



**Instructivo para el control de  
ingreso y salida de personas,  
vehículos y bienes en los  
locales institucionales, áreas  
sensibles y restringidas de la  
SUNAT  
Versión 2**

**Código:**  
**A-02.4.1-IT-002**

**Oficina de Seguridad y Defensa Nacional  
Superintendencia Nacional Adjunta de Administración y Finanzas**

**Marzo 2026**

### CUADRO DE CONTROL DE CAMBIOS

N.º Item	Breve descripción del cambio	Fecha del documento	Versión	Responsable del DONI
1	Versión inicial del instructivo	08/03/2025	1	Victor Ysaías Montoya Mori – Oficina de Seguridad y Defensa Nacional
2	Incorporación del ANEXO N.º 01 Implementación y Fortalecimiento de los Mecanismos de Control para las Salidas y Reingresos de Laptops y Tablets en las Intendencias de la Aduana Marítima del Callao y la Intendencia de Aduana Aérea y Postal.	11/03/2026	2	Lorenzo Rafael Baluarte Zolezzi – Oficina de Seguridad y Defensa Nacional

## ÍNDICE

<b>SIGLAS</b> .....	<b>4</b>
<b>I. OBJETIVO</b> .....	<b>5</b>
<b>II. ALCANCE</b> .....	<b>5</b>
<b>III. BASE NORMATIVA</b> .....	<b>5</b>
<b>IV. GLOSARIO DE TÉRMINOS</b> .....	<b>6</b>
<b>V. DESCRIPCIÓN</b> .....	<b>7</b>
<b>VI. ANEXOS</b> .....	<b>26</b>

## SIGLAS

- **DGS:** División de Gestión de Servicios
- **DSST:** División de Seguridad y Salud en el Trabajo
- **INER:** Intendencia Nacional de Estrategias y Riesgos
- **INGP:** Intendencia Nacional de Gestión y Procesos
- **INRH:** Intendencia Nacional de Recursos Humanos
- **MTPE:** Ministerio de Trabajo y Promoción del Empleo
- **OCDE:** Organización para la Cooperación y el Desarrollo Económicos
- **OSDNA:** Oficina de Seguridad y Defensa Nacional
- **PNP:** Policía Nacional del Perú
- **SGSI:** Sistema de Gestión de Seguridad de la Información
- **SUCAMEC:** Superintendencia Nacional de Control de Servicios de Seguridad, Armas, Municiones y Explosivos de Uso Civil
- **SUNAFIL:** Superintendencia Nacional de Fiscalización Laboral
- **SUNAT:** Superintendencia Nacional de Aduanas y de Administración Tributaria
- **UOSA:** Unidad de Organización de Soporte Administrativo

## **I. OBJETIVO**

Controlar y facilitar los accesos de ingreso y salida de personas, vehículos y bienes en los locales institucionales, áreas sensibles y restringidas relacionadas al intercambio de información con administraciones tributarias del extranjero; y, a la bóveda de la sede San Mateo de la SUNAT, en función a las autorizaciones otorgadas y cumplimiento de labores específicas.

## **II. ALCANCE**

El presente documento es de aplicación obligatoria para todo el personal que presta servicios en la SUNAT, bajo cualquier modalidad o convenios de modalidades formativas; así como para personal de terceros (intermediación laboral, tercerización, contratistas, subcontratistas, entre otros); y, visitantes.

## **III. BASE NORMATIVA**

- 3.1. Decreto Legislativo N.º 1213 que regula los servicios de seguridad privada.
- 3.2. Ley N.º 28024, ley que regula la gestión de intereses en la administración pública.
- 3.3. Decreto Supremo N.º 021-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N.º 27806, Ley de Transparencia y Acceso a la Información Pública.
- 3.4. Decreto Supremo N.º 120-2019-PCM aprueba el Reglamento de la Ley N.º 28024, Ley que regula la gestión de intereses en la administración pública.
- 3.5. Decreto Supremo N.º 005-2023-IN, que aprueba el Reglamento del Decreto Legislativo N.º 1213, Decreto Legislativo que regula los servicios de seguridad privada.
- 3.6. Decreto Supremo N.º 040-2023-EF, que aprueba la sección primera del Reglamento de Organización y Funciones de la SUNAT, y modificatoria
- 3.7. Decreto Supremo N.º 007-2024-JUS, que aprueba el nuevo reglamento de la Ley de Transparencia y Acceso a la Información Pública.
- 3.8. Resolución de Secretaría de Integridad Pública N.º 001-2022-PCM-SIP, que aprueba la Directiva N.º 001-2022-PCM/SIP Lineamientos para asegurar la integridad y transparencia en las gestiones de intereses y otras actividades a través del Registro de Visitas en Línea y Registro de Agendas Oficiales.
- 3.9. Resolución de Secretaría de Integridad Pública N.º 004-2023-PCM/SIP, que modifica la Resolución de Secretaría de Integridad Pública N.º 001-2022-PCMSIP.
- 3.10. Resolución de Superintendencia N.º 000235-2003-SUNAT, que aprueba el Reglamento Interno de Trabajo de la SUNAT.
- 3.11. Resolución de Superintendencia N.º 000229- 2019/SUNAT y modificatorias, que aprueba la Metodología para la Formulación, Aprobación y Control de los Documentos Normativos Institucionales (METDONI) Versión 1.4 según Resolución de Oficina N.º 000001-2024-SUNAT/1V0000.
- 3.12. Resolución de Superintendencia N.º 000081-2023/SUNAT, que aprueba la sección segunda del Reglamento de Organización y Funciones de la SUNAT.
- 3.13. Resolución de Superintendencia N.º 000050-2019/SUNAT, que aprueba documentos concernientes al sistema de gestión de seguridad de la información de la SUNAT.
- 3.14. Resolución de Superintendencia N.º 000148-2023/SUNAT, que modifica los documentos referentes al sistema de gestión de seguridad de la información de la SUNAT.

- 3.15. Resolución de Superintendencia N.º 000148-2023/SUNAT que modifica los documentos referentes al Sistema de Gestión de Seguridad de la Información de la SUNAT, Anexo SGSI-MA-02-000148-2023 y Anexo SGSI-MA-03-0001482023
- 3.16. Resolución de Superintendencia N.º 00079-2024/SUNAT, que modifica la fecha de entrada en vigencia de la Resolución de Superintendencia N.º 0000812023/SUNAT.
- 3.17. Resolución de Superintendencia Nacional Adjunta de Administración Interna N.º 000103-2013-SUNAT/400000, que oficializa el Reglamento Interno de Seguridad y Salud en el Trabajo de la SUNAT.
- 3.18. Resolución de Superintendencia Nacional Adjunta de Administración y Finanzas N.º 000114-2023-SUNAT/800000, que modifica el Reglamento Interno de Trabajo de la SUNAT.
- 3.19. Resolución de Intendencia Nacional N.º 251-2022-SUNAT/8B0000, Instructivo para la Recepción y Entrega de Bienes de Alto Valor.
- 3.20. Resolución de Intendencia Nacional N.º 379-2022-SUNAT/8B0000, que aprueba Lineamiento temporal para la Gestión de Bienes Muebles Patrimoniales en la SUNAT - versión 3.
- 3.21. Resolución de Intendencia Nacional N.º 000334-2024SUNAT/8B0000 que aprueba el lineamiento temporal para la administración del servicio de transporte en la SUNAT - versión 5
- 3.22. Resolución de la Intendencia Nacional de Recursos Humanos N.º 043-2016SUNAT-8A0000, Procedimiento de Análisis de Trabajo Seguro (ATS).

#### IV. GLOSARIO DE TÉRMINOS

- 4.1. **Análisis de Trabajo Seguro:** Registro donde se identifican las actividades a realizar, los peligros y se evalúa y anota el nivel de riesgo antes del desarrollo de alguna labor o actividad; asimismo, en él se definen y establecen las medidas de control preventivas que permitan la ejecución del trabajo de forma segura.
- 4.2. **Autorización de Acceso:** Documento electrónico que emite el directivo encargado de un órgano, o unidad de organización de la SUNAT, con conocimiento de su jefe inmediato, mediante el que se autoriza el ingreso de personas, vehículos o bienes a los locales institucionales de la SUNAT.
- 4.3. **Áreas sensibles y restringidas:** Zonas exclusivas de la SUNAT<sup>1</sup>, así definidas por los funcionarios autorizados, cuyo acceso es estrictamente controlado y se efectúa con la autorización de la unidad organizacional responsable y verificación física exhaustiva en el ingreso y la salida.
- 4.4. **Armero:** Casillero con llave para la custodia de armas de fuego.
- 4.5. **Bienes:** Bienes patrimoniales y bienes de uso y consumo de la SUNAT, desechos, armas, bienes de terceros, bienes incautados, comisados, en abandono legal, embargados, a ser devueltos, rematados, adjudicados, donados, destinados o calificados para su disposición final y otros que ingresan o son retirados de los locales institucionales de la SUNAT.
- 4.6. **Centro de Control y Monitoreo:** Espacio donde los operadores monitorean datos o videos para reaccionar de manera inmediata ante alarmas, emergencias o eventos haciendo uso de sistemas de información, verificando los controles de seguridad, así como los equipos de monitoreo del sistema de video vigilancia.

