asegura que la información sea accesible solo a las personas, entidades o procesos autorizados.

e. **Control de seguridad**: Medida administrativa, técnica, física u organizativa implementada para gestionar riesgos de seguridad de la información.

f. **Cuenta de usuario:** Es la identidad digital que se crea en un sistema de información para permitir que un usuario acceda a recursos específicos. Está compuesta de un identificador (nombre de usuario, correo) y credenciales de autenticación (contraseña, token, etc.).

g. **Disponibilidad**: Propiedad de que la información y los sistemas estén accesibles y utilizables cuando los requieran las personas o procesos autorizados.

h. **Evento de seguridad**: Ocurrencia identificada en un sistema, servicio o red que puede indicar una posible vulnerabilidad o fallo en los controles de seguridad.

i. **Incidente de seguridad de la información**: Evento o serie de eventos no deseados o inesperados que comprometen o tienen el potencial de comprometer la confidencialidad, integridad o disponibilidad de la información.

j. **Información institucional**: Conjunto de datos y registros, en cualquier formato o medio, generados, procesados o custodiados por el SAT en el marco de sus funciones.

k. **Integridad**: Propiedad de salvaguardar la exactitud y completitud de la información y de sus métodos de procesamiento.

l. **Medios removibles:** Dispositivos de almacenamiento de datos que pueden conectarse o desconectarse fácilmente de un sistema informático, tales como memorias USB, discos externos, CD, DVD, tarjetas de memoria u otros soportes equivalentes.

m. **Riesgo:** Combinación de la probabilidad de que ocurra un evento que afecte a la seguridad de la información y de la magnitud de las consecuencias resultantes para la organización. El riesgo se evalúa considerando amenazas, vulnerabilidades y controles existentes.

n. **Terceros:** Personas naturales o jurídicas externas a la entidad (ej. contratistas, proveedores, consultores) que, en el marco de sus funciones o servicios, acceden, procesan o custodian información institucional.

o. **Usuario:** Es la persona (servidor, funcionario, terceros u otro individuo autorizado) que interactúa con los sistemas, aplicaciones o recursos informáticos de la entidad.

6. PRINCIPIOS RECTORES DE LA SEGURIDAD DE LA INFORMACIÓN

Las Políticas Específicas de Seguridad de la Información del SAT se rigen por los siguientes principios:

a. **Proporcionalidad**: Los controles de seguridad deben ser adecuados y proporcionales al nivel de riesgo identificado y a la criticidad de los activos.
b. **Cumplimiento normativo**: Todas las acciones deben alinearse con la Política General de Seguridad de la Información, la normativa legal vigente y los estándares internacionales aplicables.

c. **Responsabilidad compartida**: La seguridad de la información es una responsabilidad de todo el personal, así como de terceros y contratistas vinculados con la entidad, cada uno en el ámbito de sus funciones y roles asignados.

d. **Responsabilidad legal y ética:** Todas las acciones relacionadas con la gestión de la seguridad de la información deben cumplir con las leyes, regulaciones y normativas aplicables, así como con principios éticos que garanticen un uso responsable, transparente y honesto de la información institucional y de los datos de los ciudadanos.

e. **Prevención y mejora continua**: Se prioriza la prevención de riesgos e incidentes de seguridad mediante la implementación de controles proactivos, así como la revisión y mejora continua del SGSI.

f. **Confidencialidad, integridad y disponibilidad**: Toda la gestión de seguridad se orienta a garantizar estos tres pilares fundamentales de la información institucional.

g. **Transparencia y trazabilidad**: Las actividades relacionadas con la seguridad de la información deben registrarse y ser auditables, asegurando control y rendición de cuentas.

7. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas específicas de seguridad de la información constituyen directrices de cumplimiento obligatorio que orientan la implementación de controles y buenas prácticas, alineadas con la NTP ISO/IEC 27002:2022, con el propósito de proteger los activos de información institucional frente a amenazas internas y externas.

Cada política se presenta de manera estructurada, indicando su objetivo y los lineamientos que deben ser observados por el personal de la entidad, así como por terceros y contratistas que accedan o gestionen información institucional.

Con el fin de complementar la Política y Objetivos Generales de Seguridad de la Información y dar cumplimiento a los objetivos de seguridad definidos para el SAT, se establecen las siguientes políticas específicas:

1. Política de Control de Accesos
2. Política de Clasificación y manejo de información
3. Política de Gestión y uso de activos y recursos tecnológicos
4. Política de Seguridad de los medios removibles
5. Política de seguridad en dispositivos móviles y acceso remoto
6. Política de Escritorio y pantalla limpia
7. Política de Seguridad en las relaciones con proveedores y terceros
8. Política de Seguridad física y áreas seguras
9. Política de Seguridad en redes y comunicaciones
10. Política de Copias de respaldo y recuperación
11. Política de Seguridad en el desarrollo y adquisición de software
12. Política de Gestión de vulnerabilidades técnicas
13. Política de Gestión de incidentes de seguridad de la información
14. Política de Continuidad de negocio y recuperación ante desastres

El cumplimiento de estas políticas será evaluado mediante auditorías internas y revisiones periódicas del Oficial de Seguridad y Confianza Digital.

7.1. Política de control de accesos

Objetivo: Garantizar que el acceso a la información, sistemas, aplicaciones e infraestructuras tecnológicas del SAT se realice de manera autorizada, controlada y en función de los roles y responsabilidades asignados, protegiendo la confidencialidad, integridad y disponibilidad de los activos de información.

