RESOLUCIÓN DE PRESIDENCIA

OSITRAN
Firmado por: ZAMBRANO COPELLO Rosa Veronica FAU 20420248645 hard
Motivo: Firma Digital
Fecha: 22/02/2019 13:18:05 -0500

Lima, 22 de febrero de 2019 **Nº0011-2019-PD-OSITRAN**

VISTOS:

El Informe N° 0023-2019-GPP-OSITRAN de la Gerencia de Planeamiento y Presupuesto; el Memorando N° 076-2019-GAJ-OSITRAN de la Gerencia de Asesoría Jurídica y Memorando N° 083-2019-GG-OSITRÁN de la Gerencia General;

CONSIDERANDO:

Que, mediante la Ley N° 26917, Ley de Supervisión de la Inversión Privada en Infraestructura de Transporte de Uso Público y sus modificatorias, se creó el Organismo Supervisor de la Inversión en Infraestructura de Transporte de Uso Público - OSITRAN, como organismo público encargado de normar, regular, supervisar, fiscalizar y resolver controversias respecto de los mercados relativos a la explotación de la infraestructura de transporte de uso público;

Que, la Ley N° 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos y sus modificatorias, dicta los lineamientos y normas de aplicación general para los Organismos Reguladores, encontrándose incluido dentro de sus alcances el OSITRAN;

Que, la Ley N° 29754 dispone que el OSITRAN es la Entidad competente para ejercer la supervisión de los servicios públicos de transporte ferroviario de pasajeros en las vías concesionadas que forman parte del Sistema Eléctrico de Transporte Masivo de Lima y Callao; asimismo, establece que, mediante Decreto Supremo, refrendado por el Presidente del Consejo de Ministros, a propuesta del OSITRAN, se aprueba la adecuación del Reglamento General del OSITRAN y otros documentos de gestión;

Que, de acuerdo con el artículo 6 del Reglamento General del OSITRAN, aprobado por Decreto Supremo N° 044-2006-PCM y sus modificatorias, la estructura orgánica del OSITRAN se rige por su Reglamento de Organización y Funciones;

Que, por Decreto Supremo N° 012-2015-PCM se aprobó el Reglamento de Organización y Funciones (ROF) del OSITRAN, con el fin de implementar las funciones establecidas por la Ley Nº 29754 y las instancias y órganos competentes, conforme lo señala el Reglamento General de OSITRAN, así como para promover una gestión eficiente, moderna, transparente y con enfoque de procesos y para resultados, cuyas decisiones institucionales sean predecibles;

Que, de acuerdo a lo señalado en los numerales 3 y 6 del artículo 9 del ROF de OSITRAN, son funciones de la Presidencia Ejecutiva aprobar políticas y planes de administración, de recursos humanos, finanza, así como de estrategias comunicacionales y de relaciones institucionales, a propuesta de la gerencia general, en concordancia con la normativa de la materia. Asimismo, es atribución de la Presidencia Ejecutiva la aprobación de normas, directivas, manuales y otros documentos de carácter institucional que se requiera para el cumplimiento de los fines de OSITRAN;

Que, mediante Decreto Supremo N° 092-2017-PCM se aprueba la Política Nacional de Integridad y Lucha contra la Corrupción con el objeto de contar con instituciones transparentes e íntegras que practican y promueven probidad en el ámbito público, sector empresarial y la sociedad civil;

Visado por: MEJIA CORNEJO Juan Carlos FIR 08271955 hard
Motivo: Firma Digital
Fecha: 22/02/2019 13:14:48 -0500

Que, mediante Decreto Supremo N° 042-2018-PCM se establecen medidas para fortalecer la integridad pública y lucha contra la corrupción con el objeto de orientar la correcta, transparente y eficiente actuación de los servidores públicos y de las entidades públicas, a fin de contribuir al cumplimiento de las políticas en materia de integridad pública;

Visado por: LA ROSA ROSADO Victor Hugo FIR 07546366 hard
Motivo: Firma Digital
Fecha: 22/02/2019 13:13:11 -0500

Visado por: ARTOLA GRADOS Jorge Hernan FIR 10540923 hard
Motivo: Firma Digital
Fecha: 22/02/2019 13:10:41 -0500

Que, mediante Decreto Supremo N° 044-2018-PCM se aprueba el Plan Nacional de Integridad y Lucha contra la corrupción 2018-2021;

Que, mediante, Ley N° 30424, Ley que regula la responsabilidad administrativa de las personas jurídicas por el delito de cohecho activo trasnacional", modificada a través del Decreto Legislativo N° 1352, se promueve en las organizaciones la implementación de un modelo de prevención adecuado a su naturaleza, riesgos, necesidades y características, consistentes en medidas de vigilancia y control idóneas para prevenir el delito de cohecho activo transnacional o para reducir significativamente el riesgo de su comisión;

Que, la Norma Técnica Peruana NTP-ISO 37001:2017 "Sistema de gestión antisoborno. Requisitos con orientación para su uso", aprobada por Resolución Directoral N° 012-2017/INACAL/DN, es el estándar internacional que especifica los requisitos y proporciona una guía para establecer, implementar, mantener, revisar y mejorar un sistema de gestión antisoborno;

Que, el numeral 5.2 de la NTP ISO 37001:2017 dispone que la Alta Dirección debe establecer, mantener y revisar una política antisoborno;

Que, el OSITRAN se encuentra implementando el Sistema de Gestión Antisoborno, ISO 37001:2016 o su equivalente en la Norma Técnica Peruana NTP-ISO 37001-2017, siendo para tal efecto necesaria la aprobación de una Política Antisoborno como instrumento de intención y dirección en cuyo marco se implementarán medidas orientadas a prevenir, detectar y sancionar el soborno bajo cualquier modalidad. En tal sentido, es conveniente precisar que dicha política se encuentra alineada a los documentos de gestión interna del OSITRAN;

Que, en cumplimiento del encargo de la Alta Dirección del OSITRAN, la Gerencia de Planeamiento y Presupuesto, sustentó y remitió al Gerente General mediante Informe N° 0023-2019-GPP-OSITRAN, la propuesta de Política de Gestión Antisoborno del OSITRAN y el proyecto de acto resolutivo correspondiente;

Que, mediante Memorando N° 076-2019-GAJ-OSITRAN del 22 de febrero de 2019, la Gerencia de Asesoría Jurídica, luego de la revisión del sustento normativo correspondiente, señaló que la propuesta del acto resolutivo elaborado por la Gerencia de Planeamiento y Presupuesto resulta jurídicamente viable; asimismo, precisó que en atención a lo dispuesto en los numerales 3 y 6 del Reglamento de Organización y Funciones del OSITRAN, que establecen como atribución de la Presidencia del Consejo Directivo, la aprobación de políticas institucionales, corresponde que la Política de Gestión Antisoborno sea aprobada por la Presidencia del Consejo Directivo;

Que, mediante Memorando N°083-2019-GG-OSITRAN del 22 de febrero de 2019, la Gerencia General otorgó su conformidad al proyecto de Resolución y lo remitió debidamente visado para proseguir con el trámite correspondiente;

De conformidad con lo dispuesto en la Ley N° 26917, Ley de Supervisión de la Inversión Privada en Infraestructura de Transporte de Uso Público, Ley de creación del OSITRAN y sus modificatorias; el Reglamento de Organización y Funciones del Organismo Supervisor de la Inversión en Infraestructura de Transporte de Uso Público – OSITRAN, aprobado mediante Decreto Supremo N° 012-2015-PCM, la Ley N° 30424, Ley que regula la responsabilidad administrativa de las personas jurídicas;

SE RESUELVE:

Artículo 1.- Aprobar la Política de Gestión Antisoborno del OSITRAN, que en un (01) folio anexo forma parte integrante de la presente Resolución.

Artículo 2.- Notificar la presente Resolución a todos los órganos, unidades orgánicas y oficinas que conforman el OSITRAN, para conocimiento, difusión y aplicación.

Artículo 3.- Publicar la presente Resolución en el Portal Institucional de OSITRAN (www.ositran.gob.pe).

Regístrese y comuníquese,

VERONICA ZAMBRANO COPELLO
Presidenta del Consejo Directivo

NT. 2019014593

POLÍTICA DEL SISTEMA DE GESTIÓN ANTISOBORNO

El Organismo Supervisor de la Inversión Privada en Infraestructura de Transporte de Uso Público - OSITRÁN, es un equipo de trabajo comprometido con la mejora continua de su Sistema de Gestión Antisoborno, lo que le permite garantizar a través de su intervención, el funcionamiento eficiente de la infraestructura de transporte de uso público, el servicio de transporte de pasajeros del Metro de Lima y Callao y la calidad del servicio a los usuarios, empresas concesionarias y al Estado.

OSITRÁN respecto de su Sistema de Gestión Antisoborno se compromete con:

- ✓ Prohibir el soborno bajo cualquier modalidad en toda la organización
- ✓ Cumplir las leyes, reglamentos y normas antisoborno aplicables a la organización
- ✓ Cumplir los requisitos del sistema de gestión antisoborno
- ✓ Promover el planteamiento de inquietudes de buena fe o sobre la base de una creencia razonable en confianza y sin temor a represalias.
- ✓ Designar a una persona quien asumirá la función de cumplimiento de manera independiente, con la autoridad para supervisar el diseño del sistema, asegurar la conformidad con los requisitos aplicables y orientar al personal en las cuestiones pertinentes del sistema de gestión antisoborno.

El incumplimiento de las disposiciones de esta política, será objeto de las medidas y sanciones previstas en la normativa vigente, previa investigación y establecimiento de la responsabilidad respectiva.

Versión 01, aprobada mediante Resolución N° 0011-2019-PD-OSITRAN de fecha 22 de febrero de 2019.

OSITRAN
EL REGULADOR DE LA INFRAESTRUCTURA DE TRANSPORTE DE USO PÚBLICO

Formación del Sistema de Gestión Antisoborno (ISO 37001:2016)

Empresas Supervisoras

2023

OSITRAN
EL REGULADOR DE LA INFRAESTRUCTURA DE TRANSPORTE DE USO PÚBLICO

¿Quiénes somos?

Ositrán, creado en enero de 1998 por Ley N° 26917, es un organismo público, descentralizado, adscrito a la PCM, con autonomía administrativa, funcional, técnica, económica y financiera.

OSITRAN
EL REGULADOR DE LA INFRAESTRUCTURA DE TRANSPORTE DE USO PÚBLICO

Conoce nuestra misión

“Supervisar de manera efectiva la infraestructura de transporte de uso público concesionada, contribuyendo a la mejora de la calidad de vida de los ciudadanos.”

OSITRAN
EL REGULADOR DE LA INFRAESTRUCTURA DE TRANSPORTE DE USO PÚBLICO

¿Cuáles son nuestras funciones?

Supervisar

Regular

Normar

Fiscalizar

Sancionar

Solucionar controversias y atender reclamos

OSITRAN
EL REGULADOR DE LA INFRAESTRUCTURA DE TRANSPORTE DE USO PÚBLICO

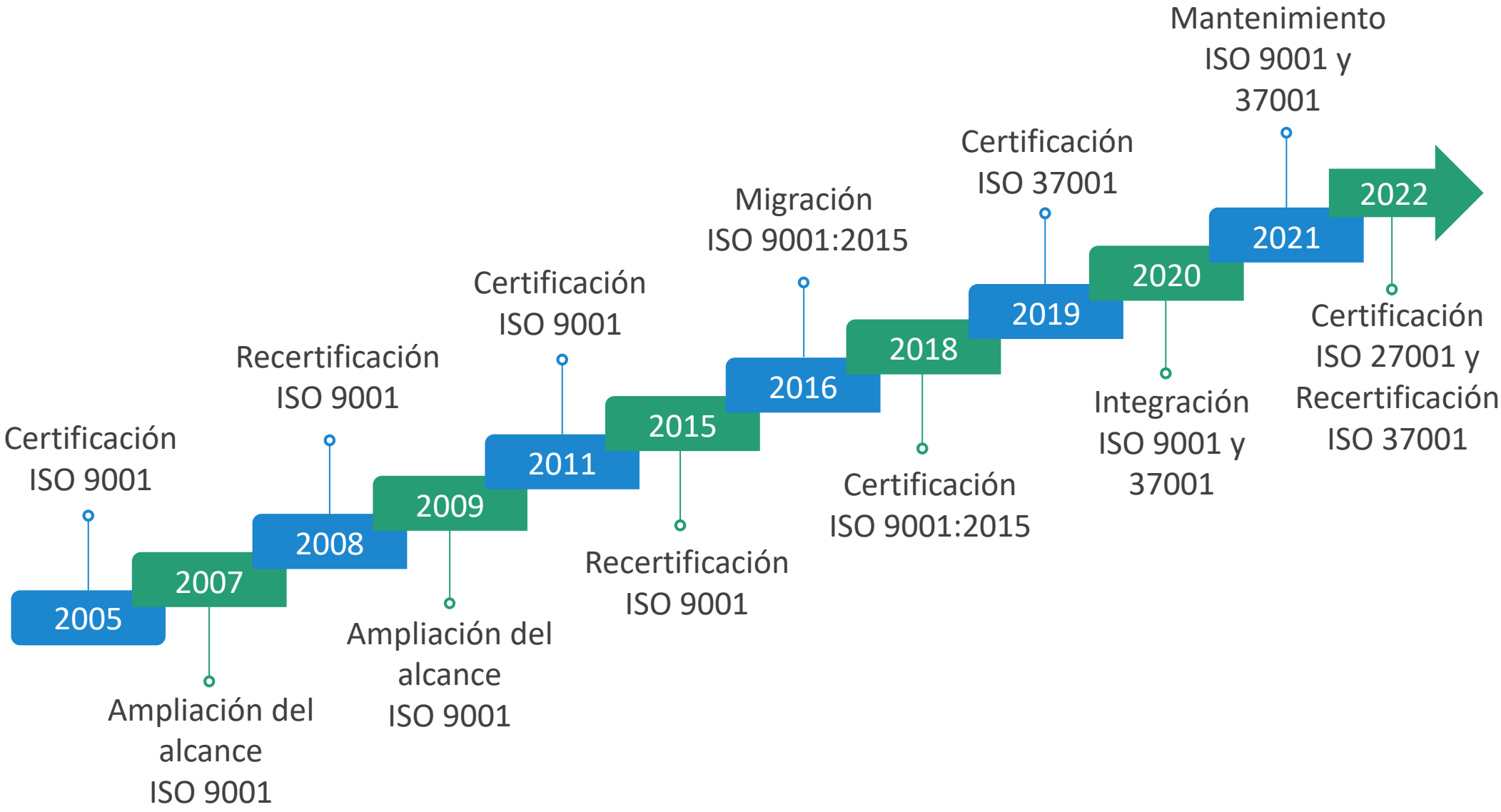
Conoce nuestra cultura y valores

“Cultura orientada al servicio, transparente, a la transformación digital, profesional y comprometida”

Nuestros valores

- EXCELENCIA
- COMPROMISO
- INTEGRIDAD
- IMPARCIALIDAD

¿Sabías que el Ositrán cuenta con la ISO 9001 y 37001?