<sup>1</sup> Tales como la bóveda ubicada en el sótano y el piso 13, ambos en el Edificio San Mateo, el piso 10 del Edificio Sulamérica, el piso 7 del Centro de Cómputo de San Isidro y el piso 6 de la sede Benavides.

- 4.7. **Confidencialidad:** Garantía que los datos o información se encuentran protegidos y, en ese sentido, no serán puestos a disposición ni serán revelados a personas, entidades o procesos no autorizados.
- 4.8. **Contratista:** Persona o empresa que presta servicios remunerados a la SUNAT con especificaciones, plazos y condiciones convenidos.
- 4.9. **Control de Acceso:** Control, verificación y revisión que realiza el servicio de seguridad y vigilancia en todos los accesos de los locales institucionales de la SUNAT; así como, de las áreas sensibles y restringidas.
- 4.10. **Coordinador de Seguridad:** Colaborador que pertenece a la OSDENA, responsable de las funciones operativas de seguridad en los locales institucionales de la SUNAT a su cargo.
- 4.11. **Documento de identidad:** Documento público que contiene datos de identificación personal, emitido por las autoridades públicas competentes para permitir la identificación personal, también conocido como cédula de identidad (CI), tarjeta de identidad (TI), cédula de ciudadanía (CC), documento nacional de identidad (DNI), pasaporte (P) o carné de identidad (CI), u otro según corresponda.
- 4.12. **Oficial de Seguridad y Confianza Digital:** Responsable operativo de la implementación y mantenimiento del SGSI.
- 4.13. **Pase de Acceso:** Documento impreso con características de la entidad, que el servicio de seguridad y vigilancia entrega al personal de terceros y visitas a cambio de su Documento de Identidad cuando ingrese a un local institucional, previa autorización de acceso, y que se devuelve al culminar la visita. Debe usarse en un lugar visible.
- 4.14. **Registro:** Documento físico o electrónico de la entidad que sirve como almacenamiento de datos y/o evidencia de bienes no autorizados que son retenidos durante un período de tiempo. Debe contener nombre del visitante, asunto, horarios de ingreso y de salida, contratistas, entre otros.
- 4.15. **Servicio de seguridad y vigilancia:** Servicio contratado por la SUNAT con el objetivo de salvaguardar la integridad física de las personas, instalaciones, así como dar seguridad al patrimonio y bienes bajo responsabilidad de la SUNAT.

## V. DESCRIPCIÓN

### 5.1. General

- a. Es obligación de todo el personal de la institución, sea cual fuere su modalidad de contratación o convenio de formación juvenil, conocer y cumplir con el marco legal vigente, así como de los documentos normativos institucionales o disposiciones establecidas en la entidad sobre el control de accesos, patrimonio, archivo, almacén, seguridad de la información, seguridad y salud en el trabajo y servicio de transporte.
- b. Se encuentra prohibido el acceso de personas: (i) indocumentadas, (ii) que muestren evidentes síntomas de alteración de la conciencia, (iii) que porten cualquier tipo de armas letales o no letales, (iv) explosivos o cualquier otro bien que pueda ocasionar daños; también está restringido el acceso de menores de edad, así como de personal de reparto para la entrega de productos (delivery).
- c. No se permite el ingreso de ninguna persona a los locales institucionales de la SUNAT sin que cuente con las respectivas autorizaciones, emitidas mediante documento electrónico y según las disposiciones establecidas por la entidad. A excepción de los visitantes que se dirigen a un área de atención al público.
- d. El registro de ingreso y salida es personal, y obligatorio para todas las personas que deban acceder a los locales institucionales. El control se realiza mediante el uso de: (i) fotocheck para el personal que labora en la

- SUNAT o (ii) pase para el personal de terceros, visitantes, contratistas, entre otros, el cual se debe portar en todo momento en lugar visible mientras se encuentre dentro del local institucional de modo que pueda identificarse a la persona.
- e. Todas las personas que ingresen o salgan de un local institucional deben permitir que el servicio de seguridad y vigilancia ubicado en los lugares de control de acceso efectúe el control correspondiente; asimismo, deberán mostrar el contenido de los bolsos, mochilas, maletines o cualquier otro bien que porten. En el caso de los bienes de uso personal que no cuenten con la autorización de acceso del encargado del órgano o de la unidad de organización, deberán ser guardados en los casilleros destinados para su custodia cuya llave será entregada a los propietarios de los bienes depositados.
  - f. La OSDENA y las UOSA deben gestionar los libros de control de seguridad para el registro de las personas, vehículos y bienes que se encuentren en los locales institucionales conforme al Anexo N.º 04.

## **5.2. Específicas**

### **5.2.1. Control de ingreso y salida para el personal que presta servicios en la SUNAT**

- a. Los servidores de la SUNAT deberán utilizar el reloj biométrico de control de asistencia para el registro de la marcación de su ingreso o salida de los locales institucionales, mediante el uso del fotocheck institucional o mediante el ingreso de sus datos con su huella digital. Excepcionalmente, el personal que recién ingresa a laborar en la entidad podrá efectuar el registro de ingresos y salidas mediante la lista de asistencia manual por un periodo máximo de tres (3) días consecutivos, información que será puesta en conocimiento de su jefe inmediato a fin de que éste comunique a la INRH la asistencia de esos días.
- b. El personal que presta servicios en la SUNAT no podrá ingresar a otros locales institucionales, distintos a su local de trabajo, salvo que cuenten con la debida autorización del supervisor y/o jefe de la unidad de organización a la que pertenecen o se encuentren en comisión de servicios.
- c. Podrá acceder al local institucional, el personal que, encontrándose de vacaciones, descanso médico, licencia, fuera del horario de labores o en días no laborables, en tanto cuente con la autorización de acceso emitida por el jefe de su unidad de organización. Dicha autorización debe estar dirigida al jefe de la OSDENA o al jefe de la UOSA, según corresponda, con copia al coordinador de seguridad y al Centro de Control y Monitoreo.
- d. Excepcionalmente, cuando el gobierno declare el estado de emergencia y conforme a las disposiciones que señale la INRH, debe contar con el permiso en formato físico o virtual donde indique la modalidad de trabajo según lo determinado por su jefatura para acceder al local institucional, además, debe cumplir con las normativas institucionales o disposiciones de la DSST.

### **5.2.2. Control de ingreso y salida para los visitantes**

- a. Los visitantes se identifican y registran con el servicio de seguridad y vigilancia, al cual entregan su Documento de Identidad. Están

exceptuados los visitantes que se dirigen a un área de atención al público.

- b. Se impartirá a los visitantes las instrucciones del control de acceso y de la ruta de evacuación de los locales institucionales correspondientes.
- c. Los visitantes deberán proporcionar la información necesaria para cumplir con el registro de visitas conforme se establece en el marco legal vigente para asegurar la integridad en las acciones del Estado y en las actividades de las personas que realizan actos de gestión.
- d. Los bienes del visitante que deben ingresar al local institucional para cumplir con las actividades relacionadas al desempeño de sus funciones deben ser previamente autorizados mediante correo electrónico por el jefe de la unidad de organización responsable que lo atenderá el cual debe estar dirigido al jefe de la OSDENA y, en el caso de provincias al jefe de la UOSA. Los bienes serán verificados al momento de su ingreso y retiro del local institucional por el servicio de seguridad y vigilancia.
- e. Para el ingreso a los locales institucionales, los visitantes deben contar con la autorización de acceso del encargado del órgano, unidad de organización o personal responsable a cargo quien, además, designará a un personal de su unidad para acompañarlo en todo momento durante su desplazamiento en la oficina y/o ambientes del local institucional a los que está autorizado.

Asimismo, debe portar el pase de forma visible mientras dure su permanencia en los locales institucionales y, a su salida del local, debe devolver el pase y recoger su Documento de Identidad con el servicio de seguridad y vigilancia o personal de la SUNAT, según corresponda. En caso de incumplimiento de lo señalado en el presente literal, el servicio de seguridad y vigilancia comunicará del incidente al jefe de la OSDENA o al jefe de la UOSA, según corresponda, quien notificará al jefe de la unidad de organización responsable que autorizó el ingreso.

- f. Está prohibido ingresar bienes similares que se almacenan y/o se encuentran en custodia en los Almacenes de la SUNAT.
- g. Excepcionalmente la OSDENA o la UOSA, según corresponda, comunicará al directivo que corresponda, según el caso, el ingreso del siguiente personal que no requiere autorización de acceso en el ejercicio de sus funciones:
  - Inspectores laborales del: MTPE y SUNAFIL.
  - Inspectores de SUCAMEC.
  - Inspectores de Defensa Civil (Inspecciones Técnicas de Seguridad).
  - Personal de transporte blindado de caudales autorizado por el banco quienes mantendrán el arma de fuego en su cartuchera o funda asegurada con tapa o broche.
  - Policía Nacional del Perú para las inspecciones oculares por pérdidas y robos, y otros directamente relacionados a la institución.
    - Personal del Escuadrón de Águilas Negras de la PNP.
  - Personal del Departamento de Seguridad de Bancos (DEPSEBAN).
  - Representantes del Poder Judicial, Ministerio Público y Policía Fiscal.
  - Profesionales de la salud, ambulancias, personal y vehículos del Cuerpo General de Bomberos Voluntarios del Perú.