Lineamientos:

- Todo acceso a los sistemas y activos de información debe basarse en los principios de acceso por roles, mínimo privilegio y necesidad de uso o conocimiento.
- Los usuarios deben acceder a los sistemas de información mediante una cuenta de usuario única, de carácter personal e intransferible.
- Está prohibido el uso de cuentas de usuario compartidas o que en un sistema se habilite más de una cuenta para un usuario, salvo casos excepcionales autorizados por la Oficina de Tecnologías de la Información, en los cuales se deben implementar controles compensatorios.
- Los usuarios son responsables de la custodia de sus credenciales, quedando estrictamente prohibido compartirlas con otros usuarios internos o externos.
- Toda acción realizada en los sistemas de información con una cuenta de usuario será atribuida a la persona a quien se asignó la cuenta, salvo que existan evidencias técnicas verificables que sugieran lo contrario. En tales casos, la atribución quedará sujeta a revisión de la entidad.
- La gestión de identidades y accesos debe seguir un proceso formal que incluya la creación, modificación, revisión periódica y eliminación de cuentas de usuario.
- Los accesos deben otorgarse en atención a un requerimiento, el cual debe ser registrado por un solicitante autorizado. Se debe documentar y mantener la trazabilidad desde el registro hasta la atención y habilitación del acceso requerido, incluyendo las autorizaciones que correspondan.

- Se deben aplicar mecanismos de autenticación seguros, priorizando el uso de contraseñas robustas y/o autenticación multifactor (MFA) para accesos críticos.
- Los privilegios de administrador y cuentas con permisos especiales deben ser restringidos, estar justificados, auditados y sujetos a revisiones periódicas.
- Los accesos de terceros y contratistas deben ser temporales, controlados y revocados inmediatamente al finalizar la relación contractual o el servicio.
- Se deben realizar revisiones semestrales de todos los accesos de usuario, con el fin de identificar y revocar accesos innecesarios o indebidos.
- Los accesos de emergencia deben estar restringidos, documentados, monitoreados y sujetos a auditoría inmediata tras su uso.
- Se debe definir un periodo y procedimiento de oficio para deshabilitar y eliminar, cuando ya no sean necesarias, las cuentas de usuario que presenten inactividad.
- Todo acceso no autorizado, sospechoso o indebido debe ser reportado como incidente de seguridad.

7.2. Política de clasificación y manejo de información

Objetivo: Establecer un marco de clasificación y manejo adecuado de la información institucional, de acuerdo con su nivel de sensibilidad, criticidad y valor para la entidad, con el fin de garantizar su confidencialidad, integridad y disponibilidad, así como el cumplimiento de la normativa legal vigente.

Lineamientos:

- Debe definirse, documentarse y aplicarse un esquema de clasificación para la información institucional (ejemplo: Pública, Interna, Confidencial y Restringida).
- Debe asignarse formalmente la propiedad de los activos de información. Los propietarios son responsables de su clasificación, con el apoyo del equipo de seguridad informática.
- El etiquetado y marcado de la información debe realizarse tanto en medio digital como físico, conforme al nivel de clasificación asignado.
- El almacenamiento, procesamiento y transmisión de la información debe realizarse aplicando controles de seguridad acordes con su clasificación (ejemplo: cifrado para información Confidencial o Restringida).
- Está prohibida la divulgación no autorizada de información clasificada.
- Debe establecerse un proceso de revisión anual de la clasificación de la información, a fin de asegurar que su nivel se mantenga actualizado según cambios en su sensibilidad o valor.
- La eliminación y destrucción de información (física o digital) debe realizarse de manera segura y conforme a su clasificación, evitando la recuperación o uso indebido posterior.
- La información de carácter personal o sujeta a reserva legal deberá recibir un tratamiento conforme a la normativa de protección de datos personales y demás disposiciones regulatorias aplicables.
- Todo el personal, terceros y contratistas deben cumplir las disposiciones de clasificación y manejo seguro de la información.

7.3. Política de gestión y uso de activos y recursos tecnológicos

Objetivo: Establecer directrices para la adecuada gestión y uso de los activos y recursos tecnológicos de la entidad, asegurando que se utilicen de forma eficiente, segura y conforme a los objetivos institucionales.

Lineamientos:

- Todos los activos de información y recursos tecnológicos deben estar inventariados, clasificados según su nivel de criticidad, asignados a un responsable y registrados en el inventario institucional de activos.
- El uso de los recursos tecnológicos debe limitarse estrictamente a fines institucionales, quedando prohibido su uso indebido o no autorizado.
- El personal debe cumplir con las restricciones y condiciones de uso establecidas por la entidad respecto de hardware, software, redes y servicios tecnológicos.
- Los equipos, sistemas y servicios tecnológicos de la entidad no deben ser modificados, configurados o intervenidos sin autorización formal y expresa de la Oficina de Tecnologías de la Información.
- Todo activo tecnológico en desuso debe ser dado de baja de manera formal y documentada, asegurando la eliminación segura y definitiva de la información que contenga.
- Los activos tecnológicos deben ser protegidos durante todo su ciclo de vida (adquisición, instalación, uso, mantenimiento y disposición final), aplicando medidas de seguridad acordes a su clasificación y criticidad.
- El uso y la administración de los activos tecnológicos deben quedar registrados o ser auditables cuando corresponda, a fin de garantizar trazabilidad y responsabilidad en su gestión.
- Todos los recursos tecnológicos son propiedad del SAT y deben ser utilizados bajo los principios de responsabilidad, seguridad, buen uso y cumplimiento normativo.
- Los activos y recursos tecnológicos deben ser sujetos de mantenimiento periódico con el fin de asegurar su correcta operación y uso seguro.
- El personal debe conocer y cumplir obligatoriamente esta política como parte de sus responsabilidades individuales en materia de seguridad de la información.

7.4. Política de seguridad de los medios removibles

Objetivo: Regular el uso de medios removibles (USB, discos externos, CDs, DVDs, tarjetas de memoria u otros) para prevenir la fuga de información, la introducción de software malicioso y otros riesgos asociados a su uso.