Recuerda las siguientes definiciones

SISTEMA DE GESTIÓN

Conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr esos objetivos.

Basados en la Norma ISO 9000:2015.

Recuerda las siguientes definiciones

POLÍTICA

Intenciones y dirección de una organización, como las expresa formalmente su alta dirección.

OBJETIVO

Resultado a lograr.

Basados en la Norma ISO 9000:2015.

¿Qué es la Norma ISO 37001?

NORMA ISO 37001

La norma ISO 37001 especifica los requisitos y proporciona orientación sobre cómo establecer, implementar, mantener, revisar y mejorar un **Sistema de Gestión Antisoborno (SGAS)**.

Basados en la Norma ISO 37001:2016.

Conoce los requisitos de la ISO 37001

OSITRAN
EL REGULADOR DE LA INFRAESTRUCTURA DE TRANSPORTE DE USO PÚBLICO

SISTEMA DE GESTIÓN ANTISOBORNO EN EL OSITRÁN

Sistema de Gestión Antisoborno

En el año 2022, el costo de la corrupción en el Perú es de **S/ 24.419 millones** según el Contralor General de la República.

57% Población opina que la corrupción es el segundo problema del país. Encuesta Proetica 2022.

Índice de Percepción de la Corrupción 2022: El Perú ocupa el puesto **101 de 180 economías.**

Nuestra Política del Sistema de Gestión Antisoborno del Ositrán

OSITRAN, es un equipo de trabajo comprometido con la mejora **continua de su Sistema de Gestión Antisoborno**, lo que le permite garantizar a través de su intervención, el funcionamiento eficiente de la infraestructura de transporte de uso público, el servicio de transporte de pasajeros del Metro de Lima y Callao y la calidad del servicio a los usuarios, empresas concesionarias y al Estado.

OSITRÁN respecto de su SGAS se compromete con:

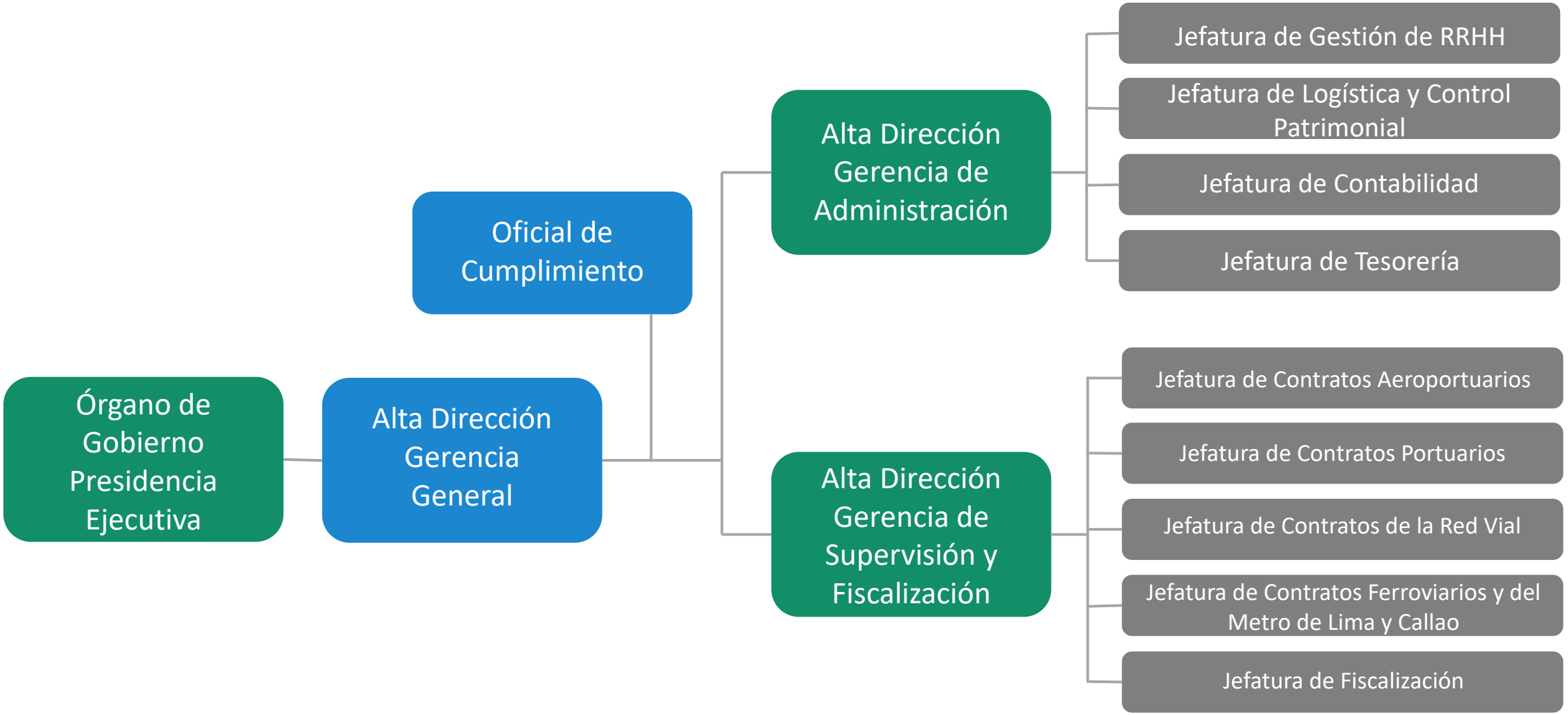
- Prohibir el soborno bajo cualquier modalidad en toda la organización
- Cumplir las leyes, reglamentos y normas antisoborno aplicables a la organización
- Cumplir los requisitos del sistema de gestión antisoborno
- Promover el planteamiento de inquietudes de buena fe o sobre la base de una creencia razonable en confianza y sin temor a represalias.
- Designar a una persona quien asumirá la función de cumplimiento de manera independiente, con la autoridad para supervisar el diseño del sistema, asegurar la conformidad con los requisitos aplicables y orientar al personal en las cuestiones pertinentes del sistema de gestión antisoborno.

RECUERDA

El incumplimiento de las disposiciones de la política será objeto de las medidas y sanciones previstas en la normativa, previa investigación y establecimiento de la responsabilidad respectiva.

Versión 01, aprobada mediante Resolución N° 0011-2019-PD-OSITRAN
https://www.ositran.gob.pe/wp-content/uploads/2019/02/011PD2019.pdf

Conoce la Organización del SGAS



Versión 01, aprobada mediante Resolución N° 014-2019-PD-OSITRAN de fecha 08 de marzo de 2019.

Conoce el Código de Conducta y Ética del Ositrán

El ***"Código de Conducta y Ética del Ositrán"*** se aprobó mediante la Resolución N° 016-2023-PD-OSITRAN.

Finalidad:

- Regular, a través de un documento de observancia obligatoria, la conducta y el comportamiento ético de los/as servidores/as del Ositrán orientado a un enfoque de integridad pública, acorde a los principios éticos y valores institucionales, así como a los deberes y prohibiciones que orientan la conducta del/la empleado/a público en el ejercicio de sus funciones.
- Estimular la probidad en los/as servidores/as del Ositrán en el cumplimiento de sus funciones, de modo que no se incurra en conflicto de intereses, discriminación, faltas contra la integridad y/o actos de corrupción, logrando el establecimiento de una óptima cultura organizacional basada en la ética e integridad.
- Establecer incentivos y estímulos a fin de promover y fortalecer una cultura ética y de integridad en la entidad con la finalidad de evitar conductas inadecuadas y contrarias a las mismas.

Resolución N° 016-2023-PD-OSITRAN publicado en la página web:
https://www.ositran.gob.pe/anterior/resoluciones/resolucion-n-016-2023-pd-ositran/

Conoce el Código de Conducta y Ética del Ositrán

- El presente Código de Conducta y Ética se aplica a todos/as los/as servidores/as del Ositrán, independientemente del régimen laboral al que pertenezcan, a quienes, en adelante, se les denominará servidores/as del Ositrán.

- Para el caso de los/as proveedores/as, contratistas, concesionarios, empresas supervisoras, consultores y otros relacionados al Ositrán, tiene calidad informativa y de aplicación, en lo que les compete.

Código de Conducta y Ética del Ositrán

Los/as servidores/as del Ositrán se encuentran **prohibidos** de incurrir en los supuestos establecidos en la **Ley del Código de Ética** que se detallan a continuación:

a. Mantener intereses de conflicto

Mantener relaciones o aceptar situaciones en cuyo contexto sus intereses personales, laborales, económicos o financieros pudieran estar en conflicto con el cumplimento de los deberes y funciones a su cargo.

b. Obtener ventajas indebidas (soborno)

Obtener o procurar beneficios o ventajas indebidas, de cualquier tipo, para sí o para otros, mediante el uso de su cargo, autoridad, influencia o apariencia de influencia. Queda expresamente prohibido a los/as servidores/as del Ositrán aceptar algún tipo de regalo, atención, donación o beneficios similares (con excepción de merchandising) que se preste a dudas sobre la probidad del colaborador en el desarrollo de sus funciones.

Código de Conducta y Ética del Ositrán

Los/as servidores/as del Ositrán se encuentran **prohibidos** de incurrir en los supuestos establecidos en la **Ley del Código de Ética** que se detallan a continuación:

c. Realizar actividades de proselitismo político

A través de la utilización de sus funciones o por medio de la utilización de infraestructura, bienes o recursos públicos, ya sea a favor o en contra de partidos u organizaciones políticas o candidatos.

d. Hacer mal uso de información privilegiada

Participar en transacciones u operaciones financieras utilizando información privilegiada del Ositrán o que pudiera tener acceso a ella por su condición o ejercicio del cargo que desempeña, ni debe permitir el uso impropio de dicha información para el beneficio de algún interés.

Código de Conducta y Ética del Ositrán

Los/as servidores/as del Ositrán se encuentran **prohibidos** de incurrir en los supuestos establecidos en la **Ley del Código de Ética** que se detallan a continuación:

e. Presionar, amenazar y/o acosar

Ejercer presiones, amenazas o acoso sexual contra otros/as servidores/as civiles o subordinados que puedan afectar la dignidad de la persona o inducir a la realización de acciones dolosas.

7.4. Perseguir, acosar o discriminar a servidores/as civiles de la entidad

Por reportar y/o denunciar algún acto de corrupción, o actos en contra de lo dispuesto en el Código de Conducta y Ética, la Ley del Código de Ética, en contra de las disposiciones aprobadas por el Ositrán respecto del Sistema de Gestión Antisoborno, y la Política Nacional de Integridad y Lucha contra la Corrupción, así como los relacionados a las normas de igualdad de género, hostigamiento sexual u otros.

Código de Conducta y Ética del Ositrán

Para el caso de nuestros proveedores, contratistas, concesionarios, empresas supervisoras, consultores y otros relacionados:

- 10.3.1 Al Ositrán le interesa relacionarse y contratar con personas naturales o jurídicas que mantengan prácticas honestas y transparentes y que puedan demostrarlo con su rectitud en el actuar; para ello, se han establecido cláusulas anticorrupción en los contratos relacionadas con el comportamiento ético y solvente, exigiéndoles el compromiso de combatir y prevenir la corrupción en todas sus modalidades, y solicitándoles la implementación de controles relacionados con la formación y concientización anticorrupción en su personal.

- 10.3.2 Respecto de los Concesionarios, se afianzará una lucha mancomunada contra la corrupción, a través de la firma de un Compromiso Ético y de Anticorrupción.

Numeral 10.3 del Código de Conducta y Ética del Ositrán, aprobada mediante Resolución N° 016-2023-PD-OSITRAN.

Recuerda

Los servidores/as del Ositrán están expresamente **prohibidos de recibir y/o aceptar algún tipo de regalo, atención, donación o beneficios similares** (con excepción de merchandising), que se preste a dudas sobre la probidad del servidor civil en el desarrollo de sus funciones.