### 5.2.3. Control de ingreso y salida para el personal de terceros (intermediación laboral, tercerización, contratistas, subcontratistas, entre otros)

- a. Cumplir con las normas vigentes de Seguridad y Salud en el Trabajo.
- b. Cumplir con lo estipulado en las cláusulas incluidas en el documento contractual que está referida a salvaguardar la confidencialidad e integridad de la información de la institución.

Unidad de organización	Responsable	Disposiciones
---	Personal de terceros autorizado por la empresa	<ol style="list-style-type: none"> <li>a. Debe identificarse y entregar al servicio de seguridad y vigilancia su Documento de Identidad en los lugares de control de acceso.</li> <li>b. Verificada su identificación con la autorización de acceso y comunicado a la unidad de organización responsable que lo autorizó, se permite el ingreso con la indicación que debe portar el pase de forma visible mientras dure su permanencia en el local institucional.</li> <li>c. Permitir la revisión exhaustiva de los bienes que porte, al personal de vigilancia ubicado en los lugares de control de acceso. Los bienes autorizados para la realización de la ejecución de los trabajos a realizar deben ser registrados de acuerdo con el Anexo 01 Acta de Inventario de Bienes del Contratista.</li> <li>d. Permitir que el servicio de seguridad y vigilancia controle y verifique al ingreso del local institucional y antes de iniciar su trabajo, cuando corresponda, la documentación siguiente:               <ul style="list-style-type: none"> <li>- Seguro Complementario de Trabajo de Riesgo – SCTR vigente.</li> <li>- Análisis de Trabajo Seguro – ATS, el cual debe estar validado por la DSST.</li> <li>- Constancia vigente de haber aprobado el curso de inducción y seguridad impartido por la DSST, información actualizada diariamente por el Centro de Control y Monitoreo.</li> </ul> </li> <li>e. Usar el vestuario de trabajo y el fotocheck de identificación de forma visible de su empresa, según lo especifique el contrato u orden de compra/servicio y lo establecido en la norma de seguridad y salud en el trabajo.</li> <li>f. Realizar el trabajo dentro de las zonas establecidas o autorizadas; reportando oportunamente las incidencias detectadas respecto a daños a los bienes patrimoniales, bienes de terceros, e instalaciones de la SUNAT; así como, eventos que puedan comprometer la seguridad de la información.</li> </ol>

		<p>g. Facilitar su registro corporal cada vez que ingrese o se retire del local institucional mediante el detector de metal y/o revisión corporal.</p> <p>h. No ingresar o retirar bienes patrimoniales sin la respectiva Guías de Remisión Electrónica (GRE) Remitente y Transportista conforme a la normativa vigente. De igual forma no ingresar o retirar bienes personales no declarados.</p> <p>i. En los Almacenes de la SUNAT, ingresar únicamente con el vestuario y bienes necesarios para la realización de su trabajo quedando prohibido el ingreso de cualquier otro bien como relojes, joyas, billeteras, celulares, dispositivos electrónicos, maletines, entre otros. Excepto que cuenten con la autorización detallada de los bienes que pueden ingresar y justificación mediante documento electrónico para su ingreso por parte de la jefe o supervisor de la unidad organizacional responsable del almacén.</p>
División de Seguridad y Salud en el Trabajo	Persona asignada por el jefe de la DSST	<p>a. Solicitar y verificar los documentos necesarios de Seguridad y Salud en el Trabajo antes del acceso al local institucional, según las normativas de la DSST.</p> <p>b. Comunicar a las unidades de organización responsables que corresponda los enlaces de los cursos de inducción del personal de terceros.</p> <p>c. Verificar y revisar los ATS antes del ingreso al local institucional.</p>
OSDNA UOSA	Coordinador de seguridad <sup>2</sup>	<p>a. Verificar que las personas que accedan a las áreas sensibles y restringidas no ingresen con ningún bien, salvo lo autorizado expresamente mediante correo electrónico por la unidad de organización responsable para su ingreso.</p> <p>b. Verificar la salida de los bienes muebles patrimoniales y constatar que los datos consignados en el formato: Orden de Salida, Reingreso y Desplazamiento Interno de Bienes Muebles Patrimoniales correspondan al bien mueble patrimonial que está siendo desplazado.</p> <p>c. En caso se detecte la posesión de bienes patrimoniales o bienes no autorizados, se procede a efectuar la inmovilización del bien y redactar el "Acta de Retención" de acuerdo con el ANEXO 02 informando al encargado del local institucional, al jefe de</p>

<sup>2</sup> Para todos los casos, el coordinador de seguridad verifica el cumplimiento mediante el contrato del servicio de seguridad y vigilancia

		la OSDENA o UOSA, según corresponda; en el caso del departamento de Lima, dicha comunicación se remite con copia al Centro de Control y Monitoreo.
--	--	--

#### 5.2.4. Control de ingreso y salida vehicular

- a. La DGS otorga la autorización para el uso de los vehículos de la entidad; asimismo, dispone la asignación de los estacionamientos existentes en los locales institucionales, el cual debe comunicar a la OSDENA para su control; en las otras jurisdicciones, las autorizaciones de los estacionamientos están a cargo de la UOSA.
- b. Sólo ingresarán a las áreas de estacionamiento, los vehículos autorizados. El conductor, de ser requerido por el servicio de seguridad y vigilancia deberá exhibir el documento de identidad, la licencia de conducir así como los documentos del vehículo.
- c. Los datos del conductor y del vehículo deben quedar registrados en el libro de control de ingreso y salida vehicular y/o en el sistema con que cuente el local institucional.
- d. Todo personal que conduzca el vehículo debe:
  - Detenerse al ingreso y salida del área de estacionamiento para el control respectivo por el servicio de seguridad y vigilancia.
  - Permitir la revisión del vehículo (salón y maletera) al ingreso y salida del área de estacionamiento. En caso que el vehículo tuviera lunas oscurecidas, deberá bajar la ventana del lado del conductor y encender la luz de salón.

Unidad de organización	Responsable	Disposiciones para el registro de salida e ingreso de vehículos
Todas las UUOO	Conductor de la SUNAT	<ol style="list-style-type: none"> <li>a. El ingreso y salida vehicular en un local institucional se efectuará con la respectiva Autorización de Acceso y anotarse en el registro de Accesos Vehiculares SUNAT.</li> <li>b. Efectuar la verificación del estado físico de conservación del vehículo, cuando salga y retorne de una comisión, debiendo reportar en el mismo día la ocurrencia al servicio de seguridad y vigilancia y al encargado de la administración de la flota vehicular cualquier situación contraria estará sujeto a la responsabilidad que corresponda asumir en caso de detectarse alguna incidencia.</li> <li>c. Al término de cada jornada laboral, las llaves de todas las unidades vehiculares de la SUNAT deben quedar en un organizador de llaves (llaveteca), bajo custodia del servicio de Seguridad y Vigilancia o por el responsable designado por el directivo a cargo de la DGS y la UOSA según corresponda.</li> </ol>
OSDENNA	Coordinador de seguridad	<ol style="list-style-type: none"> <li>a. Registrar los datos contenidos en el formato de la papeleta de autorización de salida de vehículos, que debe proporcionar el conductor.</li> </ol>

		<ul style="list-style-type: none"> <li>b. Los controles y registros necesarios para el ingreso de los vehículos a los diferentes locales de la institución están a cargo del servicio de seguridad y vigilancia, sujetándose al contenido del formato para la autorización de salida de vehículos en el que se registra, entre otros, el kilometraje de salida - retorno, destino de la comisión, nombre y registro del colaborador que conduce y datos del comisionado, entre otros.</li> <li>c. Antes de la comisión del servicio, si el conductor de un vehículo de la institución muestra indicios de no encontrarse en condiciones adecuadas para manejar, de inmediato el servicio de seguridad y vigilancia informará por correo institucional al jefe que autorizó la salida del comisionado para que adopte las medidas correspondientes con observancia al Reglamento Interno de Trabajo; igualmente al directivo a cargo de la DGS en Lima y Callao o de la UOSA correspondiente.</li> <li>d. Comunicar al directivo a cargo de la DGS en Lima y Callao o de la UOSA, correspondiente, en caso falten algunas de las llaves de los vehículos que pernoctan en el local institucional; y en caso de detectarse una incidencia, debe formular el informe respectivo.</li> </ul>
<p>Personal que presta servicios en la SUNAT</p> <p>Personal de terceros</p> <p>Visitantes</p>	<p>Conductor</p>	<ul style="list-style-type: none"> <li>a. Los vehículos particulares sólo podrán ingresar o salir del área de estacionamiento con el conductor autorizado. Los acompañantes harán su ingreso por los controles de acceso.</li> <li>b. La DGS o la UOSA, según corresponda, emitirá y entregará la tarjeta pase de estacionamiento que acredite la autorización del colaborador para el aparcamiento de su vehículo; en el caso del personal de terceros las autorizaciones las otorgaran siempre que se cuente con disponibilidad en la playa de estacionamiento.</li> <li>c. Los estacionamientos sólo podrán utilizarse durante el tiempo que el conductor y/o pasajero permanezcan en el local institucional, estando prohibido que vehículos no autorizados pernocten en las instalaciones de la SUNAT.</li> <li>d. La permanencia del vehículo en el interior del local institucional es autorizada por la jefatura de la División de Gestión de Servicios; en provincia es autorizada por el jefe de la UOSA o encargado del local.</li> <li>e. Permitir el control y verificación del servicio de seguridad y vigilancia para el ingreso y</li> </ul>