Lineamientos:

- El uso de medios removibles debe estar restringido y autorizado únicamente cuando sea estrictamente necesario, previa justificación y requerimiento formal de un usuario autorizado.
- Todos los medios removibles que contengan información institucional deben estar protegidos contra accesos no autorizados, mediante el uso contraseñas o de cifrado mediante herramientas aprobadas por la entidad.
- Está prohibido almacenar información clasificada como Confidencial o Restringida en medios removibles que no cuenten con protección contra accesos no autorizados o que sean de propiedad personal.
- Todo medio removible debe ser analizado con herramientas antimalware actualizadas antes de su conexión o uso en equipos de la entidad.
- La copia de información a medios removibles requiere autorización previa del Oficial de Seguridad y Confianza Digital y debe ser formalmente solicitada y registrada manteniendo la trazabilidad.
- Únicamente se permite el uso de medios removibles, previamente autorizados por la entidad.
- Los medios removibles en desuso deben ser eliminados o destruidos de manera segura, siguiendo procedimientos documentados de gestión de activos y garantizando la eliminación definitiva de la información contenida.

- Todo el personal, contratistas y terceros que hagan uso de medios removibles deben cumplir obligatoriamente con esta política y con los procedimientos que la desarrollan.

7.5. Política de seguridad en dispositivos móviles y acceso remoto

Objetivo: Establecer directrices para el uso seguro de dispositivos móviles y el acceso remoto a los recursos tecnológicos de la entidad, garantizando la protección de la información institucional frente a riesgos de pérdida, robo, uso indebido o accesos no autorizados.

Lineamientos:

- Todo acceso a la información institucional desde dispositivos móviles requiere autorización formal previa y cumplimiento estricto de las medidas de seguridad definidas por el SAT.
- Es obligatorio que todo dispositivo móvil que maneje información institucional cuente con mecanismos de autenticación segura (contraseña robusta, PIN, biometría) y bloqueo automático de pantalla.
- Los dispositivos móviles deben contar con soluciones de seguridad activas, tales como cifrado de almacenamiento, antivirus y herramientas de gestión remota en caso de pérdida o robo.
- El acceso remoto a los sistemas y servicios institucionales se debe realizar a través de canales seguros y empleando conexiones cifradas (VPN u otras tecnologías equivalentes), además de autenticación multifactor.
- Está prohibido almacenar información clasificada como Confidencial o Restringida en dispositivos móviles personales sin autorización expresa.
- El personal debe notificar de inmediato cualquier incidente relacionado con la pérdida, robo, manipulación indebida o compromiso de dispositivos móviles utilizados para fines institucionales.
- La instalación de aplicaciones o software en dispositivos móviles institucionales debe estar restringida y sujeta a control por la Oficina de Tecnologías de la Información.

7.6. Política de escritorio y pantalla limpia

Objetivo: Establecer prácticas obligatorias de orden y protección en los puestos de trabajo físicos y virtuales, con el fin de prevenir accesos no autorizados y garantizar la confidencialidad de la información institucional.

Lineamientos:

- Todos los documentos físicos que contengan información institucional deben mantenerse bajo resguardo y no permanecer visibles en escritorios, impresoras o áreas comunes sin supervisión.
- Al finalizar la jornada laboral o en ausencias prolongadas, los puestos de trabajo deben quedar libres de información sensible.
- Todo documento en papel que ya no sea requerido deberá ser destruido mediante mecanismos seguros (ej. trituradora de documentos).
- Toda estación de trabajo debe configurarse para el bloqueo automático de pantalla; adicionalmente, el personal está obligado a bloquearla manualmente cuando se ausente, incluso por periodos cortos.
- Está prohibido compartir credenciales de acceso o mantener contraseñas escritas en lugares visibles.

- El Oficial de Seguridad y Confianza Digital debe realizar revisiones periódicas para verificar el cumplimiento de esta política.

7.7. Política de seguridad en las relaciones con proveedores y terceros

Objetivo: Regular la gestión de la seguridad de la información en las relaciones con proveedores, contratistas y terceros que accedan a la información o recursos tecnológicos de la entidad, asegurando que cumplan con los requisitos de seguridad establecidos por el SAT.

Lineamientos:

- Todo contrato con proveedores o terceros que implique acceso, procesamiento o custodia de información institucional debe contener cláusulas obligatorias de seguridad de la información y confidencialidad, a fin de garantizar responsabilidades legales en caso de incumplimiento.
- Antes de otorgar acceso a sistemas, redes o instalaciones, los terceros deben firmar un acuerdo de confidencialidad específico y comprometerse por escrito a cumplir las políticas de seguridad de la entidad.
- Se debe evaluar el nivel de riesgo asociado a cada proveedor o tercero y aplicar controles proporcionales a la criticidad de la información o servicio gestionado.
- Los accesos otorgados a proveedores o terceros deben ser limitados en tiempo, alcance y privilegios, de acuerdo con el principio de mínimo privilegio.
- Los proveedores que gestionen servicios críticos deben cumplir con normativas y estándares de seguridad reconocidos, según corresponda.
- Todo incumplimiento de los requisitos de seguridad por parte de terceros podrá ser causal de sanciones contractuales, suspensión o terminación del servicio.
- El SAT se reserva el derecho de realizar supervisiones y auditorías periódicas a los servicios provistos por terceros con impacto en la seguridad de la información.

7.8. Política de seguridad física y áreas seguras

Objetivo: Proteger los activos de información y tecnológicos de la entidad contra accesos físicos no autorizados, daños accidentales o intencionados, garantizando la seguridad de las áreas críticas y restringidas.

Lineamientos:

- Las instalaciones del SAT deben contar con controles de acceso físico diferenciados según la criticidad de las áreas (ej. oficinas, data center, salas de comunicaciones).
- El acceso a áreas seguras (como centros de datos, salas de servidores y cuartos de comunicaciones) será autorizado únicamente a personal acreditado, con justificación documentada y de acuerdo con un procedimiento establecido.
- Toda visita a áreas restringidas debe estar registrada y supervisada en todo momento por personal autorizado.
- Los dispositivos de seguridad (cerraduras, cámaras, alarmas, sistemas de control de acceso) deben mantenerse operativos, con mantenimiento y pruebas periódicas.
- Todo el personal debe portar visiblemente su credencial institucional en las instalaciones de la entidad.
- Está prohibido el ingreso de dispositivos no autorizados en áreas seguras (ej. USB personales, cámaras, celulares, grabadoras).