El Código de Conducta y Ética del Ositrán, aprobado mediante Resolución N° 016-2023-PD-OSITRAN publicado en la página web:
https://www.ositran.gob.pe/anterior/resoluciones/resolucion-n-016-2023-pd-ositran/

Conoce la plataforma digital única de denuncias del ciudadano

Puedes **REPORTAR** cualquier **acto de soborno y corrupción y conductas inapropiadas** en contra de las medidas que regulan el **comportamiento ético** de los miembros del Ositrán, vía los siguientes canales:

Página web:
https://denuncias.servicios.gob.pe/

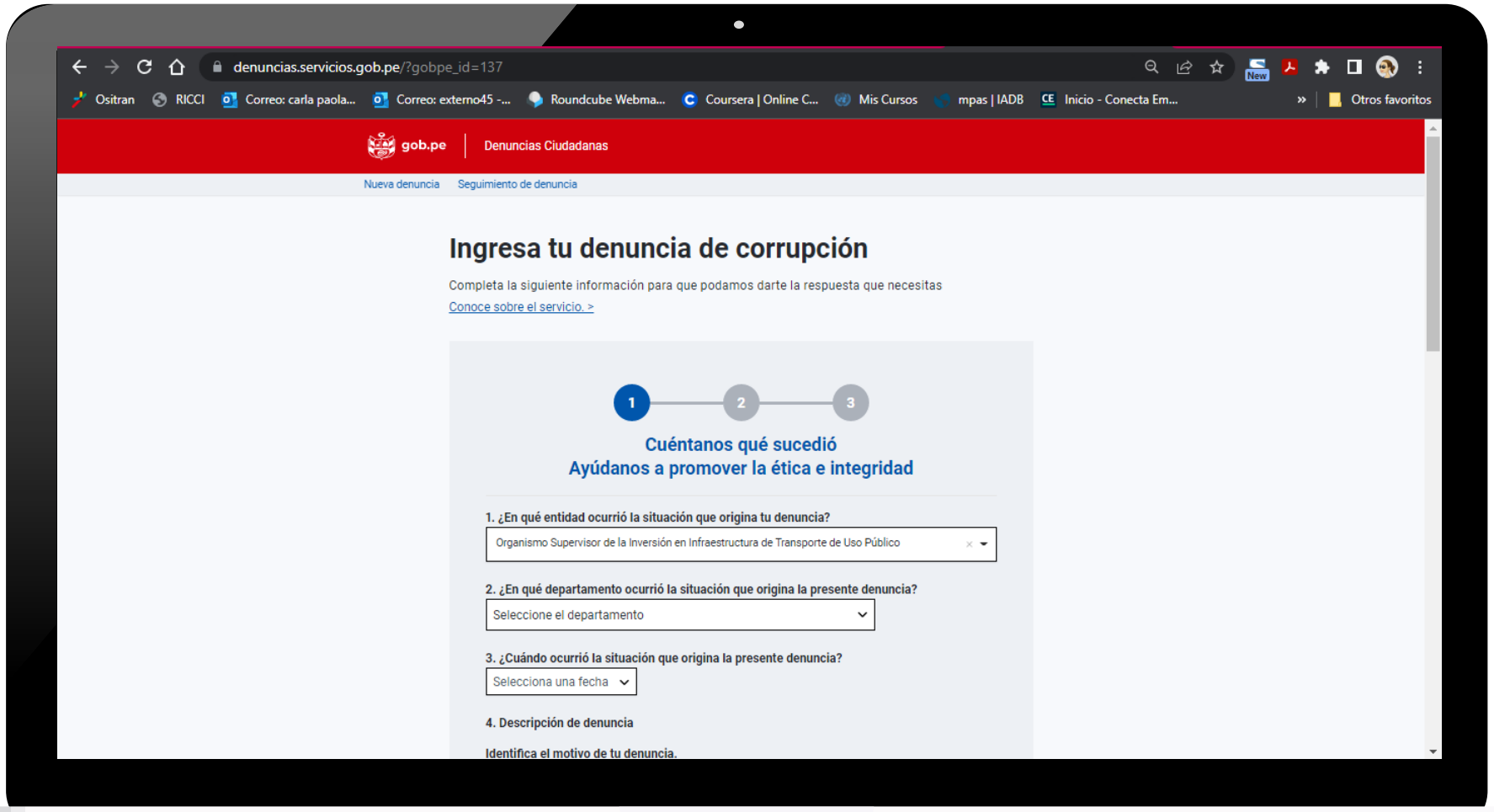
Correo electrónico:
denunciasactosdecorrupcion@ositran.gob.pe

Línea telefónica: # 500-9337

Cualquier **violación de la política antisoborno o incumplimiento** pueden contactarse con el **Oficial de Cumplimiento** al :

Correo electrónico:
funciondecumplimientoantisoborno@ositran.gob.pe

Conoce la plataforma digital única de denuncias del ciudadano



CODIGO DE CONDUCTA Y ÉTICA DEL OSITRAN

VERSIÓN 1

2023

Organismo Supervisor de la Inversión en Infraestructura de Transporte de Uso Público
OSITRÁN

CODIGO DE CONDUCTA Y ÉTICA DEL OSITRAN

I. INTRODUCCIÓN

En nuestro país, hace varios años, se viene trabajando en el establecimiento de una cultura de integridad en el sector público lo cual se evidencia en la emisión de una serie de normativa aplicable a distintos ámbitos del quehacer público, incluida una Política Nacional de Integridad y Lucha contra la Corrupción, y la consecuente aprobación de un Plan Nacional de Integridad y Lucha contra la Corrupción, que establece el Modelo de Integridad para las entidades del sector público, y viene siendo implementada por todas las entidades a través de las directrices emitidas por la Secretaría de Integridad Pública de la Presidencia del Consejo de Ministros.

El Ositrán viene implementando el modelo de integridad con mucho interés y responsabilidad; por ello, basados en la normativa de la materia, ha elaborado el presente Código de Conducta y Ética, el cual se constituye en un documento de naturaleza preventiva orientado a lograr el establecimiento y desarrollo de una sólida cultura de integridad, el mismo que además de brindar información sobre los principios, deberes y prohibiciones de los servidores civiles y de nuestros valores institucionales, está orientado, a través de ejemplos, a promover la integridad en el comportamiento y el actuar de todo funcionario y/o servidor civil de la entidad.

Por lo que, cada uno de nosotros nos hacemos responsables del óptimo y efectivo cumplimiento de los términos del presente documento, así como de las normas y procedimientos establecidos en la entidad respecto a nuestro diario quehacer dentro y fuera de la entidad, en relación con los administrados, proveedores, contratistas, concesionarios, empresas supervisoras, consultores, entre otros.

El Ositrán tiene la plena confianza en que todos/as sus funcionarios/as y/o servidores/as mantienen, en el cumplimiento de sus funciones, una conducta ética, la cual contribuye al fortalecimiento de la entidad y su imagen, a través del cumplimiento honesto, probo, transparente, de igualdad, sin discriminación, y responsable de sus deberes y obligaciones, manteniendo estándares de conducta éticos los que nos caracterizan; teniendo claro que, si se incumplen las disposiciones establecidas dará lugar a acciones disciplinarias, medidas correctivas o preventivas conforme al marco normativo vigente.

Finalmente precisamos que, todos somos responsables de nuestra actuación, ya sea dentro o fuera de la entidad; por lo que, ningún funcionario/a y/o servidor/a público del Ositrán debe cometer actos contrarios a nuestros valores institucionales, que se vean materializados en actos de corrupción como soborno u otro afín, inclusive si dichas acciones son requeridas por su superior u otro funcionario/a y/o servidor/a público, así como tampoco debe animar o incentivar a que otros/as actúen de manera deshonesta, por el contrario su actuar debe encontrarse orientada a la prevención de cualquier tipo de falta o delito que contravenga los valores éticos del Ositrán.

II. OBJETIVO

Establecer los lineamientos que sirvan para orientar a los/as servidores/as del Ositrán en el ejercicio diario de sus funciones a fin de que se conduzcan, dentro y fuera de la entidad, de manera proba, transparente, respetando la igualdad entre hombres y mujeres en su diversidad, fortaleciendo una cultura basada en los valores institucionales, especialmente en la integridad, reforzando la confianza de la ciudadanía y en pro del logro de los objetivos institucionales.

III. FINALIDAD

a) Regular, a través de un documento de observancia obligatoria, la conducta y el comportamiento ético de los/as servidores/as del Ositrán orientado a un enfoque de integridad pública, acorde a los principios éticos y valores institucionales, así como a los deberes y prohibiciones que orientan la conducta del/la empleado/a público en el ejercicio de sus funciones.

b) Estimular la probidad en los/as servidores/as del Ositrán en el cumplimiento de sus funciones, de modo que no se incurra en conflicto de intereses, discriminación, faltas contra la integridad y/o actos de corrupción, logrando el establecimiento de una óptima cultura organizacional basada en la ética e integridad.

c) Establecer incentivos y estímulos a fin de promover y fortalecer una cultura ética y de integridad en la entidad con la finalidad de evitar conductas inadecuadas y contrarias a las mismas.

IV. ALCANCE

El presente Código de Conducta y Ética se aplica a todos/as los/as servidores/as del Ositrán, independientemente del régimen laboral al que pertenezcan, a quienes, en adelante, se les denominará servidores/as del Ositrán.

Para el caso de los/as proveedores/as, contratistas, concesionarios, empresas supervisoras, consultores y otros relacionados al Ositrán, tiene calidad informativa y de aplicación, en lo que les compete.

V. BASE LEGAL

5.1. Constitución Política del Perú.

5.2. Ley Nº 26771, Ley que establece prohibición de ejercer la facultad de nombramiento y contratación de personal en el Sector Público, en casos de parentesco.

5.3. Ley N° 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República y sus modificatorias

5.4. Ley N° 27815, Ley del Código de Ética de la Función Pública y sus modificatorias.

5.5. Ley N° 27588, Ley que establece prohibiciones e incompatibilidades de funcionarios y servidores públicos, así como de las personas que presten servicios al Estado bajo cualquier modalidad contractual.

5.6. Ley N° 28175, Ley Marco del Empleo Público.

5.7. Ley N° 30057, Ley del Servicio Civil.

5.8. Ley N° 31564, Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público.

5.9. Decreto Legislativo N° 1327, Decreto Legislativo que establece medidas de protección para el denunciante de actos de corrupción y sanciona las denuncias realizadas de mala fe.

5.10. Resolución Suprema N° 120-2010-PCM, que aprobó los “Lineamientos para la selección y reconocimiento del empleado público que destaque en el cumplimiento del Código de Ética de la Función Pública”.

5.11. Decreto Supremo N° 033-2005-PCM, Reglamento de la Ley del Código de Ética de la Función Pública y sus modificatorias.

5.12. Decreto Supremo N° 040-2014-PCM, Reglamento General de la Ley del Servicio Civil y sus modificatorias.

5.13. Decreto Supremo N° 092-2017-PCM, que aprobó la Política Nacional de Integridad y Lucha contra la Corrupción.

5.14. Decreto Supremo N° 010-2017-JUS, Reglamento del Decreto Legislativo N° 1327 y su modificatoria.

5.15. Decreto Supremo N° 042–2018–PCM, Decreto Supremo que establece medidas para fortalecer la integridad pública y lucha contra la corrupción.

5.16. Decreto Supremo N° 044–2018–PCM, Decreto Supremo que aprueba el Plan Nacional de Integridad y lucha contra la corrupción 2018 – 2021.

5.17. Decreto Supremo N° 004-2019-JUS, Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General.

5.18. Decreto Supremo Nº 021–2019–JUS, Decreto Supremo que aprueba el Texto Único Ordenado de la Ley Nº 27806, Ley de Transparencia y Acceso a la Información Pública.

5.19. Decreto Supremo N° 021-2000-PCM, que aprueba el Reglamento de la Ley que establece prohibición de ejercer la facultad de nombramiento y contratación de personal en el Sector Público, en casos de parentesco.

5.20. Decreto Supremo N° 180-2021-PCM, Decreto Supremo que aprueba la Estrategia de Integridad del Poder Ejecutivo al 2022 para la Prevención de Actos de Corrupción.

5.21. Decreto Supremo N° 019-2002-PCM, que aprueba el Reglamento de la Ley Nº 27588, que establece prohibiciones e incompatibilidades de funcionarios y servidores públicos, así como de las personas que presten servicios al Estado bajo cualquier modalidad contractual.

5.22. Decreto Supremo N° 012-2015-PCM, Reglamento de Organización y Funciones del Ositrán y sus modificatorias.

5.23. Resolución de Presidencia N° 201-2015-SERVIR-PE, que aprobó la Directiva N° 002-2015-SERVIR/GPGSC "Régimen Disciplinario y Procedimiento Sancionador de la Ley N° 30057, Ley del Servicio Civil", modificada por la Resolución de Presidencia Ejecutiva N° 092-2016-SERVIR-PE.

5.24. Resolución de Secretaría de Integridad Pública N° 002-2021-PCM/SIP, que aprueba la Directiva N° 002-2021-PCM/SIP "Lineamientos para fortalecer una cultura de integridad en las entidades del sector público"

5.25. Resolución de Presidencia N° 011-2019-PD-OSITRAN, que aprobó la Política del Sistema de Gestión Antisoborno del Ositrán.

5.26. Resolución de Gerencia General N° 015-2019-GG-OSITRAN, que aprobó la Directiva que regula la atención de denuncias sobre actos de corrupción en el OSITRAN.

5.27. Resolución de Gerencia General N° 121-2018-GG-OSITRAN, modificada por la Resolución de Gerencia General N° 010-2020-GG-OSITRAN que delegan las funciones de la Oficina de Integridad a la Jefatura de Gestión de Recursos Humanos.

5.28. Resolución de Presidencia N° 013-2020-PD-OSITRAN que aprueba la Política de Integridad del Ositrán.

5.29. Resolución de Gerencia General N° 00054-2022-GG-OSITRAN, que aprobó la nueva versión del Reglamento Interno de los Servidores Civiles del Ositrán.

5.30. Resolución Directoral N° 012-2017-INACAL/DN, NTP-ISO 37001-2017, Sistemas de Gestión Antisoborno. Requisitos con orientación para su uso.