		<p>salida del vehículo por medio de las siguientes actividades:</p> <ul style="list-style-type: none"> <li>- Registrar el ingreso y salida en el libro de Accesos Vehiculares Particulares y/o sistema que cuenta el local institucional con los datos del vehículo, conductor, seguros licencias, autorizaciones, fecha, hora, empresa a la que pertenece, trabajo a realizar o motivo de su ingreso.</li> <li>- Verificar las Guías de Remisión Electrónica (GRE) Remitente y Transportista de la carga o material que ingresa o sale del local institucional.</li> <li>- Revisar la maleta del vehículo, la parte exterior y chasis de los vehículos utilizando los espejos tipo "L", detectando posibles objetos ocultos que representen un peligro.</li> <li>- Vigilar que los vehículos al interior del local institucional se desplacen a una velocidad máxima de 10 kilómetros por hora.</li> </ul>
--	--	---

#### 5.2.5. Control de ingreso y salida de armas de fuego

- a. El portador de armas de fuego debe descargar las municiones y depositarlas en el casillero que le asigne el servicio de seguridad y vigilancia, quien le entregará la llave correspondiente. El arma y las municiones que quedaron bajo custodia, serán devueltas al momento de su retiro del local institucional.
- b. La custodia temporal de las armas no excederá de la fecha de visita, en el caso contrario el servicio de seguridad y vigilancia debe reportarlo al jefe de la OSDENA en el departamento de Lima, en provincias se comunicará al jefe de la UOSA.
- c. En los casos en que el portador del arma no la declare o se niegue a dejarla en custodia, no ingresa al local institucional.
- d. El personal de las Fuerzas Armadas, Policía Nacional del Perú y de transporte blindado de caudales, que se encuentren en cumplimiento de su función, se encuentra exceptuado del presente control de acceso.

#### 5.2.6. Control de ingreso y salida para el movimiento de bienes patrimoniales y bienes de terceros en custodia de la SUNAT

El jefe o supervisor de las unidades de organización responsables que directamente deban autorizar el movimiento de bienes patrimoniales y/o bienes de terceros en custodia de la entidad, mediante documento electrónico comunicarán dicha autorización a la OSDENA o la UOSA, según corresponda, con el detalle siguiente:

- Relación de los bienes que ingresarán o saldrán de los locales institucionales, los que deben contar con la documentación y datos correspondientes, así como, los datos del vehículo de traslado y la guía correspondiente.
- Relación del personal que brinda servicios en la SUNAT y/o personal de terceros y/o visita con los datos completos para su registro, así como de la documentación que deben presentar para el control de acceso.

- Relación de los bienes personales que pueden ingresar al local institucional para cumplir con las funciones o actividades a realizar.

Unidad de organización	Responsable	Disposiciones para el movimiento de bienes
División de Gestión Patrimonial	Jefe	<ul style="list-style-type: none"> <li>a. Disponer los trámites de alta y baja de los bienes patrimoniales, así como la actualización de estos en los sistemas.</li> <li>b. En el caso de los bienes que no están codificados, la autorización de movimiento es firmada únicamente por el jefe de la unidad de Control Patrimonial o el jefe de la UOSA, según corresponda.</li> <li>c. En el caso de inventario físico, el Jefe de la División de Gestión Patrimonial o Jefes de las UOSA, enviarán a la OSDENA copia de la Resolución de Conformación de la Comisión de Inventario y/o de la relación del personal contratado para la toma de inventario indicando el nombre de la empresa que brinda el servicio.</li> <li>d. Durante el inventario físico de los bienes patrimoniales, queda prohibido el movimiento de bienes interno o externo del local institucional, con excepción de los que se encuentran autorizados por el jefe de la unidad de Control Patrimonial o jefe de la UOSA, según corresponda, dichas autorizaciones deben ser comunicadas al presidente de la comisión de inventarios indicando los datos de los bienes involucrados para su posterior inventario físico, registro y control correspondiente.</li> </ul>
División de Almacenes  División de Disposición de Bienes y Mercancías  División de Almacén de Bienes de Uso Consumo y Mobiliario	Jefe de División  Supervisor	<ul style="list-style-type: none"> <li>a. Realizar las acciones que corresponde en el marco normativo vinculadas para el ingreso, custodia y/o salida de los bienes a su cargo.</li> <li>b. Elaborar y remitir la documentación que corresponda, según la normativa vigente, a las unidades organizacionales para el movimiento de ingreso o salida de los bienes a su cargo.</li> <li>c. Supervisar las acciones del inventario de los bienes de la SUNAT y de los bienes de terceros en custodia, según corresponda.</li> </ul>
Todas las UUOO	Colaborador  Jefe inmediato  Jefe de la UOSA  Jefe de la OSDENA  Gerente	<p><b>Computadoras portátiles</b></p> <ul style="list-style-type: none"> <li>a. La salida temporal de las computadoras portátiles de propiedad de la institución, se encuentran autorizadas para el personal que trabaja en la SUNAT como personal con modalidad de teletrabajo, auditores de campo, fiscalizadores de aduanas, ejecutores coactivos, supervisores, personal directivo y los asesores de la Alta Dirección.</li> <li>b. Para el personal que presta servicios en la SUNAT y no se encuentre en el texto anterior,</li> </ul>

	<p>Intendente</p> <p>Personal que presta servicios en la SUNAT</p>	<p>sólo se permite la salida temporal de las computadoras portátiles personales de propiedad de la institución, si cuenta con:</p> <ul style="list-style-type: none"> <li>- La etiqueta del código patrimonial, para que se pueda registrar su salida e ingreso.</li> <li>- La autorización del jefe inmediato superior mediante documento electrónico dirigido al Jefe de la OSDENA o UOSA, según corresponda, indicando el detalle del período por el cual se autoriza la salida.</li> </ul> <p>c. Está prohibido el ingreso de computadoras portátiles personales, de propiedad de los servidores o de terceros, a los locales institucionales. Por excepción, sólo el Intendente o Gerente inmediato de la unidad organizacional, mediante documento electrónico dirigido al jefe de la OSDENA o de la UOSA, según corresponda, podrá autorizar temporalmente el ingreso de accesorios o equipos informáticos. En estos casos, la responsabilidad de la custodia del bien está a cargo exclusivamente del colaborador que figure en la comunicación de autorización.</p>
<p>OSDEN A</p> <p>UOSA</p>	<p>Coordinador de seguridad</p>	<p>a. Registrar el ingreso y salida de bienes en el Libro de Control de Movimiento de Bienes Patrimoniales o en el aplicativo informático "Registro de Bienes Patrimoniales", anotando entre otros, los datos requeridos como son el número del Registro del trabajador y los números del código patrimonial de los bienes, en atención a los documentos de autorización que sustentan dicho movimiento.</p> <p>b. Verificar que la información consignada en los documentos como: Guías de Remisión Electrónica (GRE) Remitente y Transportista, Orden de Salida, Reingreso y desplazamiento Interno contenga las mismas características del bien, señalando la fecha y hora del ingreso y/o salida del bien. Es responsable de los bienes patrimoniales hasta su retorno, el personal que presta servicios en la unidad organizacional Técnica que dispuso la reparación y/o mantenimiento, o el personal que presta servicios en la unidad de organización que dispuso el desplazamiento interno o externo del bien.</p> <p>c. Las incidencias ocurridas en el control de acceso son reportadas al jefe de la OSDENA, al jefe de la UOSA o al encargado del local institucional, según corresponda.</p> <p><b>Movimiento bienes patrimoniales</b></p> <p>a. Se efectúa a través de las Guías de Remisión Electrónica (GRE) Remitente y Transportista y comprende bienes que cuentan adherida la</p>

		<p>etiqueta de código patrimonial y sobre los que se dispone su traslado por:</p> <ul style="list-style-type: none"><li>- Devoluciones</li><li>- Transferencias</li><li>- Mudanzas</li><li>- Salidas Temporales.</li></ul> <p>b. Verificar que las Guías de Remisión Electrónica (GRE) Remitente y Transportista:</p> <ul style="list-style-type: none"><li>- Se encuentren impresas por el sistema informático, puede contar con los sellos y firmas de las personas que autorizan el traslado, no se acepta como válido el documento total o parcialmente que contenga información errada, incompleta o con enmendaduras.</li><li>- Mantenga coincidencia entre el detalle de bienes y los códigos, series, modelos, colores y demás características de fabricación de los bienes patrimoniales que son materia de algún tipo de movimiento.</li></ul> <p><b>Movimiento bienes de uso y consumo:</b></p> <p>a. Se efectúa a través de una Orden de Salida, Guías de Remisión Electrónica (GRE) Remitente y Transportista u otros documentos mediante los cuales se controla y verifica que:</p> <ul style="list-style-type: none"><li>- Esté confeccionada utilizando el sistema informático.</li><li>- Esté firmada por el funcionario responsable que autoriza el movimiento de bienes de uso y consumo.</li><li>- Que la información consignada sea la correcta y completa, sin errores ni enmendaduras.</li><li>- Exista coincidencia entre el detalle de bienes que son materia de algún tipo de movimiento.</li></ul> <p>b. Concluida la acción de control y verificación, el servicio de seguridad y vigilancia procederá a firmar y anotar su nombre y apellido, la hora y fecha de control, en la respectiva Guía de Remisión u Orden de Salida. De ser el caso, anota las incidencias que se hubieren detectado en el original y la copia de la Guía de Remisión u Orden de Salida y las reporta oportunamente.</p> <p><b>Movimiento de mercancías y bienes de terceros</b></p> <p>a. Deben contar con las actas respectivas para salida o ingreso al almacén, controlando documentariamente que su contenido corresponda a lo detallado en las actas.</p> <p>b. El retiro de bienes o mercancías por efecto de donaciones o adjudicaciones procede ante la presentación de la correspondiente</p>
--	--	--