- En caso de incidentes de seguridad física (robos, accesos indebidos, desastres), se deberán activar los mecanismos de contingencia definidos en el SGSI y en el Plan de Continuidad Operativa.

7.9. Política de seguridad en redes y comunicaciones

Objetivo: Garantizar la seguridad de la información que transita por las redes y comunicaciones institucionales, protegiéndola contra accesos no autorizados, alteraciones y pérdidas.

Lineamientos:

- Todo acceso a las redes institucionales deberá estar autenticado, registrado y monitoreado, mediante mecanismos de seguridad adecuados (ej. firewalls, IDS/IPS, AntiDDoS, WAF, VPN segura).
- La red institucional debe estar segmentada según niveles de criticidad y función, evitando accesos innecesarios entre segmentos.
- La transmisión de información sensible o confidencial debe realizarse únicamente mediante mecanismos de cifrado aprobados, tales como TLS, SSH, VPN, IPSec, S/MIME, PGP/GPG, FTPS o SFTP, garantizando la confidencialidad e integridad de los datos.
- Queda prohibido el uso de protocolos inseguros o versiones obsoletas como SSL, Telnet, FTP sin cifrado o HTTP sin TLS, salvo en casos debidamente justificados y autorizados por la Oficina de Tecnologías de la Información.
- El uso de redes inalámbricas sin cifrado seguro o sin autorización expresa de la Oficina de Tecnologías de la Información está prohibido.
- Todos los equipos conectados a la red deben cumplir con configuraciones seguras y mantenerse actualizados.
- Las comunicaciones externas con terceros deberán realizarse bajo protocolos de seguridad previamente aprobados.
- Se debe implementar registros y monitoreo continuo del tráfico de red para detectar anomalías o accesos indebidos.
- El acceso a la información institucional a través de redes públicas o no seguras está prohibido, salvo que se realice mediante canales cifrados autorizados.

7.10. Política de copias de respaldo y recuperación

Objetivo: Asegurar la disponibilidad e integridad de la información mediante la implementación de copias de respaldo y procedimientos de recuperación que garanticen la continuidad operativa de los servicios críticos de la entidad.

Lineamientos:

- Todo sistema, aplicación o base de datos crítica debe contar con un esquema documentado de copias de respaldo, aprobado por la Oficina de Tecnologías de la Información.
- Los respaldos deben ejecutarse con la frecuencia definida según la criticidad de la información y los tiempos de recuperación (RPO/RTO).
- Las copias de respaldo deben almacenarse en ubicaciones seguras, dentro y fuera del sitio principal, incluyendo sitios alternos cuando corresponda.
- Todos los respaldos deben estar cifrados y/o protegidos contra accesos no autorizados.
- Deben realizarse pruebas periódicas de restauración documentadas, para garantizar la eficacia de los procedimientos de recuperación.

- El acceso a las copias de respaldo está restringido al personal autorizado y registrado.
- Toda pérdida, daño o anomalía en los respaldos debe ser reportada como incidente de seguridad.
- Todos los registros de respaldos y restauraciones deben conservarse con fines de auditoría.

7.11. Política de seguridad en el desarrollo y adquisición de software

Objetivo: Asegurar que las soluciones de software desarrolladas o adquiridas por el SAT cumplan con requisitos de seguridad desde su diseño hasta su implementación, reduciendo riesgos de vulnerabilidades técnicas y operativas.

Lineamientos:

- Todo proyecto de desarrollo o adquisición de software debe incluir requisitos de seguridad documentados, alineados con la NTP ISO/IEC 27002:2022 y a las buenas prácticas de la industria.
- El software en desarrollo debe aplicar “seguridad desde el diseño” y seguir un ciclo de vida seguro (SDLC).
- Antes de ser implementadas en ambientes de producción, todas las aplicaciones deben someterse a pruebas de seguridad obligatorias (ej. análisis de vulnerabilidades, pruebas de penetración).
- En adquisiciones, los proveedores deben demostrar cumplimiento con estándares de seguridad aplicables y proveer documentación técnica.
- Está prohibida la instalación de software no autorizado o sin licenciamiento válido.
- El código fuente crítico debe ser gestionado en repositorios seguros con controles de acceso y trazabilidad.
- Todas las dependencias externas o librerías de terceros deben validarse y mantenerse actualizadas.
- Las actualizaciones y parches de seguridad deben aplicarse de forma oportuna y validada.
- Ninguna aplicación con vulnerabilidades críticas puede implementarse en producción hasta ser corregida.

7.12. Política de gestión de vulnerabilidades técnicas

Objetivo: Establecer lineamientos para la identificación, evaluación y tratamiento oportuno de vulnerabilidades técnicas que puedan afectar la seguridad de los sistemas, aplicaciones y redes institucionales.

Lineamientos:

- Todos los sistemas, servidores y aplicaciones deben ser objeto de escaneos periódicos de vulnerabilidades con herramientas autorizadas.
- Las vulnerabilidades detectadas deben clasificarse por criticidad (alta, media, baja) y tratarse dentro de los plazos que se definan en la entidad.
- El personal responsable debe aplicar parches y actualizaciones de seguridad de forma oportuna.
- Cuando no sea posible aplicar un parche inmediato, se deben implementar medidas compensatorias documentadas y aprobadas.
- Los hallazgos de vulnerabilidades deben registrarse y dar seguimiento hasta su cierre.
- Las pruebas de seguridad no deben afectar la disponibilidad de los sistemas críticos; deben programarse y comunicarse previamente.

- Los resultados de la gestión de vulnerabilidades deben reportarse periódicamente como parte de los procesos de gestión de riesgos y mejora continua del SGSI.

7.13. Política de gestión de incidentes de seguridad de la información

Objetivo: Garantizar una respuesta efectiva y coordinada ante incidentes de seguridad de la información, minimizando su impacto en la confidencialidad, integridad y disponibilidad de los activos institucionales.