Las normas contenidas en el presente reglamento tienen carácter enunciativo, más no limitativo.

VI. DISPOSICIONES GENERALES

6.1. CONCEPTOS

a) **Código de conducta y ética:** Es el instrumento mediante el cual se establecen los lineamientos para la correcta, transparente y eficiente actuación de los servidores civiles con el fin de promover una cultura de integridad y servicio a la ciudadanía al interior de cada entidad.

b) **Corrupción**: Mal uso del poder público o privado para obtener un beneficio indebido; económico, no económico o ventaja directa o indirecta; por agentes públicos, privados o ciudadanos; vulnerando principios y deberes éticos, normas y derechos fundamentales.

c) **Cultura de integridad:** Es la expresión de saberes y prácticas compartidas en una institución donde se actúa de manera consistente con sus valores organizacionales y en coherencia con el cumplimiento de los principios, deberes

y normas destinados a privilegiar el interés general, luchar contra la corrupción y elevar permanentemente los estándares de la actuación pública. Para contribuir a fortalecer una cultura de integridad en el sector público, las entidades cuentan con un Modelo de Integridad.

d) **Enfoque de integridad**: Es un enfoque transversal de gestión destinado a evaluar y fortalecer el desempeño ético de los/as servidores/as y funcionarios/as públicos, mitigando los riesgos que pudieran conducir o facilitar en una entidad la comisión de prácticas contrarias a la ética o corruptas, de modo que se actúe con prevención, debida diligencia y de manera oportuna.

e) **Integridad pública:** Es la actuación coherente con valores, principios y normas, que promueve y protege el desempeño ético de la función pública, de modo que los poderes y recursos confiados al Estado se dispongan hacia los fines que se destinaron, asegurando que el servicio público a la ciudadanía esté orientado al interés general y a la generación de valor público.

f) **Modelo de integridad:** Es el conjunto de orientaciones dirigidas a fortalecer la capacidad preventiva y defensiva de las entidades frente a la corrupción y diversas prácticas contrarias a la ética. Desde la normativa vigente, dichas orientaciones se organizan de manera sistémica en una estructura de trabajo de nueve componentes sobre la base de conceptos y pautas específicas a nivel organizacional y funcional, que, a la fecha, constituyen el estándar peruano de integridad y un marco de trabajo para implementar el enfoque de integridad en la entidad.

g) **Reconocimiento:** Es la expresión de felicitación como consecuencia del desempeño sobresaliente de un/a servidor/a civil y constituye un incentivo que contribuye a potenciar las capacidades, competencias y habilidades de los/as servidores/as, así como su satisfacción laboral, desempeño, incremento de autoestima y productividad laboral. Para el presente caso se reconoce el compromiso y buenas prácticas especialmente las relacionadas a la cultura de ética e integridad, en el diario quehacer en cumplimiento de las funciones y fuera de ella.

6.2. NUESTRA MISION

"Supervisar de manera efectiva la infraestructura de transporte de uso público concesionada, contribuyendo a la mejora de la calidad de vida de los ciudadanos".

6.3. VALORES INSTITUCIONALES

Los/as servidoresas del Ositrán, actúan de conformidad con los siguientes valores:

6.3.1. Excelencia: Orientamos nuestra gestión al logro de resultados, demostrando profesionalismo y criterio técnico para el desarrollo de nuestras funciones y para brindar servicios eficientes y de calidad a nuestros usuarios. Con equipos versátiles, capaces de adaptarse al cambio, utilizando metodologías ágiles y apoyándonos en la tecnología para la mejora continua.

6.3.2. Imparcialidad: Tomamos decisiones de manera justa, objetiva, técnica y transparente en beneficio de la sociedad, cautelando el bien común y respetando los intereses de cada una de las partes.

6.3.3. Compromiso: Estamos comprometidos con la satisfacción de las necesidades y la generación de valor a nuestros usuarios y servidores, con calidad en el ejercicio de nuestro rol y espíritu innovador.

6.3.4. Integridad: Somos honestos y congruentes con los principios de respeto, equidad, inclusión y autocontrol, cumpliendo la normativa. Compartimos información y rendimos cuentas para mantener la confianza y credibilidad en nuestra labor y funciones.

6.4. INTERROGANTES PARA APLICAR EN CASO DE DUDA EN EL CUMPLIMIENTO DE NUESTRAS FUNCIONES

6.4.1. Interrogantes para tener en cuenta antes de tomar una decisión[1]

- ¿La decisión que voy a tomar es justa, está alineada al esquema de valores establecidos en el presente código?
- ¿Cómo afecta esta decisión a las y los demás?
- ¿Me sentiría cómodo/a si esta decisión fuera de conocimiento público?
- ¿Esta decisión perjudica la reputación de la institución?
- ¿La decisión que voy a tomar tiene consecuencias legales?

6.4.2. Interrogantes para tener en cuenta ante situación de conflicto de intereses[2]

- ¿Puedo yo, un/a familiar, una amistad o un/a asociado/a, obtener algún beneficio a causa de la decisión o acción que debo adoptar en nombre de la organización?

---

[1] Código de Ética y Conducta del Ministerio de Economía y Finanzas, aprobado mediante Resolución Ministerial N°099-2019-MEF/43.

[2] "Manual de Principios, Deberes y Prohibiciones Éticas en la Función Pública", publicado por la Comisión de Alto Nivel Anticorrupción – CAN (2016).

- ¿Soy miembro de alguna organización, club, o tengo vínculos con personas que puedan verse afectadas o beneficiadas con el resultado de la decisión que me corresponde adoptar sobre el asunto?
- ¿Podría haber en el futuro beneficios personales para mí o alguien vinculado/a a mí, por la decisión en la que participaré, que puedan generar duda sobre mi objetividad?

6.5. COMPROMISOS Y RESPONSABILIDADES PERSONALES

6.5.1. Los/as servidores/as del Ositrán estamos comprometidos a realizar nuestras labores con diligencia, honradez, profesionalismo, imparcialidad, transparencia e integridad.

6.5.2. Nos comprometemos, a actuar en todo momento acorde a lo dispuesto en las leyes, reglamentos y toda disposición de índole legal y administrativa emitida, ya sean éstas de alcance nacional o interna.

6.5.3. Nos comprometemos a compartir información veraz y a rendir cuentas a nuestros clientes internos, externos y a la sociedad, en todo momento, de nuestro trabajo y decisiones para mantener confianza y credibilidad en nuestra labor y funciones.

6.5.4. Nos comprometemos a leer y comprender el contenido del Código de Conducta y Ética del Ositrán; así como, actuar conforme los comportamientos deseados.

6.5.5. Nos comprometemos a no solicitar o aceptar cualquier regalo o dádiva que encierre un valor monetario, a menos que este código u otra norma de alcance nacional o interno prevean una excepción, o que se trate de algún souvenir o artículo publicitario, cuyo valor no represente suma de dinero excesivo.

6.5.6. Nos comprometemos y somos responsables de no participar en transacciones financieras que estén en conflicto o colisionen con el escrupuloso cumplimiento de nuestros deberes.

6.5.7. Nos comprometemos a tratar a nuestros compañeros/as de trabajo y a nuestros/as usuarios/as o cualquier otra persona con la que tengamos relación en el cumplimiento de nuestras funciones, de manera profesional, con cortesía, sin discriminar, debiendo siempre cuidar de tener un trato igualitario, valorando la diversidad, la pluralidad de opiniones, creencias, no toleramos ningún tipo de acción discriminatoria; y, no incurrimos en actos de acoso sexual, laboral u otro.

6.5.8. Nos comprometemos a utilizar de manera correcta los recursos públicos que nos fueran asignados en el cumplimiento de nuestras funciones, sin incurrir en actos deshonestos, antiéticos y contrarios a la integridad.

6.5.9. Nos comprometemos a no divulgar ni utilizar la información confidencial obtenida durante el ejercicio de nuestras funciones, en beneficio propio o de terceros.

VII. DISPOSICIONES ESPECÍFICAS

7.1. PRINCIPIOS

Los/as servidores/as del Ositrán tienen la obligación de actuar bajo los Principios de la Función Pública establecidos en la Ley del Código de Ética de la Función Pública y los principios que orientan la integridad pública[3], los cuales se detallan a continuación:

a. **Respeto**: Adecúan su conducta hacia el respeto de la Constitución y las leyes, garantizando que en todas las fases del proceso de toma de decisiones o en el cumplimiento de los procedimientos administrativos, se respeten los derechos a la defensa y al debido procedimiento.

   Comportamiento esperado:

   - Conocer, cumplir y aplicar debidamente las disposiciones legales y normativas vigentes, en el cumplimiento de nuestras funciones como servidores públicos.
   - Fomentar el trabajo en equipo y tratar con respeto, sin acosar sexualmente y sin discriminación de ninguna índole a nuestros compañeros/as de trabajo, directivos, usuarios/as u otros, según corresponda.
   - Si un/a servidor/a que atiende en mesa de partes tiene enemistad con un usuario; tiene la obligación de atender con respeto al usuario en cumplimiento de sus funciones y normas, sin importar su afinidad con él/ella.

b. **Probidad**: Actúan con rectitud, honradez y honestidad, procurando satisfacer el interés general y desechando todo provecho o ventaja personal, obtenido por sí o por interpósita persona.

   Comportamiento esperado:

   - Actuar en todo momento con objetividad y basado en los principios de igualdad, meritocracia, transparencia en las evaluaciones de procesos que nos asignen, motivando debidamente nuestras decisiones.
   - Cumplir con las tareas y responsabilidades asignadas (por ejemplo, los horarios que la entidad establezca) independientemente de la modalidad de prestación laboral en la que nos encontremos; así como con los demás compromisos dispuestos por el Ositrán.

---

[3] Artículo 2° del Decreto Supremo N° 042-2018-PCM, Decreto Supremo que establece medidas para fortalecer la integridad pública y lucha contra la corrupción.

- Utilizar los recursos y herramientas proporcionadas por la entidad, solo para el cumplimiento de nuestras funciones.
- Un/a servidor/a que percibe viáticos para una comisión de servicios, debe reintegrar el monto no utilizado en dicha comisión, rindiendo cuentas claras, sustentadas y en la oportunidad establecida en el procedimiento.

c. **Eficiencia**: Brindan calidad en cada una de las funciones a su cargo, procurando obtener una capacitación sólida y permanente.

Comportamiento esperado:

- Presentar dentro de los plazos establecidos, la documentación, evaluación o información requerida a fin de cumplir con lo solicitado.
- Un/a servidor/a del Ositrán debe aprovechar al máximo las actividades de capacitación brindadas por la entidad, lo cual se verá reflejada en la mejora en el cumplimiento de sus labores, lo que redundará en beneficio de nuestros/as usuarios/as.
- El/la servidor/a de Logística debe observar las exigencias y plazos establecidos en la norma para la contratación de bienes y servicios, de modo que garantice una correcta adjudicación en los plazos, evitando incurrir en causales de nulidad u otros similares.

d. **Idoneidad**: Entendida como aptitud técnica, legal y moral, es condición esencial para el acceso y ejercicio de la función pública. Los/as servidores/as del Ositrán deben propender a una formación sólida acorde a la realidad, capacitándose permanentemente para el debido cumplimiento de sus funciones.

Comportamiento esperado:

- Los/as servidores/as del Ositrán deben actualizarse y mantener vigentes sus conocimientos, a fin de desarrollar idóneamente sus funciones.
- Encontrarnos siempre predispuestos a cambios, respecto a métodos de trabajo y procedimientos, en pro de una mejora continua.
- El/la servidor/a a cargo de la ejecución del Plan de Desarrollo de Personas (PDP) de la entidad debe cumplir obligatoriamente con lo programado por la entidad, y con aquellas otras capacitaciones que son necesarias para el óptimo desempeño de los puestos.

e. **Veracidad**: Se expresan con autenticidad en las relaciones funcionales de quienes integran la institución y con la ciudadanía, y contribuye al esclarecimiento de los hechos.

Comportamiento esperado:

- Indagar, recopilar e investigar concienzudamente, a través de la información y documentación obtenida, a fin de consignar en los documentos que formulamos, decisiones basadas en sustentos auténticos y confiables.

- El/la servidor/a debe consignar información veraz, fidedigna e íntegra en su Declaración Jurada de Intereses, según lo requerido en la normativa sobre la materia.

f. **Lealtad y obediencia**: Actúan con fidelidad y solidaridad hacia todos los miembros de su institución, cumpliendo las órdenes que le imparta el superior jerárquico competente, en la medida que reúnan las formalidades del caso y tengan por objeto la realización de actos de servicio que se vinculen con las funciones a su cargo, salvo los supuestos de arbitrariedad o ilegalidad manifiesta, los cuales deberán poner en conocimiento del/la superior jerárquico de la entidad.

Comportamiento esperado:

- Cumplir con las órdenes impartidas por nuestros superiores jerárquicos, a fin de lograr las metas y objetivos de la unidad de organización y, por ende, de la entidad.
- El/la servidor/a debe denunciar cualquier orden o mandato que reciba de su superior o invitación de algún/a compañero/a de trabajo o usuario, de realizar algún acto contrario al ordenamiento jurídico.
- Los/as servidores/as del Ositrán no deben tomar decisiones sin encontrarse facultados para hacerlo o no contar con la autorización correspondiente.

g. **Justicia y equidad**: Tienen permanente disposición para el cumplimiento de sus funciones, otorgando a cada uno lo que le es debido, actuando con equidad en sus relaciones con el Estado, con el administrado, con sus superiores, con sus subordinados y con la ciudadanía en general.