		<p>Resolución o actas de entrega emitidas por las áreas correspondientes, documento sobre el cual se ejecuta la acción de control.</p> <p>c. Cuando las mercancías se encuentren lacradas o selladas por cadena de custodia dispuesta por la autoridad competente, se procede a tomar nota del número de custodia o Acta, haciendo la observación que no se ha revisado el contenido, ya que no deben ser deslacradas o abiertas de sus contenedores sin autorización de los fiscales que las ingresan.</p> <p>d. Llevar el control cronológico y adecuado de las autorizaciones de ingreso, salida y desplazamientos para su fácil ubicación, debiendo anotar en el Libro de Control de Ocurrencias el ingreso, salida y desplazamiento de los bienes.</p> <p><b>Movimiento de bienes en los almacenes</b></p> <p>a. En el ingreso de bienes incautados, comisados, en abandono legal o embargados, el servicio de seguridad y vigilancia realiza:</p> <ul style="list-style-type: none"><li>- El registro de acceso de todas las personas que intervienen en dicho proceso.</li><li>- Solicita una copia del documento de recepción de los bienes.</li></ul> <p>b. En el caso del movimiento de insumos químicos o mercancías peligrosas, el servicio de seguridad y vigilancia comunica al responsable del almacén que se han presentado para su ingreso dichos insumos o mercancías, para proceder con su almacenamiento de acuerdo con lo señalado en su ficha de seguridad.</p> <p>c. En la salida de bienes a ser devueltos, rematados, adjudicados, donados o calificados para su disposición final, el servicio de seguridad y vigilancia controla su salida del almacén, verificando que estos correspondan a la descripción detallada en el Acta de Salida. Asimismo, efectúa el Registro de Acceso de las personas que intervienen en dicho proceso y del documento mediante el cual se autoriza la salida de bienes, obteniendo una copia de dicho documento.</p> <p>d. Cuando los bienes a ser ingresados al almacén se encuentran lacrados o sellados por cadena de custodia dispuesta por la autoridad competente, se efectúa el Registro de Acceso de las personas que intervienen y del documento en el cual se indica el lacrado o sellado de los bienes, precisando que el contenido no ha sido revisado.</p> <p>e. Cuando los bienes a ser ingresados al almacén, por su cantidad o volumen no</p>
--	--	---

		<p>pueden ser contabilizados a detalle, se efectúa el Registro de Acceso de las personas que intervienen y del documento, precisando que el contenido no ha sido contabilizado a detalle.</p> <p>f. Cuando los bienes a ser ingresados al almacén son de alto valor, se coordina su internamiento en bóveda considerando las disposiciones y protocolos de seguridad establecidos para su ingreso a este ambiente y se efectúa el Registro de Acceso de las personas que intervienen y del documento que sustenta el ingreso.</p> <p><b>Movimiento de bienes considerados como desechos o material reciclable</b></p> <p>a. La unidad de organización responsable de la supervisión de la remodelación o construcción de nuevos locales institucionales, así como de la instalación de equipos o muebles, mediante documento electrónico, comunica al jefe de la OSDENA o al jefe de la UOSA, según corresponda, su autorización para el retiro de desechos o material reciclable como escombros, envases o material de embalaje, restos de madera, restos de vidrio, entre otros; esta comunicación se enviará con copia al servicio de seguridad y vigilancia. Dicha autorización contiene la relación de los desechos que se retirarán, así como el nombre, apellido y número de Documento de Identidad de la persona que efectuará el retiro de los desechos, acompañantes y placa de rodaje del vehículo.</p> <p>b. Verificar y controlar el retiro de los desechos o material reciclable conforme a la relación remitida en el documento electrónico de autorización.</p>
--	--	---

**5.2.7. Control de ingreso y salida para el movimiento de bienes particulares del personal que presta servicios en la SUNAT**

- a. Todos los bienes que sean absolutamente necesarios y aplicables a la ergonomía en la seguridad y salud en el trabajo, y que la entidad no pueda atender de manera inmediata, previa coordinación con la DSST, pueden ingresar al local institucional con los siguientes requisitos:
- El jefe inmediato lo autorice, mediante documento electrónico dirigido al jefe de la OSDENA o USA, según corresponda, con el detalle de la marca, modelo, serie e imagen del bien.
  - Garantía comercial o póliza de seguro del bien que proporcione seguridad económica y protección ante cualquier eventualidad o siniestro que sufra el bien asegurado, como generar una sobre carga eléctrica.

- Declaración jurada del personal que presta servicios en la SUNAT, en la que asume la responsabilidad de custodiar el bien de su propiedad, liberando de cualquier responsabilidad a la entidad y al personal de terceros que tengan un vínculo contractual con la institución, por no ser parte de sus funciones.

Debe quedar registrado el ingreso y salida de los bienes particulares del personal que presta servicios en la SUNAT, junto con una copia de toda la documentación mencionada en el control de accesos del local institucional.

- b. Durante el inventario patrimonial, debe presentar la documentación mencionada en el párrafo anterior al encargado de inventariar para que no sea considerado como un excedente de los bienes de la SUNAT.

#### **5.2.8. Control de ingreso y salida en las áreas sensibles y restringidas relacionadas al intercambio de información con administraciones tributarias del extranjero.**

- a. El jefe de la OSDENA es el responsable directo de la seguridad de las áreas sensibles y restringidas de SUNAT<sup>3</sup>, por lo que debe emitir las disposiciones de seguridad necesarias para el control de acceso y resguardo del personal y bienes de las áreas sensibles y restringidas. Asimismo, debe informar a la Alta Dirección cuando los colaboradores, incluyendo al personal directivo, no cumplan o trasgredan las medidas de seguridad y las normas impuestas en el instructivo correspondiente.
- b. El nivel de seguridad establecido para las áreas sensibles y restringidas es calificado de extremo, conforme a la Resolución de Superintendencia N.º 050-2019/SUNAT, metodología de gestión de riesgos de seguridad de la información SGSI-ME-01.
- c. El acceso físico a las áreas sensibles y restringidas se encuentra prohibido, con excepción del personal de la SUNAT debidamente autorizado y asignado al área funcional, así como del personal institucional o externo autorizado por el directivo del área sensible y restringida mediante documento electrónico.
- d. Están prohibidas las reuniones de trabajo con personal de otras unidades de organización de la SUNAT o con consultores externos en el interior de estas oficinas, excepto cuando el Intendente de la INER, mediante documento electrónico dirigido al jefe de la OSDENA comunique la realización de una reunión extraordinaria. En dicho documento se debe detallar los datos de los participantes, día, hora y cualquier otra precisión que sea necesaria según los requerimientos de seguridad establecidos.
- e. Al término de las labores diarias, los documentos oficiales y dispositivos de almacenamiento magnético quedarán guardados bajo llave en los armarios o escritorios designados por el directivo del área sensible y restringida.
- f. Todo movimiento de bienes patrimoniales es autorizado previamente por el directivo encargado del área sensible y restringida en coordinación con el jefe de la OSDENA.
- g. El personal de los servicios de soporte interno o externo ingresará con la autorización del directivo encargado del área sensible y restringida,

<sup>3</sup> Piso 13 en el Edificio San Mateo, el piso 10 del Edificio Sulamérica, el piso 7 del Centro de Cómputo de San Isidro y el piso 6 de la sede Benavides.

en coordinación con el jefe de la OSDENA de acuerdo con los documentos normativos institucionales de seguridad.

- h. El personal involucrado en el presente instructivo de seguridad tiene la obligación de mantener el cumplimiento de la confidencialidad de la información referida a las labores que realiza en la institución y cumplir con los documentos normativos institucionales de seguridad.
- i. Está prohibido el ingreso y uso de los equipos celulares en el interior de las áreas sensibles y restringidas.

Solo el Intendente y los colaboradores que éste designe mediante documento electrónico, podrán hacer uso del celular institucional para el cumplimiento de sus funciones, decisión que será comunicada al Oficial de Seguridad y Confianza Digital y al jefe de la OSDENA. Dichos equipos podrán ser requeridos para inspecciones técnicas y control cuando así lo requiera el Oficial de Seguridad y Confianza Digital.