Lineamientos:

- Todo incidente de seguridad de la información debe ser registrado y comunicado de manera inmediata al Equipo de Seguridad Informática y al Oficial de Seguridad y Confianza Digital.
- Se debe implementar y mantener un procedimiento documentado para la identificación, análisis, contención, erradicación, recuperación y cierre de incidentes.
- Todo el personal de la entidad y los terceros vinculados tienen la obligación de reportar de forma inmediata cualquier evento o actividad sospechosa que pueda constituir un incidente de seguridad.
- Los incidentes deben ser clasificados y priorizados de acuerdo con su impacto y urgencia, siguiendo criterios establecidos por la Oficina de Tecnologías de la Información.
- Toda acción realizada durante la gestión de un incidente debe quedar documentada y archivada para fines de auditoría y mejora continua.
- Después de cada incidente se realizará un análisis de lecciones aprendidas para fortalecer los controles y evitar recurrencias.
- La comunicación de incidentes graves a entes reguladores o partes externas debe realizarse conforme a los protocolos institucionales y la normativa vigente.

7.14. Política de continuidad de negocio y recuperación ante desastres

Objetivo: Asegurar la continuidad de las operaciones críticas de la entidad y la recuperación oportuna de los servicios de tecnología de la información en caso de desastres, incidentes de gran impacto o interrupciones graves, minimizando el efecto en los procesos institucionales y en la prestación de servicios a los ciudadanos.

Lineamientos:

- Se deben identificar los procesos críticos de negocio y los activos de información asociados, definiendo sus prioridades de recuperación.
- Se debe establecer y mantener actualizado un Plan de Contingencia Informático (PCI) y un Plan de Pruebas de Contingencia (PPC).
- Todo sistema crítico debe contar con objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO) formalmente definidos y aprobados.
- Los planes de contingencia y recuperación deben ser probados periódicamente, con el fin de validar su eficacia y garantizar la preparación del personal involucrado.
- Se debe mantener infraestructura y recursos alternos (sitios de respaldo, comunicaciones, energía) que garanticen la operación en escenarios de contingencia.
- Se debe asegurar la capacitación del personal clave en los procedimientos de activación, ejecución y retorno a la normalidad.
- Integrar a los planes de contingencia y recuperación, las lecciones aprendidas derivadas de cada prueba o incidente real, con el fin de fortalecerlos y mejorarlos continuamente.

8. RESPONSABILIDADES Y CUMPLIMIENTO

El cumplimiento de las políticas específicas de seguridad de la información es obligatorio para todo el personal del SAT, así como para terceros y contratistas que accedan a la información o a los recursos tecnológicos de la entidad.

Para garantizar la correcta implementación y cumplimiento de las políticas específicas de seguridad de la información, se asignan las siguientes responsabilidades:

a. Gerencia General / Comité de Gobierno y Transformación Digital:

- Aprobar las políticas de seguridad de la información.
- Aprobar los recursos humanos, tecnológicos y financieros necesarios para su implementación.
- Promover y consolidar la cultura de seguridad de la información en toda la entidad.

b. Oficial de Seguridad y Confianza Digital (OSCD):

- Coordinar la implementación, difusión, monitoreo y revisión de las políticas.
- Informar periódicamente al Comité de Gobierno y Transformación Digital y a la Gerencia General sobre el nivel de cumplimiento.
- Coordinar y supervisar la ejecución de acciones correctivas y preventivas que eviten o corrijan desviaciones de cumplimiento.
- Asesorar a las unidades orgánicas y a la Oficina de Tecnologías de la Información en la aplicación de controles de seguridad.

c. Oficina de Tecnologías de la Información (OTI):

- Implementar y administrar las soluciones tecnológicas necesarias para dar cumplimiento a las políticas de seguridad de la información.
- Mantener actualizada la infraestructura tecnológica, garantizando su disponibilidad, integridad, confidencialidad y resiliencia.
- Coordinar con el OSCD la gestión de incidentes de seguridad y vulnerabilidades técnicas.
- Velar por la correcta aplicación de controles técnicos como autenticación, cifrado, copias de seguridad, monitoreo y gestión de accesos.
- Colaborar con las auditorías internas y externas del SGSI proporcionando la información y evidencias requeridas.

d. Responsables de Unidades Orgánicas:

- Asegurar que el personal a su cargo cumpla estrictamente las políticas.
- Reportar de inmediato cualquier anomalía o incidente de seguridad al OSCD y a la Oficina de Tecnologías de la Información.
- Facilitar las actividades de concienciación y capacitación en seguridad de la información.

e. Usuarios:

- Cumplir las políticas de seguridad de la información en el desarrollo de sus funciones.
- Proteger las credenciales y accesos proporcionados por la entidad, evitando su uso indebido.

- Notificar de inmediato cualquier anomalía, vulnerabilidad o incidente de seguridad detectado.

f. Proveedores y contratistas:

- Cumplir las disposiciones establecidas en estas políticas, así como lo estipulado en los acuerdos de confidencialidad y seguridad firmados con la entidad.
- Garantizar que los servicios y productos entregados cumplan con los requisitos de seguridad establecidos por la entidad.
- Reportar oportunamente cualquier incidente de seguridad relacionado con los servicios o bienes proporcionados

9. MONITOREO, REVISIÓN Y ACTUALIZACIÓN

Las políticas de seguridad de la información serán objeto de:

- Monitoreo continuo por parte del Oficial de Seguridad y Confianza Digital, a fin de verificar su cumplimiento y detectar desviaciones.

- Revisión periódica al menos una vez al año, o antes si existen cambios significativos en el marco normativo, tecnológico, de riesgos o en la estructura de la entidad.

- Actualización y mejora conforme a los resultados de auditorías internas, revisiones de la alta dirección, lecciones aprendidas de incidentes de seguridad y recomendaciones de partes interesadas.

Los resultados del monitoreo y revisión de estas políticas deben documentarse y ser presentados al Comité de Gobierno y Transformación Digital y a la Gerencia General en el marco de la Revisión por la Dirección del SGSI, con el fin de evaluar su eficacia, identificar oportunidades de mejora y asegurar la toma de decisiones oportunas para la gestión de riesgos y controles de seguridad**.**

10. VIGENCIA Y APROBACIÓN

El presente documento de Políticas Específicas de Seguridad de la Información entra en vigor a partir de la fecha de su publicación en la Intranet Institucional del SAT, constituyéndose en políticas de cumplimiento obligatorio para todas las unidades orgánicas, personal, terceros y contratistas vinculados con la entidad.