Comportamiento esperado:

- Los/as servidores/as del Ositrán, en el cumplimiento de sus funciones, no deben tener preferencias u otorgar beneficios o privilegios que no correspondan a personas, empresas o instituciones.
- Los miembros de los comités de selección deben de realizar la evaluación de los perfiles y los requisitos mínimos según lo establecido en la convocatoria, considerando los principios de mérito, transparencia e igualdad de oportunidades.
- Un/a servidor/a de la Jefatura de Fiscalización debe recomendar la interposición de sanción a aquella concesionaria que no cumpla con alguno de los compromisos dispuestos en los contratos, aun cuando mantenga alguna relación de amistad o afinidad con algún socio o propietario o directivo de la empresa.

h. **Lealtad al Estado de Derecho**: El funcionario de confianza debe lealtad a la Constitución y al Estado de Derecho. Ocupar cargos de confianza en regímenes de facto, es causal de cese automático e inmediato de la función pública.

Comportamiento esperado:

- Inducir y promover el respeto por el Estado de Derecho y la institucionalidad del país.
- Un/a servidor/a con cargo de confianza, debe actuar cumpliendo sus funciones en beneficio de la entidad y con lealtad a la Constitución, las leyes y al Estado de Derecho.

7.2. DEBERES

Los/as servidores/as del Ositrán cumplen los deberes establecidos en la Ley del Código de Ética de la Función Pública, los cuales se detallan a continuación:

a) **Neutralidad**: Deben actuar con absoluta imparcialidad política, económica o de cualquier otra índole en el desempeño de sus funciones demostrando independencia en sus vinculaciones con personas, partidos políticos o instituciones.

Comportamiento esperado:

- Los/as servidores/as de la entidad con capacidad de decisión, deberán cumplir con sus funciones basados en la honestidad, equidad, imparcialidad, objetividad y transparencia, debiendo motivar correctamente sus decisiones.
- El/la servidor/a del Ositrán, no debe aprovechar su estatus o cargo para favorecer el ingreso a la entidad o la contratación, de familiares o amigos, en detrimento de las normas que regulan la contratación de personal, y de las normas establecidas relacionadas al nepotismo. Nuestro accionar está basado en la búsqueda del bien común, salvaguardando el interés general.

b) **Transparencia**: Debemos ejecutar los actos del servicio de manera transparente, ello implica que dichos actos tienen en principio carácter público y son accesibles al conocimiento de toda persona natural o jurídica. Los/as servidores/as del Ositrán deben brindar y facilitar información fidedigna, completa y oportuna.

Comportamiento esperado:

- Todoslos servidores/as del Ositrán,debemos desempeñar nuestras funciones con transparencia.
- El/la servidor/a del Ositrán no induce o persuade a otro/a servidor/a a cargo de la toma de alguna decisión, a fin de que lo haga a favor de algún familiar, amigo o conocido, aun cuando no le alcance el beneficio por no corresponderle o por no cumplir con los requisitos establecidos.
- El/la servidor/a a cargo de la atención de solicitudes de acceso a la información pública deberá atenderlas dentro de los plazos fijados por norma, garantizando, cuando se trate de una denegatoria, que ésta se encuentre debidamente fundamentada.

c) **Discreción**: Deben guardar reserva respecto de hechos o informaciones de los que tengan conocimiento con motivo o en ocasión del ejercicio de sus funciones, sin perjuicio de los deberes y las responsabilidades que le correspondan en virtud de las normas que regulan el acceso y la transparencia de la información pública.

Comportamiento esperado:

- Los/as servidores/as del Ositrán cumplen con las normas dispuestas respecto a la protección de datos personales, tanto de sus compañeros de labores como de la ciudadanía en general.
- Cumplimos con resguardar la información con la que contamos en el cumplimiento de nuestras funciones cuando tengan carácter de confidencialidad o de reserva.
- El/la servidor/a que labora en la Secretaría Técnica de Procedimientos Administrativos Disciplinarios deberá guardar la debida reserva de la información a que hubiere tenido acceso a mérito de una investigación sobre presuntas faltas administrativas de un/a servidor/a.

d) **Ejercicio adecuado del cargo**: Con motivo o en ocasión del ejercicio de sus funciones los/as servidores/as del Ositrán no deben adoptar represalia de ningún tipo o ejercer coacción alguna contra otros/as servidores/as civiles u otras personas.

Comportamiento esperado:

- Los/as servidores/as del Ositrán debemos garantizar que, en el cumplimiento de nuestras funciones y la relación laboral con nuestros/as compañeros/as de trabajo, no exista ningún acto de discriminación, abuso o amenaza, teniendo siempre por prerrogativa, la inclusión, igualdad de género, de trato y el respeto a la diversidad.
- Debemos propiciar que nuestro entorno laboral, se encuentre libre de violencia, acoso físico, laboral, sexual, psicológico.
- Un/a jefe/a, debe ejercer sus funciones con total rectitud hacia todo su personal a cargo, aunque tenga conocimiento que lo han denunciado por temas que son a todas luces infundados.

e) **Uso adecuado de los bienes del Estado**: Deben proteger y conservar los bienes del Estado, utilizando los que le fueran asignados para el desempeño de sus funciones de manera racional, evitando su abuso, derroche o desaprovechamiento, sin emplear o permitir que otros empleen los bienes del Estado para fines particulares o propósitos que no sean aquellos para los cuales hubieran sido específicamente destinados.

Comportamiento esperado:

- Los/as servidores/as del Ositrán debemos cumplir y respetar las disposiciones establecidas para el uso y utilización de los recursos que nos asignan para el cumplimiento de nuestras funciones.
- No debemos utilizar los bienes asignados para fines políticos o de otra índole.

- Un/a servidor/a debe dar el uso adecuado a la movilidad que le ha sido asignada para el cumplimiento de sus funciones o para actividades oficiales.

f) **Responsabilidad**: Deben desarrollar sus funciones a cabalidad y en forma integral, asumiendo con pleno respeto su función pública. Ante situaciones extraordinarias, los/as servidores/as del Ositrán pueden realizar aquellas tareas que por su naturaleza o modalidad no sean las estrictamente inherentes a su cargo, siempre que ellas resulten necesarias para mitigar, neutralizar o superar las dificultades que se enfrenten.

Comportamiento esperado:

- El/la servidor/a debe cumplir con las tareas asignadas dentro de los plazos establecidos por el/la superior jerárquico.
- Debemos garantizar el respeto a los derechos de los usuarios en el ejercicio de nuestras funciones.
- Debemos emitir de manera oportuna y sustentada cualquier decisión que corresponda a la entidad, con total responsabilidad, basada en los hechos advertidos y la normatividad vigente.
- Asimismo, todos los/as servidores/as del Ositrán deben respetar los derechos de los administrados establecidos en el artículo 66° del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por el Decreto Supremo N° 004-2019-JUS.

7.3. PROHIBICIONES

Los/as servidores/as del Ositrán se encuentran prohibidos de incurrir en los supuestos establecidos en la Ley del Código de Ética que se detallan a continuación:

a) **Mantener intereses de conflicto:** Mantener relaciones o aceptar situaciones en cuyo contexto sus intereses personales, laborales, económicos o financieros pudieran estar en conflicto con el cumplimiento de los deberes y funciones a su cargo.

Comportamiento esperado:

- Un/a servidor/a, que es miembro de un comité de selección para la contratación de un servicio de supervisión de obra, cuyo familiar o amigo cercano es propietario de una de las empresas que se presentan a un concurso público convocado por la entidad, debe abstenerse de participar en el proceso.

- Nuestro actuar se encuentra basado en el bien común, desterrando cualquier acción que, evidentemente tenga un contexto de satisfacción de intereses personales u orientado a favorecer a algún particular.

b) **Obtener ventajas indebidas (soborno u otro acto de corrupción):** Obtener o procurar beneficios o ventajas indebidas, de cualquier tipo, para sí o para otros, mediante el uso de su cargo, autoridad, influencia o apariencia de influencia.

Asimismo, queda expresamente prohibido a los/as servidores/as del Ositrán aceptar algún tipo de regalo, atención, donación o beneficios similares (con excepción de merchandising) que se preste a dudas sobre la probidad del servidor civil en el desarrollo de sus funciones.

Ejemplo: El/la servidor/a de la entidad debe rechazar cualquier tipo de presente, agasajo, abono, invitación o reconocimiento de alguna persona o empresa que desea prestar o presta servicios o vende bienes a la entidad y que participa de un procedimiento de contratación, salvo que se trate solo de merchandising, como lápices, lapiceros de menor valor, agendas comunes, llaveros, cuadernos o block, folder o file, almanaques o calendarios, planners u otros, cuyo valor sea básico o mínimo.

c) **Realizar actividades de proselitismo político:** A través de la utilización de sus funciones o por medio de la utilización de infraestructura, bienes o recursos públicos, ya sea a favor o en contra de partidos u organizaciones políticas o candidatos.

Ejemplo: El/la servidor/a, cuida que, en los bienes de la entidad o los asignados a su persona para el cumplimiento de su función, no se incorporen lemas o logos, ni se induzca de manera directa o indirecta a intereses electorales de algún partido o candidato.

d) **Hacer mal uso de información privilegiada:** Participar en transacciones u operaciones financieras utilizando información privilegiada del Ositrán o que pudiera tener acceso a ella por su condición o ejercicio del cargo que desempeña, ni debe permitir el uso impropio de dicha información para el beneficio de algún interés.

Ejemplo: El/la servidor/a del Ositrán suscribe Declaración Jurada comprometiéndose a guardar la reserva sobre la información a la que tiene acceso en cumplimiento de sus funciones o como parte de la entidad.

e) **Presionar, amenazar y/o acosar:** Ejercer presiones, amenazas o acoso sexual contra otros/as servidores/as civiles o subordinados que puedan afectar la dignidad de la persona o inducir a la realización de acciones dolosas.

Ejemplo: El/la servidor/a de la entidad que ostente un cargo de jefe o similar, llamará la atención a su personal a cargo, observando los defectos de su actuación técnica o profesional, procurando la mejora de sus capacidades, sin utilizar términos o frases denigrantes o calificativos similares en su contra.

7.4. **Asimismo, queda prohibido perseguir, acosar o discriminar a servidores/as civiles de la entidad** por reportar y/o denunciar algún acto de corrupción, o actos en contra de lo dispuesto en el presente Código de Conducta y Ética, la Ley del

Código de Ética, en contra de las disposiciones aprobadas por el Ositrán respecto del Sistema de Gestión Antisoborno, y la Política Nacional de Integridad y Lucha contra la Corrupción, así como los relacionados a las normas de igualdad de género, hostigamiento sexual u otros.

7.5. La transgresión de los principios, deberes y de las prohibiciones establecidas en el presente documento, la Ley del Código de Ética de la Función Pública y demás normas concordantes, constituyen infracciones que serán procesadas conforme al procedimiento disciplinario establecido por la Ley N° 30057, Ley del Servicio Civil, su Reglamento, la Directiva N° 02-2015-SERVIR/GPGSC y aquellas normas que las sustituyan o complementen.

VIII. DIFUSIÓN DEL CÓDIGO DE CONDUCTA Y ÉTICA DE LOS SERVIDORES DEL OSITRÁN

La Oficina de Integridad Institucional o la que haga sus veces difunde y promueve el Código de Conducta y Ética de los servidores del Ositrán, así como la Ley del Código de Ética de la Función Pública, las disposiciones aprobadas por el Ositrán respecto del Sistema de Gestión Antisoborno y la Política Nacional de Integridad y Lucha contra la Corrupción al interior del Ositrán.

IX. CONSECUENCIAS DEL INCUMPLIMIENTO DE LOS PRINCIPIOS, DEBERES Y PROHIBICIONES ESTABLECIDOS EN EL CÓDIGO DE CONDUCTA Y ÉTICA DE LOS SERVIDORES DEL OSITRÁN

De conformidad con la normativa en materia de Servicio Civil, el incumplimiento de los principios, deberes, así como la infracción respecto de las prohibiciones señaladas en los numerales anteriores, constituirán infracciones de conformidad con lo previsto en el artículo 100° del Reglamento de la Ley N° 30057[4] y serán pasibles de la aplicación de sanción de conformidad con el artículo 88°[5] de dicha ley y de las demás normas, según corresponda.

---

[4] Artículo 100.- Falta por incumplimiento de la Ley N° 27444 y de la Ley N°27815. También constituyen faltas para efectos de la responsabilidad administrativa disciplinaria aquellas previstas en los artículos 11.3, 12.3, 14.3, 36.2, 38.2, 48 numerales 4 y 7, 49, 55.12, 91.2, 143.1, 143.2, 146, 153.4, 174.1, 182.4, 188.4, 233.3 y 239 de la Ley N° 27444, Ley del Procedimiento Administrativo General y en las previstas en la Ley N°27815, las cuales se procesan conforme a las reglas procedimentales del presente título".

[5] Artículo 88. Sanciones aplicables
Las sanciones por faltas disciplinarias pueden ser:
a) Amonestación verbal o escrita.
b) Suspensión sin goce de remuneraciones desde un día hasta por doce (12) meses.
c) Destitución.
Toda sanción impuesta al servidor debe constar en el legajo

Asimismo, si cualquier conducta inapropiada se constituye en un presunto delito, el Ositrán deberá informar a las autoridades pertinentes.