Unidad de organización	Responsable	Disposiciones
OSDNA	<p>Jefe</p> <p>Supervisor</p>	<ul style="list-style-type: none"> <li>a. Revisar los documentos electrónicos remitidos por los directivos a cargo de las áreas sensibles y restringidas donde comunica las autorizaciones de acceso de alta y baja, a fin de disponer a seguridad electrónica y al servicio de seguridad y vigilancia las acciones a realizar que les corresponde para cada caso.</li> <li>b. Efectuar tres veces al año las inspecciones que le corresponde a la OSDENA en las áreas sensibles y restringidas con la finalidad de actualizar y minimizar los riesgos.</li> <li>c. Realizar inspecciones de seguridad inopinadas a todas las áreas sensibles y restringidas sin previo aviso a fin de constatar que las medidas de seguridad impuestas se desarrollen según las normativas vigentes.</li> <li>d. Gestionar para las áreas sensibles y restringidas la implementación de: <ul style="list-style-type: none"> <li>- Sistemas de seguridad electrónica como: detección y alarma contra incendio, control de acceso, cámaras de video vigilancia.</li> <li>- Servicio de seguridad y vigilancia con el equipamiento que corresponda.</li> </ul> </li> <li>e. Disponer el control y supervisión de los sistemas de seguridad electrónica y del servicio de seguridad y vigilancia implementados en las áreas sensibles y restringidas.</li> <li>f. Requerir a los directivos que administran los contratos del servicio de limpieza y del servicio de seguridad y vigilancia los antecedentes penales, judiciales o certificado unico laboral del personal que labora dentro de las áreas sensibles y restringidas.</li> </ul>

		<p>g. Disponer la retroalimentación a todo el personal involucrado en las áreas sensibles y restringidas sobre las medidas de seguridad en forma semestral y cuando la situación lo amerite.</p> <p>h. Ejecutar las acciones de mitigación del riesgo mediante la capacitación y simulacros según el Plan de Seguridad y posteriores actualizaciones de este documento.</p>
<p>OSDNA</p>	<p>Supervisor</p> <p>Operador</p> <p>Coordinador de seguridad</p>	<p>El supervisor debe comprobar la ejecución de las disposiciones del personal a su cargo.</p> <p><b>CENTRO DE CONTROL Y MONITOREO</b> El operador del centro de control y monitoreo debe:</p> <p>a. Monitorear los sistemas de seguridad electrónica; en caso de observar alguna irregularidad, comunicar directamente al jefe de la OSDENA y registrar en el libro de ocurrencias.</p> <p>b. Efectuar las coordinaciones con seguridad electrónica para la autenticación biométrica del nuevo personal autorizado para ingresar a las áreas sensibles y restringidas, por el tiempo que indiquen los directivos encargados de las áreas sensibles y restringidas.</p> <p>c. Abrir de forma remota las puertas de acceso de las áreas sensibles y restringidas cuando el jefe de la OSDENA lo autoriza.</p> <p>d. Realizar el monitoreo aleatorio de imágenes referidas al cumplimiento de los controles de seguridad que se realizan en las áreas sensibles y restringidas, el mismo que debe comunicarse a la jefatura de la OSDENA en el Parte Diario.</p> <p><b>SEGURIDAD Y VIGILANCIA</b> El coordinador de seguridad mediante el contrato del servicio de seguridad y vigilancia debe:</p> <p>a. Verificar y registrar el ingreso y salida de los trabajadores asignados al área restringida y sensible.</p> <p>b. Emplear el detector de metales para el control de acceso al personal de terceros que accede a las áreas sensibles y restringidas.</p> <p>c. Denegar el acceso de ingreso por las escaleras de evacuación. Sólo en caso de emergencia pueden usar las escaleras de evacuación para salir.</p> <p>d. Negar el acceso a visitas y al personal no</p>

		<p>autorizado, registrando la ocurrencia y comunicando al jefe de la OSDENA con copia al Centro de Control y Monitoreo de los intentos detectados.</p> <ul style="list-style-type: none"><li>e. Acompañar al personal de terceros mientras que duren los trabajos a realizar, previa autorización del directivo encargado de las áreas sensibles y restringidas.</li><li>f. Permanecer en las áreas sensibles y restringidas sólo cuando los colaboradores se encuentran laborando. Cuando la totalidad de estos se retire, las áreas sensibles y restringidas quedarán bajo el control de los sistemas de seguridad electrónica.</li><li>g. Cumplir con mantener la confidencialidad de las actividades que se desarrollan al interior de las áreas sensibles y restringidas.</li><li>h. Verificar que las puertas de acceso a las áreas sensibles y restringidas se encuentren debidamente cerradas a fin de que el sistema de control de acceso funcione con normalidad.</li><li>i. Controlar el acceso del personal asignado para realizar la limpieza de las áreas sensibles y restringidas.</li></ul> <p><b>En el Centro de Cómputo</b></p> <ul style="list-style-type: none"><li>a. Verificar la autorización de acceso a la llegada del proveedor, donde se confirme la realización de trabajos dentro del Centro de Cómputo. Dicha autorización, en la que se especifica los trabajos a realizar y el tiempo estimado de la labor, debe ser emitida por los Supervisores de la División de Soporte y Operación de la Infraestructura Tecnológica o personal encargado en reemplazo, con copia al Coordinador de Seguridad y jefe de la OSDENA.</li><li>b. Verificar la identidad de cada persona y que cuente con su respectivo SCTR al día, equipos de protección personal (EPP), herramientas y materiales que ingresarán.</li><li>c. Comunicar a los supervisores de la División de Soporte y Operación de la Infraestructura Tecnológica, según corresponda, de la presencia de la(s) persona(s) que ingresarán al Centro de Computo para que él designe al personal a su cargo que lo acompañará al Centro de Cómputo.</li><li>d. Sólo cuando el supervisor de División de Soporte y Operación de la Infraestructura Tecnológica confirme que puede ingresar con todos sus materiales y herramientas y en tanto esté el personal de</li></ul>
--	--	---

		<p>acompañamiento, se le permitirá el paso otorgándole el respectivo pase de proveedor.</p> <p>e. Todas las personas que ingresan al Centro de Cómputo deben llenar sus datos en el "Registro de Ingreso" que se encuentra en el interior del Centro de Cómputo.</p> <p>f. El personal que realizará trabajos en el Centro de Computo debe estar acompañado, en todo momento, por el personal de División de Soporte y Operación de la Infraestructura Tecnológica hasta que se retire del edificio.</p> <p>g. Recibir la confirmación del supervisor de la División de Soporte y Operación de la Infraestructura Tecnológica que los servicios y trabajos se realizaron sin novedad.</p> <p>h. Verificar que el personal de limpieza sea el autorizado por la División de Servicios Generales y la OSDENA</p> <p>i. Revisar el contenido de las bolsas de residuos sólidos, que diariamente retire el personal de limpieza.</p> <p>j. Controlar el movimiento de bienes patrimoniales verificando que se encuentre autorizado por la directivo del área sensible y restringida, y del jefe de la OSDENA mediante la documentación respectiva.</p> <p>k. Comunicar en forma oportuna al supervisor y coordinador de seguridad la ocurrencia o incumplimiento de los normas y disposiciones de seguridad.</p>
División de Soporte y Operación de la Infraestructura Tecnológica	Supervisor	<p>a. Para el acceso a los Centros de Cómputo de la SUNAT se deben seguir las normas y disposiciones vigentes para mantener la seguridad física, ambiental y de la información.</p> <p>b. Supervisar las labores específicas del personal externo cuyo ingreso al Centro de Cómputo fue debidamente autorizado.</p> <p>c. Verificar y controlar el ingreso, salida y permanencia de los servidores de la entidad y del personal externo, autorizados a ingresar al Centro de Cómputo, quienes deberán portar en un lugar visible el fotocheck institucional o pase de acceso otorgado.</p>
INSI INER	Directivos encargados de las áreas sensibles y restringidas	<p>a. Es el responsable que los trabajadores a su cargo cumplan con los documentos normativos institucionales de seguridad y las disposiciones emitidas por la OSDENA.</p>

INGP <sup>4</sup>		<ul style="list-style-type: none"> <li>b. Actualizar mensualmente la lista que comprenda a todos los trabajadores autorizados para acceder a estas áreas.</li> <li>c. Coordinar y comunicar al jefe de la OSDENA la autorización de acceso para el personal de terceros conforme a las normativas de seguridad establecidas.</li> <li>d. Delegar la responsabilidad de autorizar el acceso al funcionario que designe para tal fin, lo que comunicará previamente al jefe de la OSDENA por documento electrónico con la indicación del periodo de dicho encargo.</li> <li>e. Coordinar con el jefe de la OSDENA las mejoras en los documentos normativos y disposiciones de seguridad en las oficinas clasificadas como áreas sensibles y restringidas.</li> <li>f. Solicitar a la OSDENA que brinde retroalimentación a todo el personal involucrado en las áreas sensibles y restringidas sobre las medidas de seguridad. Dicha retroalimentación se efectuará semestralmente y cuando lo estimen necesario.</li> <li>g. Gestionar ante la OSDENA, mediante memorándum, el enrolamiento de iris y de la huella dactilar para el control de acceso de los trabajadores autorizados a ingresar a las áreas sensibles y restringidas.</li> </ul>
<p>INSI</p> <p>INER</p> <p>INGP</p>	<p>Colaboradores de las áreas sensibles y restringidas</p>	<ul style="list-style-type: none"> <li>a. Darán cumplimiento estricto a las disposiciones y documentos normativos de seguridad para proteger la seguridad física de los procesos institucionales que se realizan en su área de labores, manteniendo la confidencialidad y reserva necesaria.</li> <li>b. Antes de acceder al interior de las oficinas, el personal debe dejar los celulares y/o dispositivos de almacenamiento magnético dentro de los casilleros.</li> <li>c. En caso de contingencias, deberán evacuar el área usando las puertas y rutas de evacuación señaladas o indicadas por el servicio de seguridad y vigilancia.</li> <li>d. Deberán registrar sus ingresos y salidas a través de los dispositivos electrónicos de control de acceso biométricos o los que se encuentren disponibles.</li> <li>e. No pueden ingresar o retirar bienes electrónicos como laptops, dispositivos de almacenamiento magnético o documentos impresos, que no estén autorizados por su directivo.</li> </ul>