Su revisión y actualización se realizará de manera periódica o cuando se produzcan cambios normativos, tecnológicos u organizacionales que lo requieran.

ALCANCE Y LIMITES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Documento Técnico Informático: OTIDT0001

Versión: 01

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

Elaborado por: Juan Martin Camino León **Cargo/Rol:** Oficial de Seguridad y Confianza Digital	**Firma:** SAT Firma Digital – SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por CAMINO LEON Juan Martin FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 16:06:54 -05:00
Revisado por: Kevin Maison Cámara Palomino **Cargo/Rol:** Analista III Organización y Procesos	**Firma:** SAT Firma Digital – Servicio de Administración Tributaria de Lima Firmado digitalmente por CAMARA PALOMINO Kevin Maison FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 16:16:31 -05:00
Revisado por: Beatriz del Carmen Aquino Fernández **Cargo/Rol:** Jefe de la Oficina de Modernización	**Firma:** SAT Firma Digital – SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por AQUINO FERNANDEZ Beatriz Del Carmen FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 16:37:50 -05:00
Revisado por: Silvio Elisban Aiquipa Mendoza **Cargo/Rol:** Jefe de la Oficina General de Asesoría Jurídica / Oficial de Datos Personales	**Firma:** SAT Firma Digital – Servicio de Administración Tributaria de Lima Firmado digitalmente por AIQUIPA MENDOZA Silvio Elisban FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 17:47:32 -05:00

Revisado por: Juan Martin Yarleque More **Cargo/Rol:** Oficial de Gobierno de Datos	**Firma:** SAT Firma Digital – SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por YARLEQUE MORE Juan Martin FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 16:39:51 -05:00
Revisado por: Jose Luis Rodriguez Alayo **Cargo/Rol:** Jefe de la Oficina de Recursos Humanos	**Firma:** SAT Firma Digital – Servicio de Administración Tributaria de Lima Firmado digitalmente por RODRIGUEZ ALAYO Jose Luis FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 17:33:45 -05:00
Revisado por: Wilfredo Jhon Calderon Valenzuela **Cargo/Rol:** Subgerente de Orientación y Registro	**Firma:** SAT Firma Digital – SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por CALDERON VALENZUELA Wilfredo Jhon FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 17:11:52 -05:00
Revisado por: Jorge Alberto Ramirez Lopez **Cargo/Rol:** Jefe de la Oficina General de Planeamiento, Presupuesto y Modernización	**Firma:** SAT Firma Digital – SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por RAMIREZ LOPEZ Jorge Alberto FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 16:52:59 -05:00
Revisado por: Alvaro Hernando Aquino Ingunza **Cargo/Rol:** Jefe de la Oficina General de Administración	**Firma:** SAT Firma Digital – SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por AQUINO INGUNZA Alvaro Hernando FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 18:38:55 -05:00
Revisado por: Erik Ronald Soria Chuquillin **Cargo/Rol:** Gerente de Operaciones	**Firma:** SAT Firma Digital – SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por SORIA CHUQUILIN Erik Ronald FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 17:36:10 -05:00
Aprobado por: Sandro Iván Rodriguez Romero **Cargo/Rol:** Jefe de la Oficina de Tecnologías de la Información/ Secretario Técnico	**Firma:** SAT Firma Digital – SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por RODRIGUEZ ROMERO Sandro Ivan FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 17:37:14 -05:00
Aprobado por: Ottoniel Waldir Tume Ledesma **Cargo/Rol:** Jefe de la Oficina General de Innovación y Desarrollo Tecnológico	**Firma:** SAT Firma Digital – SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por TUME LEDESMA Ottoniel Waldir FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 17:22:05 -05:00
Aprobado por: Maria del Pilar Caballero Estella **Cargo/Rol:** Gerente General/ Líder de Gobierno y Transformación Digital del SAT	**Firma:** SAT Firma Digital – SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA Firmado digitalmente por CABALLERO ESTELLA Maria Del Pilar FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 04.02.2026 18:48:30 -05:00

HOJA DE CONTROL DE CAMBIOS

Nro.	MODIFICACIÓN	CÓDIGO - VERSIÓN	FECHA	RESPONSABLE
1	Elaboración inicial del documento	GINDT052 V01	30/07/2024	Gerencia de Informática
2	Documento actualizado: • Se modifica por cambio de estructura organizacional. • Se actualizó la nomenclatura de los procesos nivel 0 y 1 de “Alcance del SGSI” dada la entrada en vigencia del nuevo Mapa de Procesos del SAT, así como los puntos 6.2 y 6.3 en donde se mencionan.	OTIDT0001 V01	03/02/2026	Oficina de Tecnologías de la Información

ÍNDICE

1. INTRODUCCION

El Servicio de Administración Tributaria - SAT, como parte de su compromiso por preservar la seguridad de la información en la entidad, ha tomado la decisión estratégica de implementar un Sistema de Gestión de la Seguridad de la Información (SGSI), el cual debe cumplir con los requisitos de la Norma Técnica Peruana NTP ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos. 3ª Edición.

Entre los requisitos establecidos por la mencionada norma, se establece la necesidad de determinar el alcance del SGSI, el cual debe estar disponible como información documentada.

2. OBJETIVO

Determinar los límites y la aplicabilidad del Sistema de Gestión de Seguridad de la Información (en adelante SGSI) del Servicio de Administración Tributaria (SAT) de Lima, para establecer su alcance, en concordancia con los requisitos establecidos en la norma técnica peruana NTP ISO/IEC 27001:2022.

3. ALCANCE

En el presente documento, se describen los procesos y las actividades de negocio, unidades orgánicas, ubicaciones físicas e infraestructura de TI que se encuentran incluidas dentro del alcance del SGSI del SAT.