X. DISPOSICIONES ESPECÍFICAS

10.1. De las actividades de promoción y difusión

10.1.1. La Oficina de Integridad Institucional o la que haga sus veces, a fin de promover y difundir el Código de Conducta y Ética de los/as servidores/as del Ositrán, así como la Ley del Código de Ética de la Función Pública, las disposiciones aprobadas por el Ositrán respecto del Sistema de Gestión Antisoborno, y la Política Nacional de Integridad y Lucha contra la Corrupción, llevará a cabo, entre otras, las siguientes actividades:

a) Difundir con regular frecuencia el contenido del presente Código, así como principales contenidos de la Ley del Código de Ética de la Función Pública y otras normas relacionadas a la ética e integridad; asimismo, publicará el contenido en los paneles y en zonas visibles de la entidad, lo cual se verificará periódicamente.

b) Consignar en el enlace del portal institucional de Ositrán denominado Integridad y Ética, el contenido del presente documento, así como la Ley del Código de Ética de la Función Pública y su Reglamento, y demás normas sobre la materia.

c) Desarrollar jornadas informativas y de socialización y concientización sobre la importancia de las normas éticas, de integridad y demás relacionadas, y sobre las sanciones que acarrea su incumplimiento.

d) Ejecutar en el Ositrán, las medidas que correspondan para promover la cultura de ética e integridad en el servicio público.

e) Fomentar que las personas reporten, de buena fe o sobre la base de una creencia razonable, el intento o ejecución de algún acto de corrupción o soborno, de alguna falta contra la ética e integridad, supuesto y real, que se constituya en violación de la política de integridad del Ositrán y política antisoborno o cualquier incumplimiento o debilidad en el Sistema de Gestión Antisoborno, en contra de la Ley del Código de Ética o de la Política Nacional de Integridad y Lucha contra la Corrupción.

f) Difundir la existencia de la Plataforma Digital Única de Denuncias del Ciudadano, así como los canales establecidos por el Ositrán para reportar o denunciar los actos de corrupción, hechos o incidencias en contra de la Ley del Código de Ética de la Función Pública, en contra de las disposiciones aprobadas por el Ositrán respecto del Sistema de Gestión Antisoborno o de la Política Nacional de Integridad y Lucha contra la Corrupción, respecto de los cuales el Ositrán se compromete a prohibir

represalias y proteger a las personas que realicen reportes de buena fe y a que las investigaciones se hagan de manera confidencial y reservada.

10.2. Incentivos y estímulos

10.2.1. La Presidencia Ejecutiva o la Gerencia General cuando corresponda, otorgará un reconocimiento a los/as servidores/as del Ositrán que se destaquen en el cumplimiento de los principios, deberes y respeten las prohibiciones de la Ley del Código de Ética de la Función Pública y las que se establecen en el presente Código de Conducta y otras que tengan relación con las normas antisoborno y de integridad. Dicho reconocimiento estará acorde a lo dispuesto en los Lineamientos del Programa de reconocimiento al personal del Ositrán.

10.2.2. Los/as servidores/as del Ositrán que sean reconocidos/as, serán beneficiados/as con los siguientes incentivos y/o estímulos:

a) El reconocimiento público (Laurel, Medalla o Diploma del Ositrán) o por escrito, el cual formará parte de su legajo personal, y será entregado en una ceremonia con la participación del personal del Ositrán.
b) Los demás que la Presidencia Ejecutiva o Gerencia General consideren conveniente aplicar.

10.3. Para el caso de nuestros proveedores, contratistas, concesionarios, empresas supervisoras, consultores y otros relacionados

10.3.1. Al Ositrán le interesa relacionarse y contratar con personas naturales o jurídicas que mantengan prácticas honestas y transparentes y que puedan demostrarlo con su rectitud en el actuar; para ello, se han establecido cláusulas anticorrupción en los contratos relacionados con el comportamiento ético y solvente, exigiéndoles el compromiso de combatir y prevenir la corrupción en todas sus modalidades, y solicitándoles la implementación de controles relacionados con la formación y concientización anticorrupción en su personal.

10.3.2. Respecto de los Concesionarios, se afianzará una lucha mancomunada contra la corrupción, a través de la firma de un Compromiso Ético y de Anticorrupción.

XI. RESPONSABILIDAD

a) Es responsabilidad de la Gerencia General y de la Jefatura de Gestión de Recursos Humanos, como encargada de la función de integridad, realizar las acciones necesarias para la supervisión del cumplimiento de lo dispuesto en el presente Código de Conducta y Ética, así como su difusión.

b) Todo lo establecido en el presente documento, es de obligatorio cumplimiento por parte de todos/as los/as servidores/as del Ositrán.

XII. DISPOSICIÓN FINAL

Si bien las disposiciones del presente Código no le son aplicables a los miembros de los Consejos de Usuarios, así como tampoco a los Supervisores contratados en virtud de la facultad establecida en la Ley N° 26917[6], toda vez que no califican

---

[6] Empresas Supervisoras

Ley N° 26971

"DISPOSICIONES COMPLEMENTARIAS, TRANSITORIAS Y FINALES (...)

Tercera. - Mecanismos de Fiscalización de OSITRAN

Las funciones de fiscalización atribuidas por el Capítulo II de la presente Ley a OSITRAN podrán ser ejercidas a través de Empresas Fiscalizadoras. Dichas Empresas son personas naturales o jurídicas, debidamente calificadas y clasificadas por OSITRAN. La contratación de las mismas se realizará respetando los principios de igualdad, no discriminación y libre concurrencia. Mediante Decreto Supremo refrendado por el Ministro de Transportes, Comunicaciones, Vivienda y Construcción se establecerán los criterios y procedimientos para la calificación, designación y ejecución de las tareas de fiscalización que realizarán dichas empresas. Para efecto de lo establecido en el Artículo 425 del Código Penal, los funcionarios responsables de los informes que emitan las Empresas Fiscalizadoras, así como los representantes legales de las mismas, serán considerados como funcionarios públicos".

Reglamento General del OSITRAN

"Artículo 26.- Trámite de las denuncias presentadas contra terceros por las actividades de supervisión

Las denuncias que se presenten contra las personas naturales o jurídicas por la realización de sus actividades de supervisión, conforme lo señala el artículo 25 del presente Reglamento, así como los incumplimientos detectados por el OSITRAN, se tramitarán conforme al procedimiento y plazos que establezca la Directiva de Procedimientos Administrativos y otras directivas que apruebe el Consejo Directivo".

Consejos de Usuarios

Reglamento de la Ley Marco de los Organismos Reguladores-Decreto Supremo N°042-2005-PCM

"Artículo 16.- Duración del mandato y vacancia

Los miembros de los Consejos de Usuarios se eligen democráticamente por período de dos (2) años renovables.

El cargo de miembro de Consejo de Usuarios vaca por las siguientes causales:

(---)

iv) Remoción ordenada por el Consejo Directivo por falta grave del miembro del Consejo de Usuarios, aplicándosele las faltas descritas en el artículo 12 del presente Reglamento, previo procedimiento (...)".

"Artículo 12.- Falta Grave

Para efectos de la aplicación de la remoción prevista en el numeral 6.4 y en el literal e) del numeral 6.6. del Artículo 6 de la Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos, constituyen faltas graves:

(...)

b) La obtención o procuración de beneficios o ventajas indebidas, para sí o para otros, mediante el uso de su cargo, autoridad o influencia.

recursos públicos, ya sea a favor o en contra de partidos u organizaciones políticas o candidatos (...)".

Reglamento de Funcionamiento de Consejos de Usuarios de OSITRAN, aprobado mediante Resolución de Consejo Directivo N° 022-2016-CD- OSITRAN

"Artículo 20.- Incompatibilidad

Los miembros de los Consejos de Usuarios, en ningún caso podrán:

a) Tener vinculación con las Entidades Prestadoras, bajo el ámbito de competencia de OSITRAN conforme a lo dispuesto por el artículo 17 del presente Reglamento.

b) Tener vinculación con el Ministerio de Transportes y Comunicaciones, conforme a lo dispuesto con el artículo 18 del presente Reglamento.

como funcionarios/as o servidores/as públicos, los mismos se ceñirán a las disposiciones que en materia de ética e integridad disponga el Reglamento de Funcionamiento de Consejos de Usuarios de Ositrán, así como los Contratos de Supervisión, respectivamente.

---

c) Tener vinculación con OSITRAN, conforme a lo dispuesto con el artículo 18 del Reglamento del presente Reglamento".

RESOLUCION DE PRESIDENCIA

N° 0013-2020-PD-OSITRAN

Lima, 26 de mayo de 2020

VISTOS:

El Informe N° 048-2020-JGRH-GA-OSITRAN de la Jefatura de Gestión de Recursos Humanos; el Informe N° 0051-2020-GPP-OSITRAN de la Gerencia de Planeamiento y Presupuesto; el Memorando N° 0171-2020-GAJ-OSITRAN de la Gerencia de Asesoría Jurídica y el Memorando de Gerencia General N° 154-2020-GG-OSITRAN;

CONSIDERANDO:

Que, mediante Ley N° 26917, Ley de Supervisión de la Inversión Privada en Infraestructura de Transporte de Uso Público y sus modificatorias, se creó el Organismo Supervisor de la Inversión en Infraestructura de Transporte de Uso Público – OSITRAN, como organismo público encargado de normar, regular, supervisar, fiscalizar y resolver controversias respecto de los mercados relativos a la explotación de la infraestructura de transporte de uso público;

Que, la Ley N° 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los servicios públicos y sus modificatorias, dicta los lineamientos y normas de aplicación general para los Organismos Reguladores, encontrándose incluido dentro de sus alcances el Ositrán;

Que, la Ley N° 29754, dispone que el Ositrán es la entidad competente para ejercer la supervisión de los servicios públicos de transporte ferroviario de pasajeros en las vías concesionadas que forman parte del Sistema Eléctrico de Transporte Masivo de Lima y Callao; asimismo, establece que, mediante decreto supremo refrendado por el presidente del Consejo de Ministros, a propuesta del Ositrán, se aprueba la adecuación del Reglamento General del Ositrán y otros documentos de gestión;

Que, de acuerdo con el artículo 6°del citado reglamento, aprobado por Decreto Supremo N° 044-2006-PCM y sus modificatorias, la estructura orgánica del OSITRAN se rige por su Reglamento de Organización y Funciones;

Que, por Decreto Supremo N° 012-2015-PCM se aprobó el Reglamento de Organización y Funciones – ROF del Ositrán, con el fin de implementar las funciones establecidas por la Ley N° 29754 y las instancias y órganos competentes, conforme lo señala el Reglamento General de OSITRAN, así como para promover una gestión eficiente, moderna, transparente y con enfoque de procesos y para resultados, cuyas decisiones institucionales sean predecibles;

Que, de acuerdo con lo señalado en el numeral 3 del artículo 9° del ROF del OSITRAN, son funciones de la Presidencia Ejecutiva aprobar políticas y planes de administración, de recursos humanos, finanzas, así como de estrategias comunicacionales y de relaciones institucionales, a propuesta de la Gerencia General, en concordancia con la normativa de la materia;

Que, la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, establece que el proceso de modernización de la gestión del Estado tiene como finalidad fundamental la obtención de mayores niveles de eficiencia del aparato estatal, de manera que se logre una mejor atención a la ciudadanía, priorizando y optimizando el uso de los recursos públicos, con el objetivo de alcanzar un Estado al servicio de la ciudadanía y transparente en su gestión, entre otros;

Que, mediante Decreto Supremo N° 092-2017-PCM se aprobó la Política Nacional de Integridad y Lucha contra la Corrupción cuyo objetivo general es dotar al Estado Peruano, de

OSITRAN
EL REGULADOR DE LA INFRAESTRUCTURA DE TRANSPORTE DE USO PÚBLICO
Calle Los Negocios 182, piso 2
Surquillo - Lima
Central Telefónica: (01) 500-9330
www.ositran.gob.pe

mecanismos que garanticen la prevención y sanción frente a actos de corrupción, la identificación y gestión de riesgos y la capacidad sancionadora del Estado frente a los actos de corrupción, de modo que se propicie el mejoramiento continuo de las instituciones, corrigiendo aquellas fallas del sistema que aprovecha la corrupción;

Que, mediante Decreto Supremo Nº 044-2018-PCM, se aprobó el Plan Nacional de Integridad y Lucha contra la Corrupción 2018 - 2021, que establece las acciones priorizadas que sobre la materia se deben emprender para prevenir y combatir la corrupción e impulsar la integridad pública, en el marco de la Política Nacional de Integridad y Lucha contra la Corrupción;

Que, mediante Resolución de Secretaría de Integridad Pública N° 001-2019-PCM/SIP, se aprobó la Directiva "Lineamientos para la implementación de la función de integridad en las entidades de la Administración Pública", por la que se aprueban los Lineamientos para la implementación de la función de integridad en las entidades de la administración pública;

Que, mediante Resolución de Gerencia General N° 121-2018-GG-OSITRAN modificada por Resolución de Gerencia General Nº 132-2019-GG-OSITRAN y Resolución de Gerencia General Nº 010-2020-GG-OSITRAN, la Gerencia General, en su calidad de máxima autoridad administrativa del Ositrán, delegó las funciones de integridad institucional a la Jefatura de Gestión de Recursos Humanos; por ello, dicha Jefatura mediante Informe N° 048-2020-JGRH-GA-OSITRAN del 7 de febrero del 2020, sustenta la necesidad de la aprobación de una Política de Integridad del Ositrán, proponiéndola en el marco de la implementación de la Política Nacional de Integridad y Lucha contra la Corrupción en la entidad y como una buena práctica;

Que, la Gerencia de Planeamiento y Presupuesto a través del Informe N° 051-2020-GPP-OSITRAN del 23 de abril de 2020, emitió opinión favorable respecto de la propuesta presentada por la Jefatura de Gestión de Recursos Humanos;

Que, a través del Memorando N° 0171-2020-GAJ-OSITRAN del 21 de mayo de 2020, la Gerencia de Asesoría Jurídica considera viable continuar con la tramitación para la aprobación de la Política de Integridad del Ositrán.