<sup>4</sup> Las disposiciones se aplican a todo el personal de la unidad de organización que se encuentre dentro del área sensible y restringida del intercambio de información.

		f. Deberán mostrar al servicio de seguridad y vigilancia el interior de sus carteras, bolsas y maletines, tanto al ingreso como a su salida.
--	--	--

### 5.2.9. Control de ingreso y salida en las áreas sensibles y restringidas relacionadas a la bóveda de la sede San Mateo

- a. El jefe de la OSDENA informa al Gerente de Almacenes cuando los colaboradores, incluyendo el personal directivo, no cumplan o trasgredan los documentos normativos de seguridad y del almacén.
- b. Cuando se programe una diligencia en la bóveda, la unidad de organización responsable deberá designar al servidor, de preferencia directivo, que estará a cargo de dirigir y/o participar en la recepción de bienes, en la fecha y hora programada. Para tal efecto, mediante documento electrónico deberá remitir al jefe de la OSDENA la autorización correspondiente e indicaciones necesarias para que actúe según su competencia funcional.
- c. La OSDENA, mediante el servicio de seguridad y vigilancia, realiza el control y revisión de las personas autorizadas para el ingreso y salida del área sensible y restringida; permanece en la puerta de la bóveda mientras dure la diligencia y por ningún motivo ingresa a los ambientes de la bóveda.
- d. El directivo encargado de la unidad de organización responsable autorizará el ingreso de personal de terceros cuando deba ingresar a la bóveda y dispondrá su acompañamiento por un colaborador designado durante el tiempo que dure su labor.

## VI. ANEXOS

- Anexo N.° 01 Implementación y fortalecimiento de mecanismos de control para las salidas y reingresos de laptops y tablets en las Intendencias de la Aduana Marítima del Callao y la Intendencia de Aduana Aérea y Postal.
- Anexo N.° 02 Modelo de Acta de Inventario de bienes del contratista/proveedor
- Anexo N.° 03 Modelo de Acta de Retención de Bienes.
- Anexo N.° 04 Libros de control de seguridad.

## ANEXO N.º 01

### IMPLEMENTACIÓN Y FORTALECIMIENTO DE LOS MECANISMOS DE CONTROL PARA LAS SALIDAS Y REINGRESOS DE LAPTOPS Y TABLETS EN LAS INTENDENCIAS DE LA ADUANA MARÍTIMA DEL CALLAO Y LA INTENDENCIA DE ADUANA AÉREA Y POSTAL.

1. **Mecanismos de Control para la salida y reingresos de Laptops y Tablets de la Intendencia de Aduana Marítima del Callao y la Intendencia de Aduana Aérea y Postal.**
  - a. La salida temporal de las Laptops y Tablets de propiedad de la institución, se encuentran autorizadas para los colaboradores con modalidad de teletrabajo, fiscalizadores de aduanas, oficiales de aduanas, supervisores y directivos.
  - b. Para los colaboradores que no se encuentren en el inciso "a", la salida temporal de las Laptops y Tablets, será, mediante la presentación de:
    - La autorización del jefe inmediato mediante correo electrónico dirigido al Jefe de la OSDENA o UOSA, según corresponda, indicando el detalle del período por el cual se autoriza la salida.
    - Presentación del fotocheck, para verificar los datos del colaborador.
    - Se verificará el código patrimonial, para registrar su salida e ingreso.
    - No está permitido el retiro de Laptops y Tablets sin la autorización de su jefe inmediato.
  - c. Se dará cumplimiento a lo dispuesto por el Lineamiento temporal para la gestión de bienes muebles patrimoniales en la SUNAT vigente:
    - Verificación de la identidad del colaborador que retira el bien patrimonial, a través del fotocheck.
    - El servidor que por necesidad del servicio u otro motivo requiera ingresar o retirar bienes muebles que no sean de propiedad de la SUNAT solicitara a su jefe inmediato el registro de ingreso o salida en el registro a cargo de la OSDENA.
    - Es obligación de la OSDENA verificar la salida de los BMP y constatar que los datos consignados en la Guía de Remisión Electrónica correspondan al BMP que está siendo desplazado.
  - d. El ingreso de Laptops y Tablets de propiedad de los colaboradores está prohibido, excepcionalmente, los directivos de la unidad organizacional mediante correo electrónico dirigido al jefe de la OSDENA o de la UOSA, según corresponda, puede autorizar temporalmente el ingreso de estos, la responsabilidad de la custodia del bien está a cargo del colaborador que solicitó la autorización de acceso.
2. **Mecanismos de Control para el Coordinador de Seguridad de la OSDENA responsable de la Intendencia de Aduana Marítima del Callao y la Intendencia de Aduana Aérea y Postal.**
  - a. El Coordinador de seguridad de la OSDENA responsable de la sede dispondrá que el Personal de Seguridad y Vigilancia cumpla con:
    - Registrar el ingreso y salida de Laptops y Tablets en el Libro de Control de Movimiento de Bienes Patrimoniales y el aplicativo informático "Sistema de Vigilancia - Bandeja de movimientos de bienes de

movimiento frecuente”, verificando los datos requeridos como son: el número del Registro del trabajador y los números del código patrimonial de los bienes y el correo electrónico de autorización, que sustentan dicho movimiento.

- Verificar mediante la presentación del fotocheck, que la Laptop o Tablet esté asignada al colaborador que realiza el movimiento.
  - Verificar en el aplicativo las características de la Laptop y Tablet (código patrimonial, descripción, serie, marca, modelo, color), ingresando a la opción Número de Movimiento.
  - De identificar, posible retiro de Laptop y Tablets no asignados al colaborador, registrar en el cuaderno de ocurrencia el hecho, reportando al Coordinador de Seguridad de la OSDENA responsable de la sede e inmovilizar el bien formulando el Acta de Retención de Bienes (Anexo N° 3).
  - Verificar que, para la salida de más de una Laptop y Tablet, la información consignada en los documentos Guías de Remisión Electrónica (GRE), Pedido de Comprobante de Salida (PECOSA) de ser el caso, Remitente y Transportista, corresponda a los bienes descritos.
  - Efectuar rondas dentro de las Intendencias antes mencionadas para detectar Laptops o Tablets en condiciones inseguras, de presentarse esta situación, formular el informe correspondiente al Coordinador de Seguridad de la OSDENA, trasladando el bien a la garita de Seguridad y Vigilancia para la custodia respectiva, para su posterior devolución al colaborador con el acta respectiva.
  - Presentar al Coordinador de Seguridad de la OSDENA las recomendaciones que pudiera implementar para mejorar las condiciones de seguridad de las Laptop y Tablets, con la finalidad de prevenir pérdidas o hurtos.
- b. El Coordinador de Seguridad de la OSDENA, dentro de sus competencias funcionales, ejecutará lo siguiente:
- Llevar un registro mensual de ingreso y salida de Laptop y Tablet de las Intendencias de la Aduana Marítima del Callao y la Intendencia de Aduana Aérea y Postal.
  - Elaborar un cuadro estadístico de ingreso y salida de Laptop y Tablet de las Intendencias de la Aduana Marítima del Callao y la Intendencia de Aduana Aérea y Postal de manera mensual
  - Llevar un registro mensual de reportes de hallazgos de condiciones inseguras de Laptop y Tablet de la Aduana Marítima del Callao y la Intendencia de Aduana Aérea y Postal.
  - Programar mensualmente la capacitación teórico - práctico sobre el control de ingreso y salida de Laptop y Tablet para el personal de seguridad y vigilancia.
  - Llevar el registro de inducción y capacitación del personal de seguridad y vigilancia.

### **3. Medidas para prevenir pérdidas o hurtos**

- a. **Utilización del Fotocheck institucional**, de acuerdo con lo dispuesto por el Artículo 14 del Reglamento Interno de Trabajo (RIT), cuyo uso es obligatorio y

personal, debiendo presentar al servicio de seguridad y vigilancia cada vez que realice un movimiento de la laptop y/o Tablet.