4. DOCUMENTOS DE REFERENCIA

- Norma Técnica Peruana NTP ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos. 3ª Edición.
- Estándar Internacional ISO/IEC 27000:2018. “Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Visión general y vocabulario”.
- Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.
- Decreto Supremo Nº 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, que establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las Entidades Públicas.
- Documento: Plan de Implementación del Sistema de Gestión de Seguridad de la Información del SAT.
- Documento: Mapa de procesos del SAT.
- Documento: Análisis de Contexto para el Sistema de Gestión de Seguridad de la información.
- Documento: Requisitos de Seguridad de las partes interesadas del Sistema de Gestión de Seguridad de la información (SGSI).

5. TERMINOS Y DEFINICIONES

En el presente documento se utilizan las siguientes definiciones y abreviaturas consideradas en la Norma ISO/IEC 27000:2018: Tecnología de la Información – Técnicas de seguridad – Sistemas de Gestión de Seguridad de la Información – Descripción general y vocabulario:

a. Contexto externo

Entorno externo en el que la organización busca alcanzar sus objetivos

Nota 1: El contexto externo puede incluir:

- El entorno cultural, social, político, legal, reglamentario, financiero, tecnológico, económico, y ambiental; ya sea internacional, nacional, regional o local.
- Los impulsores clave y las tendencias que tienen impacto sobre los objetivos de la organización.
- Las relaciones con partes interesadas externas, sus percepciones y valores

b. Contexto interno

Entorno interno en el que la organización busca alcanzar sus objetivos

Nota 1: El contexto interno puede incluir:

- El gobierno, la estructura de la organización, las funciones y responsabilidades.
- Las políticas, los objetivos y las estrategias que se establecen para conseguirlo.
- Las capacidades, entendidas en términos de recursos y conocimientos (por ejemplo, capital, tiempo, personas, procesos, sistemas y tecnologías).
- Sistemas de información, los flujos de información y procesos de toma de decisiones (tanto formales como informales). - Las relaciones con, y las percepciones y valores de las partes interesadas internas.
- La cultura de la organización.
- Las normas, directrices y modelos adoptados por la organización.
- La forma y el alcance de las relaciones contractuales.

c. Parte interesada

Persona u organización que puede afectar, verse afectada, o percibirse a sí misma como afectada por una decisión o actividad.

d. Requisito

Necesidad o expectativa declarada, generalmente implícita u obligatoria.

NOTA: Los requisitos de las partes interesadas pueden incluir requisitos legales, regulatorios y obligaciones contractuales

e. Mapa de procesos

Interrelación de todos los procesos que realiza una organización.

f. Proceso

Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman insumos en productos ***con valor agregado***.

g. Sistema de información

Aplicaciones, servicios, activos de tecnología de información, u otros componentes de manejo de la información.

6. DEFINICION DEL ALCANCE Y LIMITES DEL SGSI

El Servicio de Administración Tributaria de Lima (SAT) determina los límites y la aplicabilidad del SGSI para establecer su alcance e identificar qué información necesita proteger.

Para ello se ha tomado en consideración los resultados del análisis de las cuestiones internas y externas identificadas en el documento "Análisis de Contexto para el Sistema de Gestión de Seguridad de la información", las necesidades y expectativas que se detallan en el documento "Requisitos de Seguridad de las partes interesadas del Sistema de Gestión de Seguridad de la información, y se han identificado las interfaces y dependencias entre las actividades desarrolladas por la institución y las de otras organizaciones.

6.1 Procesos y actividades

Al momento de definir los procesos considerados dentro del alcance del SGSI del SAT, se ha tomado en consideración el Artículo 109.3 del Reglamento de la Ley de Gobierno Digital, el cual establece lo siguiente:

"Las entidades de la Administración Pública implementan un SGSI en su institución, teniendo como alcance mínimo sus procesos misionales y aquellos que son relevantes para su operación".

En ese sentido, se han incluido dentro del alcance del SGSI del SAT, los siguientes procesos y actividades:

Cuadro N°01: Alcance del SGSI

N.º	PROCESO NIVEL 0	PROCESO NIVEL 1	ACTIVIDADES	DENOMINACIÓN PARA EL SGSI
1	***Atención al Ciudadano y Determinación de Obligaciones***	***Orientación al ciudadano***	Atender consultas de los ciudadanos por el Centro de Llamadas (telefónica, correo, chat)	Atención del Centro de Llamadas
2	Gestión de Cobranza	Cobranza Inductiva	Gestión de cobranza telefónica	
3		Recepción de pagos	Recaudación de pagos no presencial	Recaudación de pagos por canales virtuales
4	Gestión de Tecnologías de la Información	***Gestión de Desarrollo y Mantenimiento de Servicios digitales***	Implementar y administrar mecanismos de respaldo y contingencia sobre la infraestructura tecnológica crítica	Disponibilidad de los servicios virtuales

El alcance del SGSI del SAT queda definido sobre los procesos de "Atención del Centro de Llamadas, Recaudación de pagos por canales virtuales y Disponibilidad de los servicios virtuales".

El SGSI aplica a toda la información producida, manejada, y transmitida y almacenada en los procesos antes mencionados e involucra a todos los colaboradores, contratistas y terceros que tengan acceso o que estén desarrollando, adquiriendo o usando cualquier forma de los sistemas de información y/o datos relacionados con los procesos en mención.

6.2 Descripción de los procesos

Los procesos de nivel 0, ***Atención al Ciudadano y Determinación de Obligaciones***, ***Gestión de Cobranza***, y ***Gestión de Tecnologías de la Información***, son procesos misionales relacionados con la razón de ser de la entidad y sus objetivos estratégicos.
El proceso de nivel 0, Gestión de Tecnologías de la información, ha sido incluido en el alcance del SGSI considerando su relevancia en el reforzamiento de los servicios y procesos internos y la dependencia que el resto de procesos de la institución tiene sobre ellos.