Que, mediante Memorando Nº 154-2020-GG-OSITRAN, la Gerencia General expresó que el proyecto de resolución de presidencia cuenta con su conformidad y lo remitió visado para la suscripción correspondiente;

Que, estando a lo propuesto, y a mérito de lo establecido en el Decreto Supremo N° 092-2017-PCM, que aprobó la Política Nacional de Integridad y Lucha contra la Corrupción; Decreto Supremo Nº 044-2018-PCM, que aprobó el Plan Nacional de Integridad y Lucha contra la Corrupción 2018 – 2021; Decreto Supremo N° 012-2015-PCM y modificatoria, Reglamento de Organización y Funciones del OSITRAN;

SE RESUELVE:

Articulo 1.- Aprobar la Política de Integridad del Ositrán, el mismo que como anexo forma parte integrante de la presente resolución.

Articulo 2.- Notificar la presente resolución a todas las unidades de organización que conforman el Ositrán, para conocimiento, difusión y aplicación.

Articulo 3.- Publicar la presente resolución y su anexo en el portal institucional de la entidad (www.ositran.gob.pe).

Regístrese y comuníquese

VERÓNICA ZAMBRANO COPELLO
Presidenta del Consejo Directivo

NT: 2020035303

OSITRAN
EL REGULADOR DE LA INFRAESTRUCTURA DE TRANSPORTE DE USO PÚBLICO

Calle Los Negocios 182, piso 2
Surquillo - Lima
Central Telefónica: (01) 500-9330
www.ositran.gob.pe

OSITRAN

POLÍTICA DE INTEGRIDAD DEL OSITRAN

En el Organismo Supervisor de la Inversión Privada en Infraestructura de Transporte de Uso Público - OSITRÁN, brindamos un servicio en favor del bienestar de la ciudadanía, garantizando a través de nuestra intervención, el funcionamiento eficiente de la infraestructura de transporte de uso público, el servicio de transporte de pasajeros del Metro de Lima y Callao y la calidad del servicio a los usuarios, empresas concesionarias y al Estado.

Por ello, la Alta Dirección y todos sus servidores expresan su voluntad y compromiso de:

- ✓ Cumplir con la Política Nacional de Integridad, a través de la implementación efectiva del Sistema de Control Interno, la Promoción de la Transparencia y el Acceso a la Información Pública, el adecuado funcionamiento de los canales de denuncias garantizándose una investigación imparcial y sanciones oportunas, brindando las medidas de protección; además de mostrar un comportamiento personal ejemplar y un alto nivel de decoro en el desempeño de sus funciones acorde a las medidas de comportamiento ético, nuestra política del Sistema de Gestión Antisoborno y demás normas.

- ✓ Priorizar la identificación y la gestión de riesgos, a fin de evitar conflictos de interés, el uso inadecuado de recursos y la gestión indebida de intereses, esto para evitar infracciones a las normas de integridad pública.

- ✓ Dotar al responsable de la función de integridad del empoderamiento al más alto nivel para el monitoreo y supervisión de las políticas de integridad y de todos los componentes del sistema.

- ✓ Exhortar a nuestros proveedores y empresas concesionarias, como una responsabilidad compartida, para que respeten nuestros valores y normas en todas las interacciones con nuestros servidores, comprometiéndolos a no incurrir en algún acto, ofrecimiento u otro que se constituya en acto de corrupción o similar.

Versión 1, aprobada mediante Resolución N° 0013-2020-PD-OSITRAN de fecha 26.05.2020

OSITRAN
EL REGULADOR DE LA INFRAESTRUCTURA DE TRANSPORTE DE USO PÚBLICO

Calle Los Negocios 182, piso 2
Surquillo - Lima
Central Telefónica: (01) 500-9330
www.ositran.gob.pe

Firmado por: ZAMBRANO COPELLO Rosa Veronica FAU 20420248645 hard
Motivo: Firma Digital
Fecha: 11/09/2019 17:43:59 -0500

OSITRAN
EL REGULADOR DE LA INFRAESTRUCTURA DE TRANSPORTE DE USO PÚBLICO

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

OSITRAN en cumplimiento de su misión, visión y valores y comprometido con la mejora continua de sus procesos, mantiene un SGSI (Sistema de Gestión de Seguridad de la Información) para coadyuvar al funcionamiento eficiente de los mercados de infraestructura de transporte de uso público (ITUP), del servicio de transporte de pasajeros del Metro de Lima y Callao, y su calidad en beneficio de los usuarios, las empresas concesionarias y el Estado. En tal sentido, manifiesta su compromiso de:

- Proteger los activos de información con la finalidad de preservar la confidencialidad, integridad y disponibilidad de la información de los procesos del alcance establecido.
- Proporcionar los recursos necesarios para asegurar la implementación de las medidas de control establecidas para el tratamiento de los riesgos de la seguridad de la información.
- Garantizar la continuidad de las operaciones, mediante el resguardo de los activos asociados a los procesos y servicios dentro del alcance establecido.
- Sensibilizar y/o capacitar a los funcionarios, proveedores, terceros y colaboradores de la entidad, a fin de fomentar una cultura de seguridad de la información.
- Cumplir con los requisitos legales, normativa y estándares aplicables a la entidad en materia de seguridad de la información.
- Promover la mejora continua del Sistema de Gestión de Seguridad de la Información del OSITRAN.

Visado por: MEJIA CORNEJO Juan Carlos FIR 08271955 hard
Motivo: Firma Digital
Fecha: 11/09/2019 15:24:20 -0500

Visado por: TALLEDO LEON Cesar Enrique FAU 20420248645 hard
Motivo: Firma Digital
Fecha: 04/09/2019 09:20:56 -0500

OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

En el marco de la Política de Seguridad de la Información y del alcance establecido, los objetivos del Sistema de Gestión de Seguridad de la Información del OSITRAN son los siguientes:

- Garantizar la confidencialidad, integridad y disponibilidad de la información vinculada a los procesos dentro del alcance establecido.

- Gestionar oportunamente los riesgos e incidentes de seguridad de la información para evitar o reducir su ocurrencia.

- Garantizar la continuidad de los procesos y servicios, que formen parte del alcance establecido.

- Fortalecer la cultura de seguridad de la información en los funcionarios, proveedores, terceros y colaboradores de la entidad.

- Mejorar continuamente el Sistema de Gestión de Seguridad de la Información.

POLÍTICA ESPECÍFICA DE SEGURIDAD DE LA INFORMACIÓN PARA RELACIONES CON PROVEEDORES

El Ositrán ha establecido la siguiente política especifica de seguridad de la información para sus relaciones con proveedores:

1. Antes de iniciar la fase de ejecución contractual, el proveedor deberá tomar conocimiento de y aceptar la presente política específica, así como de la Política y objetivos de Seguridad de la Información de la entidad.
2. El proveedor deberá garantizar que todos los recursos de información que la entidad le proporcione en el marco de la contratación sean utilizados únicamente para cumplir con las actividades previstas.
3. De la misma manera, el proveedor deberá emplear la información que el Ositrán le proporcione en el marco del servicio únicamente para los fines pactados, no debiendo ser utilizada para beneficio propio o de terceros.
4. El proveedor deberá cumplir todas las cláusulas de confidencialidad establecidas en los Términos de referencia o especificaciones técnicas de la contratación, según corresponda. Esto, incluso luego de culminado el vínculo contractual, ya sea por finalización del servicio u otra causal.
5. El proveedor deberá garantizar que toda la información que el Ositrán le provea para la ejecución del servicio sea eliminada de su poder según se especifique en el requerimiento integrante del contrato u orden de compra o de servicio, una vez finalizado este.
6. En el caso de que el proveedor tome conocimiento o advierta cualquier pérdida, uso no autorizado, revelación de la información proporcionada o de propiedad del Ositrán o cualquier otro evento/debilidad/incidente de seguridad de la información, deberá comunicarlo inmediatamente a la unidad de organización contratante del servicio y al correo seguridad.informacion@ositran.gob.pe y, en caso fuera necesario, deberá adoptar los mecanismos necesarios para brindar el apoyo correspondiente al Ositrán, a efectos de remediar tal uso no autorizado o revelación de la información.
7. El proveedor se asegurará que el personal con el que ejecutará el servicio conozca, acepte y se someta a la presente política específica.
8. Asimismo, deberá asegurarse que el personal antes mencionado, cumpla con lo establecido en la presente política específica. En caso de incumplimiento, la entidad podrá solicitar al proveedor el cambio del personal.
9. En el caso de que se realice cualquier cambio en el personal, el proveedor deberá asegurarse que se cumpla con los numerales 7 y 8.
10. En caso de tratarse un servicio para cuya ejecución el Ositrán haya proporcionado información de carácter sensible o confidencial, al finalizar sus servicios, el proveedor deberá eliminar la información proporcionada por la entidad, que se encuentre alojada en sus ambientes de trabajo (físico o Digital), debiendo informar y evidenciar el método de eliminación utilizado, previo al cierre del servicio y conforme las directrices que estipule el Ositrán.

OSITRAN
Firmado por: TALLEDO LEON Cesar Enrique FAU 20420248645 soft
Motivo: Firma Digital
Fecha: 09/07/2025 18:34:05 -0500

OSITRAN
Firmado por: ARRESCURRENAGA SANTISTEBAN Angela FAU 20420248645 soft
Motivo: Firma Digital
Fecha: 09/07/2025 18:40:46 -0500

OSITRAN
Firmado por: MEJIA CORNEJO Juan Carlos FAU 20420248645 hard
Motivo: Firma Digital
Fecha: 09/07/2025 18:45:43 -0500

OSITRAN
Firmado por: MERCADO TOLEDO Ricardo Javier FAU 20420248645 hard
Motivo: Firma Digital
Fecha: 09/07/2025 18:59:35 -0500

OSITRAN
Firmado por: CHOCANO PORTILLO Javier Eugenio Manuel Jose FAU 20420248645 soft
Motivo: Firma Digital
Fecha: 09/07/2025 19:02:44 -0500

OSITRAN
Firmado por: TORRES CASTILLO Luis Miguel FAU 20420248645 hard
Motivo: Firma Digital
Fecha: 09/07/2025 21:30:45 -0500

OSITRAN
Firmado por: VALENZUELA CAVELLO Alina Aimee FAU 20420248645 hard
Motivo: Firma Digital
Fecha: 10/07/2025 09:53:10 -0500

Visado por: CASTILLO URDAY Karem Paola FAU 20420248645 soft
Motivo: Firma Digital
Fecha: 10/07/2025 16:50:02 -0500

Visado por: NORIEGA QUIROZ Eyleen Carolina FAU 20420248645 hard
Motivo: Firma Digital
Fecha: 09/07/2025 18:28:52 -0500

Firmado por
JUAN CARLOS MEJÍA CORNEJO
Gerente General
Gerencia General

Firmado por
JAVIER CHOCANO PORTILLO
Jefe de la Gerencia de Asesoría Jurídica
Gerencia de Asesoría Jurídica

Firmado por
MIGUEL TORRES CASTILLO
Jefe de Gestión de Recursos Humanos
Jefatura de Gestión de Recursos Humanos

Firmado por
ANGELA ARRESCURRENAGA SANTISTEBAN
Gerente de Atención al Usuario
Gerencia de Atención al Usuario

Visado por
KAREM PAOLA CASTILLO URDAY
Especialista de Seguridad de la Información y Ciberseguridad
Jefatura de Tecnologías de la Información

Firmado por
CÉSAR ENRIQUE TALLEDO LEÓN
Jefe de Tecnologías de la Información
Jefatura de Tecnologías de la Información

Firmado por
RICARDO MERCADO TOLEDO
Jefe de la Gerencia de Planeamiento y Presupuesto
Gerencia de Planeamiento y Presupuesto

Firmado por
AIMEE VALENZUELA CAVELLO
Coordinadora de la Oficina de Gestión Documentaria
Oficina de Gestión Documentaria

Visado por
EYLEEN CAROLINA NORIEGA QUIROZ
Especialista de Gobierno Digital y Proyectos
Jefatura de Tecnologías de la Información

	Denominación	Código:
OSITRAN EL REGULADOR DE LA INFRAESTRUCTURA DE TRANSPORTE DE USO PÚBLICO	**DIRECTIVA DE SEGURIDAD DE LA INFORMACIÓN DEL OSITRAN**	DIR-GA-JTI-01
		Versión 03
	Aprobado por Resolución N°	00004-2025-GG-OSITRAN

I. Objeto

Establecer lineamientos para la gestión y operación de la seguridad de la información en el Organismo Supervisor de la Inversión en Infraestructura de Transporte de Uso Público (en adelante, Ositrán).

II. Finalidad

Procurar la preservación de la confidencialidad, disponibilidad e integridad de la información del Ositrán.

III. Base legal

3.1. Ley N° 27269, Ley de Firmas y Certificados Digitales y su modificatoria.
3.2. Ley N° 27815, Ley del Código de Ética de la Función Pública.
3.3. Ley N° 29733, Ley de Protección de Datos Personales y su modificatoria.
3.4. Ley N° 30096, Ley de Delitos Informáticos y sus modificatorias.
3.5. Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.
3.6. Decreto de Urgencia N° 007-2020, que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento.
3.7. Decreto Supremo N° 033-2005-PCM, que aprueba el Reglamento de la Ley del Código de Ética de la Función Pública.
3.8. Decreto Supremo N° 052-2008-PCM, que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales y sus modificatorias.
3.9. Decreto Supremo N° 012-2015-PCM, que aprueba el Reglamento de Organización y Funciones del Ositrán.
3.10. Decreto Supremo N° 021-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.
3.11. Decreto Supremo Nº 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 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.
3.12. Decreto Supremo N° 075-2023-PCM, que modifica el Reglamento del Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
3.13. Decreto Supremo N° 007-2024-JUS, que aprueba el Reglamento de la Ley de Transparencia y Acceso a la Información Pública.
3.14. Decreto Supremo N° 016-2024-JUS, que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales.
3.15. Resolución Ministerial N° 087-2019-PCM que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.
3.16. Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD, que aprueba la Directiva N° 001-2023-PCM/ SGTD, Directiva que establece el perfil y responsabilidades del Oficial de Seguridad y Confianza Digital.
3.17. 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.