- b. **Obligación de Reportar**, todo colaborador que por necesidad de servicio tenga que ingresar o retirar su laptop o Tablet a pie o en vehículo, deberá registrarlo de manera obligatoria en el servicio de seguridad y vigilancia.
- c. **Programación de charlas de capacitación para el personal del servicio de seguridad y vigilancia**, el Coordinador de Seguridad de la OSDENA realizará charlas de seguridad de manera mensual, relacionado al control de ingreso y salida de Laptop y Tablets, con la finalidad de mantener una retroalimentación permanente de las medidas de seguridad orientadas a prevenir pérdidas y hurtos de los equipos.
- d. **Verificación de movimiento de laptops y tablets almacenados**, el Gestor de Patrimonio de las Intendencias de la Aduana Marítima del Callao y la Intendencia de Aduana Aérea y Postal, deberá contar con la autorización del Jefe de la UOSA para el movimiento de los bienes patrimoniales indicados.

#### 4. **Trazabilidad, responsabilidad y control continuo en la sede de la Intendencia Marítima del Callao y la Intendencia Aérea y Postal.**

##### **Componentes para la Trazabilidad:**

- a. **Identificación y Control de Acceso:** Presentación de fotocheck institucional para registrar el movimiento de ingreso y salida de laptop y Tablet.
- b. **Aplicativo informático** “Sistema de Vigilancia - Bandeja de movimientos de bienes de movimiento frecuente”, verificando que los datos del equipo coincidan con la información registrada en el aplicativo en mención:
  - Código de Bien Patrimonial.
  - Número de serie.
  - Marca de la Laptop o Tablet.
  - Modelo.
  - Color.
- c. **Libros de Control de Seguridad:** el personal de seguridad registrará las condiciones inseguras y posibles retiros de laptop y tablets no asignados al colaborador, garantizando la trazabilidad de lo descrito.  
De manera excepcional, en caso de fallas en el aplicativo informático “Sistema de Vigilancia - Bandeja de movimientos de bienes de movimiento frecuente”, los movimientos de Laptop y Tablet serán registrados en el Libro de Seguridad N° 4 “Movimiento de Bienes Patrimoniales”
- d. **Difusión de medidas correctivas**, para garantizar la seguridad de las laptops y tablets, el Coordinador de Seguridad informará a las Gerencia de OSDENA y Seguridad de la Información, posibles retiros de bienes no asignados al colaborador, para garantizar la ejecución de acciones correctivas que correspondan.



**ANEXO N.º 03**  
**MODELO DE ACTA DE RETENCIÓN DE BIENES**

**ACTA DE RETENCIÓN DE BIENES**

En la ciudad de *(indicar la ciudad)* provincia de *(indicar la provincia)* siendo las *(indicar la hora)* horas del *(indicar la fecha)* de 2023 en el local *(indicar nombre del local)* en presencia de *(indicar los nombres del vigilante, el intervenido y del supervisor de vigilancia, de ser el caso)* en cumplimiento a los documentos normativos de control de acceso en *(indicar el puesto de vigilancia)* se detectó que, el Sr. *(indicar el nombre del intervenido)* identificado con DNI N°....., trabajador perteneciente a *(indicar a que empresa contratista pertenece)* el cual intentaba retirar del local *(indicar el material que pretendía retirar)*, se procedió a verificar los bienes cuyas características son:

1. *Señalar la descripción de los artículos y su condición (nuevo, usado, etc.)*
2. \_\_\_\_\_
3. \_\_\_\_\_

El Sr. *(Indicar el nombre del intervenido)*, a quien se le retuvo los mencionados artículos, manifestó que *(indicar en qué circunstancias lo encontró)*.

Dando fe de lo actuado, se procedió a la firma del Acta de Retención de Bienes.

\_\_\_\_\_  
**FIRMA DEL INTERVENIDO**


\_\_\_\_\_  
**AGENTE DE SEGURIDAD**

\_\_\_\_\_  
**SUPERVISOR DE SEGURIDAD**

## ANEXO N.º 04 LIBROS DE CONTROL DE SEGURIDAD

### Tapa, carátula y formato del Libro de Control N° 01 Accesos Peatonales





NOMBRE DEL LOCAL

LIBRO DE CONTROL N° 1 - ACCESOS PEATONALES

PUESTO


Fecha de inicio: .....  
Fecha de cierre: .....  
Foliado del 001 al 400 páginas

AÑO .....



## Tapa, carátula y formato del Libro de Control N° 02 Accesos vehiculares SUNAT





NOMBRE DEL LOCAL

**LIBRO DE CONTROL N° 02 ACCESOS  
VEHICULARES SUNAT**

PUESTO

Fecha de inicio: .....  
Fecha de cierre: .....  
Foliado del 001 al 400 páginas

AÑO .....



## Tapa, carátula y formato del Libro de Control N° 03 Accesos Vehículos Particulares




The image shows the format of the control book cover. It is a white rectangular box with a black border. At the top right is the SUNAT logo. Below it are several input fields:

- NOMBRE DEL LOCAL
- LIBRO DE CONTROL N° 03 ACCESOS VEHÍCULOS PARTICULARES
- PUESTO
- Fecha de inicio: .....
- Fecha de cierre: .....
- Foliado del 001 al 400 páginas
- AÑO .....



## Tapa, carátula y formato del Libro de Control N° 04 Movimiento de Bienes Patrimoniales





NOMBRE DEL LOCAL

**LIBRO DE CONTROL N° 04 MOVIMIENTO DE BIENES PATRIMONIALES**

PUESTO

Fecha de inicio: .....  
Fecha de cierre: .....  
Foliado del 001 al 400 páginas

AÑO .....



## Tapa, carátula y formato del Libro de Control N° 05 Ocurrencias



The image shows the format for the cover of the control book. It features the SUNAT logo at the top right. Below the logo are several input fields:

- A box for 'NOMBRE DEL LOCAL'.
- A box containing the text 'LIBRO DE CONTROL N° 05 OCURENCIAS'.
- A box for 'PUESTO'.
- A box containing the text: 'Fecha de inicio: .....', 'Fecha de cierre: .....', and 'Foliado del 001 al 400 páginas'.
- A box for 'AÑO .....



## Tapa, carátula y formato del Libro de Control N° 06 Ronda Interna



The image shows the format of the control book cover, which is a white rectangular area with a black border. At the top right, the SUNAT logo is displayed in blue. Below the logo, there are four rectangular boxes for text entry. The first box contains the text 'NOMBRE DEL LOCAL'. The second box contains the text 'LIBRO DE CONTROL N° 06 Ronda Interna'. The third box contains the text 'PUESTO'. The fourth box contains the text 'Fecha de inicio: .....', 'Fecha de cierre: .....', and 'Foliado del 001 al 400 páginas'. At the bottom center, there is a line for the year: 'AÑO .....



## Tapa, carátula y formato del Libro de Control N° 07 Ronda Externa



The image shows the format of the control book. It features the SUNAT logo at the top right. Below the logo are several input fields:

- NOMBRE DEL LOCAL
- LIBRO DE CONTROL N° 07 RONDA EXTERNA
- PUESTO
- Fecha de inicio: .....
- Fecha de cierre: .....
- Foliado del 001 al 400 páginas
- AÑO .....

0001

**RONDA EXTERNA**



SEDE: \_\_\_\_\_

TURNO	
-------	--

FECHA	
-------	--

HORA DE INGRESO	
-----------------	--

HORA DE SALIDA	
----------------	--

VERIFICACIONES REALIZADAS		
ITEM	Cantidad	Estado
Personal		
Carné SUCAMEC		
Uniforme		

NOMBRE DEL SUPERVISOR
-----------------------

--

FIRMA DEL SUPERVISOR
----------------------

--

OBSERVACIONES

VºBº

SEDE: \_\_\_\_\_

TURNO	
-------	--

FECHA	
-------	--

HORA DE INGRESO	
-----------------	--

HORA DE SALIDA	
----------------	--

VERIFICACIONES REALIZADAS		
ITEM	Cantidad	Estado
Personal		
Carné SUCAMEC		
Uniforme		

NOMBRE DEL SUPERVISOR
-----------------------

--

FIRMA DEL SUPERVISOR
----------------------


--

OBSERVACIONES

VºBº

## Tapa, carátula y formato del Libro de Control N° 08 Cargos





NOMBRE DEL LOCAL

**LIBRO DE CONTROL N° 08 CARGOS**

PUESTO

Fecha de inicio: .....  
Fecha de cierre: .....  
Foliado del 001 al 400 páginas

AÑO .....

001

## CARGOS



SEDE: \_\_\_\_\_

FECHA		HORA		
Trabajador ( )	Visitante ( )	Contratista ( )		
Descripción del Artículo				
Recibido por				
				Firma N° DNI / Registro
Entregado por				
				Firma

FECHA		HORA		
Trabajador ( )	Visitante ( )	Contratista ( )		
Descripción del Artículo				
Recibido por				
				Firma N° DNI / Registro
Entregado por				
				Firma

FECHA		HORA		
Trabajador ( )	Visitante ( )	Contratista ( )		
Descripción del Artículo				
Recibido por				
				Firma N° DNI / Registro
Entregado por				
				Firma

FECHA		HORA		
Trabajador ( )	Visitante ( )	Contratista ( )		
Descripción del Artículo				
Recibido por				
				Firma N° DNI / Registro
Entregado por				
				Firma