6.3 Áreas involucradas

Las unidades orgánicas que tienen responsabilidad y autoridad sobre los procesos y actividades comprendidas dentro del alcance del SGSI son:

- ***Oficina de Administración y*** Finanzas
- ***Subg***erencia de Gestión de Cobranzas
- ***Subgerencia de Orientación y Registro***
- ***Oficina de Tecnologías de la Información***

Como responsable de la dirección, mantenimiento y supervisión estratégica de los planes, resultados y recursos del SGSI, también se incluye al Comité de Gobierno y Transformación Digital.

6.4 Limites

a) Ubicaciones físicas

Dentro del alcance del SGSI se consideran solo los activos de información ubicados en las siguientes locaciones del Servicio de Administración Tributaria:

- Oficina Principal del SAT, sito en Jr. Camaná 370 Lima

b) Procesos

El proceso definido dentro del alcance del SGSI: Recaudación de pagos por canales virtuales; solo considera los pagos que se reciben en bancos o se realizan por la página web del SAT.

c) Activos, servicios, sistemas de Información y aplicaciones

Para los procesos que forman parte del alcance del SGSI se manejan los siguientes activos, servicios, sistemas de información y aplicaciones relacionadas a la información:

Cuadro N°02: Matriz del alcance y relación de activos y servicios del SGSI

ID	Alcance SGSI	Actividades	Activos	Servicios	Sistemas de información y aplicaciones
1	Atención del Centro de Llamadas	Atender consultas de ciudadanos por el Centro de Llamadas	▪ Equipos de escritorio. ▪ Zoiper (SW)	• Intranet • Internet	▪ SIAT Transito ▪ SIAT Tributario

ID	Alcance SGSI	Actividades	Activos	Servicios	Sistemas de información y aplicaciones
		(telefónica, correo electrónico o chat)	▪ Anexos telefónicos ▪ Data Protector (SW) ▪ VmWare ESXI (SW) ▪ WhatsApp (SW) Veeam Backup (SW) ▪ Microsoft Excel	• Correo electrónico • Servicios de Directorio • Servicios de networking • Servicio de suministro y respaldo eléctrico para cómputo	▪ Agencia virtual (www.sat.gob.pe) ▪ SGD ▪ Call Center Asterix ▪ Marcador predictivo ▪ Sistema Cobranza WEB ▪ File Server
2		Gestionar cobranza telefónica			
3	Recaudación de pagos por canales virtuales	Recaudación de pagos no presencial.			
4	Disponibilidad de los servicios virtuales	Implementar y administrar mecanismos de respaldo y contingencia sobre la infraestructura tecnológica critica			

6.5 Interfaces y dependencias

A continuación, se identifican las interfaces y dependencias de los procesos incluidos en el alcance del SGSI con otros procesos dentro de la organización y con entidades externas:

a) Atención del Centro de Llamadas:

Cuadro N°03: Mapa de Dependencias e Interfaces – Atención de llamadas

N.º	Proceso del alcance	Dependencias externas	Interfaces externas
1	Atender consultas de los ciudadanos por el Centro de Llamadas (telefónica, correo, chat) Gestión de cobranza telefónica	1. Ciudadanos 2. Contribuyentes 3. Proveedores de telefonía 4. Entidades certificadoras	1. Internet 2. Primarios telefonía 3. Contratos y acuerdos de servicio 4. Políticas y procedimientos
		Dependencias internas	**Interfaces Internas**
		1. Subgerencia de Gestión de Cobranza 2. Oficina de Comunicaciones e Imagen Institucional 3. Oficina de Tecnologías de la Información 4. Oficina de Modernización	1. Archivo EXCEL 2. Correo electrónico 3. Sistema de Gestión de Requerimientos 4. Políticas y procedimientos

b) Recaudación de pagos por canales virtuales

Cuadro N°04: Mapa de Dependencias e Interfaces – Recaudación de pagos virtuales

N.º	Proceso del alcance	Dependencias externas	Interfaces externas
2	Recaudación de pagos no presencial	1. Notarias 2. Concesionarias 3. SUNAT, RENIEC, SUNARP 4. Ciudadanos 5. Bancos 6. MML 7. MEF	1. PIDE 2. EXTRASAT 3. ASBANC 4. Agencia Virtual 5. Convenios 6. SIAF
		Dependencias internas	**Interfaces Internas**
		1. ***Oficina de Tecnologías de la Información*** 2. ***Oficina de Administración y Finanzas***	1. Soporte 2. SIAT 3. Sistema de Gestión de requerimientos

c) Implementar y administrar mecanismos de respaldo y contingencia sobre la infraestructura tecnológica critica.

Cuadro N°04: Mapa de Dependencias e Interfaces –Implementar contingencias sobre la infraestructura

N.º	Proceso del alcance	Dependencias externas	Interfaces externas
3	Implementar y administrar mecanismos de respaldo y contingencia sobre la infraestructura tecnológica critica	1, PCM 2. Notarias 3. Concesionarias 4. SUNAT, RENIEC, SUNARP 5. Ciudadanos 6. MML 7. Bancos 8. Proveedores 9. ISP	1. Pide 2. Extrasat 3. ASBANC 4. Agencia Virtual 5. Convenios 6. Proceso Intercambio de información. 7. Contratos y acuerdos de confidencialidad 8. Acuerdos de servicio
		Dependencias internas	**Interfaces Internas**
		1. Unidades orgánicas de los servicios de TI	1. BIAs 2. Sistema de Gestión de requerimientos 3. Plan de Contingencia 4.Proc. Gestión de Incidentes

7. REVISIÓN Y ACTUALIZACIÓN

El presente documento debe ser revisado y actualizado, en caso corresponda, por lo menos una vez al año o cuando se presente una situación que lo amerite.

El Oficial de Seguridad y Confianza Digital del SAT, es el responsable de la revisión del documento y de proponer las actualizaciones o cambios que resulten pertinentes.

El alcance y los límites establecidos en el presente documento solo podrán ser modificados y/o actualizados con la aprobación de los miembros del Comité de Gobierno y Transformación Digital y del Titular de la entidad.