Las normas mencionadas en la base legal de la presente directiva incluyen sus disposiciones modificatorias, complementarias y conexas.

IV. Alcance

Las disposiciones contenidas en la presente directiva son de aplicación obligatoria para todo el personal del Ositrán, cualquiera fuere su régimen laboral o relación contractual.

V. Glosario de términos y acrónimos

Para efectos de la presente directiva se considerarán las siguientes definiciones, las cuales han sido tomadas de la ISO 27001 y del marco normativo vigente aplicable, o en su defecto han sido desarrolladas específicamente para el entendimiento del presente documento:

5.1. **Acceso:** Permiso otorgado a una cuenta de usuario, que faculta a dicho usuario a hacer uso de determinada información, sistemas, servicios u otros recursos informáticos que sean necesarios para el ejercicio de sus funciones.

5.2. **Acceso privilegiado:** Permiso otorgado a una cuenta de usuario, que brinda facultades superiores a las atribuidas a las cuentas estándar. Son asignados a los administradores de TI y faculta a los mismos a realizar configuraciones en un sistema o aplicación, añadir o eliminar cuentas, datos, entre otros.

5.3. **Acceso remoto:** Mecanismo que permite a los usuarios conectarse a una red de datos o una computadora de forma remota a través de una conexión a internet, a fin de poder hacer uso de los servicios tecnológicos, sistemas o información digital necesaria para el ejercicio de sus funciones.

5.4. **Activos de información:** Todo aquello que represente valor para el Ositrán y que participe en el proceso de almacenamiento o tratamiento de la información. Pueden ser de tipo proceso, información, sistema, hardware, software, medio de soporte, personal, red y comunicaciones, servicios tecnológicos, sitio, entre otros.

5.5. **Área segura:** Espacio definido por la entidad, en el cual se procesa, almacena o transfiere información sensible y que contiene equipos informáticos críticos. Este espacio cuenta con barreras de seguridad física para proteger los activos de información de amenazas físicas.

5.6. **Backup:** Copia de seguridad o de respaldo. Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de pérdida o alteración.

5.7. **Ciberseguridad:** Capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital. Comprende la perspectiva técnica de la Seguridad Digital y es un ámbito del Marco de Seguridad Digital del país.

5.8. **Colaborador:** Servidor civil perteneciente al régimen del D. Leg. 728, del D. Leg. 1057 y de la Ley N° 30057 o practicante de las unidades de organización del Ositrán.

5.9. **Comité de Gobierno y Transformación Digital:** Grupo de personas responsables del gobierno y transformación digital en la entidad, conformado en cumplimiento de lo dispuesto por la PCM mediante Resolución Ministerial N° 087-2019-PCM. Entiéndase como equivalente la denominación de Comité de Gobierno Digital.

5.10. **Confianza digital:** Estado que emerge como resultado de cuán veraces, predecibles, éticas, proactivas, transparentes, seguras, inclusivas y confiables son las interacciones digitales que se generan entre personas, empresas, entidades públicas o cosas en el entorno digital, con el propósito de impulsar el desarrollo de la economía digital y la transformación digital. Es un componente de la transformación digital y tiene como ámbitos la protección de datos personales, la ética, la transparencia, la seguridad digital y la protección del consumidor en el entorno digital.

5.11. **Confidencialidad:** Propiedad por la cual la información no está disponible o no puede ser divulgada a personas, entidades o procesos de negocio no autorizados.
5.12. **Cuenta de Usuario:** Credenciales que se le otorga a un usuario para el acceso a la red de datos o computadora de la entidad.
5.13. **Custodio:** Colaborador de la entidad designado para administrar y hacer efectivos los controles de seguridad que el propietario del activo de información haya definido.
5.14. **Datos personales:** Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.
5.15. **Disponibilidad:** Propiedad de la información de estar accesible para el uso de las personas, entidades o procesos autorizados cuando lo requieran.
5.16. **Dispositivos móviles:** Teléfonos móviles o tablets que son asignados a los servidores civiles para el cumplimiento de sus funciones.
5.17. **Dispositivos de usuario:** Equipos terminales (equipos informáticos y dispositivos móviles) otorgados a los servidores civiles para el cumplimiento de sus funciones.
5.18. **Dueño del proceso:** Titular de la unidad de organización responsable del proceso.
5.19. **Evento de seguridad de la información:** Ocurrencia que podría comprometer la confidencialidad, integridad y disponibilidad de un activo de información y que aún no ha afectado la operación o procesos de la organización.
5.20. **Incidente de seguridad de la información:** Ocurrencia que ha comprometido la confidencialidad, integridad y/o disponibilidad de un activo de información, generando una afectación en las operaciones o procesos de la entidad.
5.21. **Integridad:** Propiedad de precisión y completitud de la información.
5.22. **Información:** Conjunto de datos que tiene valor para el Ositrán.
5.23. **Mesa de ayuda:** Servicio de atención y gestión de requerimientos e incidencias vinculadas con los equipos o recursos informáticos de la entidad.
5.24. **Oficial de Seguridad y Confianza Digital:** Servidor civil designado formalmente por la alta dirección y comunicado a la entidad para liderar las coordinaciones necesarias para la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información dentro de la entidad. Entiéndase como equivalente la denominación de Oficial de Seguridad de la Información.
5.25. **Propietario del activo de información:** Responsable de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.
5.26. **Propietario del riesgo:** Responsable de aprobar el plan de tratamiento de los riesgos de seguridad de la información. Tiene la responsabilidad y autoridad para gestionar el riesgo. Generalmente este rol o función recae en los propietarios de los procesos.
5.27. **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.
5.28. **Seguridad Informática:** Protección de las infraestructuras tecnológicas y de comunicaciones.
5.29. **Seguridad Digital:** Estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad y los objetivos nacionales en dicho entorno.
5.30. **Sesión:** Tiempo determinado de interacción del usuario con la computadora.
5.31. **Técnicas de seudonimización o anonimización:** Técnicas que se usan para proteger la privacidad de los datos personales de los usuarios. Su objetivo es ocultar los datos personales de los usuarios, para desconectar el vínculo entre la información y la identidad del propietario de la misma y así resguardar su identidad.
5.32. **Unidades de organización:** órganos, unidades orgánicas u oficinas establecidas en el ROF del Ositrán.
5.33. **Usuario:** Colaborador de la entidad o proveedor que por razones justificadas cuenta con acceso a la red de datos y que hace uso de servicios y recursos tecnológicos.

Asimismo, se precisan los siguientes acrónimos a ser mencionados en el presente documento:

5.34. **OSCD:** Oficial de Seguridad y Confianza Digital
5.35. **SGTD:** Secretaría de Gobierno y Transformación Digital
5.36. **SGSI**: Sistema de Gestión de Seguridad de la Información
5.37. **CNSD:** Centro Nacional de Seguridad Digital
5.38. **CSCD**: Coordinador de Seguridad y Confianza Digital

VI. Disposiciones Generales

6.1. Todos los usuarios del Ositrán deben cumplir las disposiciones, directrices y lineamientos de seguridad de la información establecidos en la presente directiva.
6.2. La información y los activos de información a la que los usuarios accedan, deben ser empleados exclusivamente para el cumplimiento de sus funciones y/o actividades.
6.3. Todos los usuarios del Ositrán deben involucrarse en la gestión y operación de la seguridad de la información en la entidad, de acuerdo con los roles y responsabilidades definidos en la presente directiva.
6.4. La Jefatura de Tecnologías de la Información (en adelante JTI) en coordinación con la Jefatura de Gestión de Recursos Humanos (en adelante JGRH) debe planificar y ejecutar acciones de capacitación y concientización en materia de seguridad de la información.
6.5. La JTI, en coordinación con las unidades de organización, debe ejecutar acciones para velar por el cumplimiento de las políticas y controles de seguridad de la información por parte de los proveedores. Cualquier incumplimiento por parte de estos últimos se comunicará a la Jefatura de Logística y Control Patrimonial (en adelante JLCP) para la notificación formal al proveedor.
6.6. Todos los colaboradores deben participar de las acciones de capacitación y concientización que sean programadas en materia de seguridad de la información.
6.7. La JTI es responsable de implementar los controles tecnológicos que contribuyan a preservar la confidencialidad, integridad y disponibilidad de la información institucional almacenada en los sistemas de información.
6.8. Los titulares de las unidades de organización deben velar por la preservación de la confidencialidad, integridad y disponibilidad de la información de la que son propietarios, así como facilitar las revisiones periódicas para la verificación del cumplimiento de la política, procedimientos y controles de seguridad de la información bajo el ámbito de sus competencias.
6.9. Los titulares de las unidades de organización son responsables de la identificación y gestión de los riesgos de seguridad de la información vinculados a los procesos que se encuentran bajo el ámbito de sus competencias.
6.10. Los titulares de las unidades de organización son responsables de identificar y proteger los activos de información bajo el ámbito de sus competencias, así como procurar el tratamiento de los mismos según su clasificación; lo cual no exime de responsabilidad directa al colaborador que se le asignó el activo de información para el uso de sus actividades.
6.11. La difusión de la información institucional del Ositrán tanto a nivel interno como externo, debe realizarse exclusivamente por el personal autorizado y a través de los canales y medios oficiales.
6.12. Ningún usuario de la entidad debe divulgar información declarada como confidencial y/o restringida de la Ositrán, a la cual haya accedido en el ejercicio de sus funciones.
6.13. Todo usuario que identifique algún posible evento o incidente en materia de seguridad de la información debe reportarlo a las instancias correspondientes, a través de los canales establecidos para dicho fin.

6.14. El incumplimiento de las disposiciones de la presente directiva, de corresponder, podría ser pasible del ejercicio de la potestad sancionadora en materia disciplinaria de la entidad, conforme lo establecido en los artículos 44 [Sanciones] y 45 [Faltas] del Reglamento Interno de Servidores Civiles del Ositrán.

VII. Disposiciones Específicas

7.1. CONTROLES ORGANIZACIONALES

7.1.1. Roles y responsabilidades para la seguridad de la información

El Ositrán ha establecido los siguientes roles y responsabilidades para la gestión de la seguridad de la información:

Alta Dirección
La Alta Dirección para el SGSI está compuesta por el Comité de Gobierno y Transformación Digital.

Comité de Gobierno y Transformación Digital (CGTD)

a) Liderar la implementación del SGSI en la entidad.
b) Gestionar la asignación de personal y recursos necesarios para la implementación del SGSI en sus Planes Operativos Institucionales, Plan Anual de Contrataciones y otros.
c) Promover y gestionar la implementación de estándares y buenas prácticas en Seguridad de la información.
d) Vigilar el cumplimiento de la normatividad relacionada con la implementación de la seguridad de la información en las entidades públicas.
e) Gestionar, mantener y documentar el SGSI de la entidad.

Las responsabilidades antes señaladas para el CGTD en el marco del SGSI de la entidad, se ejercen sin perjuicio de las demás funciones atribuidas a dicha instancia, conforme el marco normativo vigente.

Oficial de Seguridad y Confianza Digital (OSCD)
Conforme a lo dispuesto en la Directiva N° 001-2023-PCM/SGTD, Directiva que establece el perfil y responsabilidades del OSCD, el OSCD del Ositrán tiene las siguientes responsabilidades:

a) Coordinar la implementación, operación, mantenimiento y mejora continua del SGSI de la entidad, atendiendo las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.
b) Coordinar con las unidades de organización de la entidad las acciones orientadas a implementar y/o mantener el SGSI, de acuerdo con lo establecido por la alta dirección y las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.
c) Formular y proponer políticas, procedimientos y planes en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad y confianza digital.
d) Promover la conformación y adecuada operación del equipo de respuestas ante incidentes de seguridad de la información.

e) Proponer medidas para la gestión de riesgos e incidentes de seguridad de la información, seguridad digital y ciberseguridad.
f) Crear y mantener un registro de los eventos e incidentes de seguridad de la información identificados.
g) Comunicar al CNSD los incidentes de seguridad digital críticos que afecten a los procesos misionales o servicios que brinda la entidad, y de ser el caso, coordinar y/o participar en su atención con el CNSD.
h) Planificar y coordinar la ejecución de pruebas de evaluación de vulnerabilidades de los aplicativos informáticos, sistemas, infraestructura, datos y redes que soportan los servicios digitales, procesos misionales o relevantes de la entidad.
i) Elaborar informes de los riesgos e incidentes de seguridad de la información críticos para la entidad pública e informarlos a la máxima autoridad administrativa.
j) Informar a la máxima autoridad administrativa acerca de los riesgos de seguridad de la información, incidentes de seguridad de la información críticos, avances y dificultades en la implementación u operación del SGSI, resultados de las auditorías de seguridad de la información internas y/o externas realizadas anualmente a la entidad, y sobre la aplicación efectiva de las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.
k) Coordinar con el CNSD acciones de sensibilización y capacitación para los funcionarios y servidores civiles de la entidad sobre seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.
l) Coordinar con el Oficial de Gobierno de Datos y el Oficial de Datos Personales en todas las cuestiones relativas a la implementación de controles de seguridad de la información relacionados con las materias de gestión de datos y protección de datos personales en la entidad, respectivamente.
m) Coordinar con el Líder de Gobierno y Transformación Digital, lo concerniente a iniciativas y proyectos en materia de seguridad y confianza digital.
n) Coordinar con los dueños de procesos, propietarios de riesgos y responsables de las unidades de organización de la entidad su apoyo en la gestión de riesgos e implementación de los controles de seguridad de la información identificados en sus ámbitos de competencia, así como en la gestión de incidentes de seguridad de la información.
o) Liderar a los CSCD designados en la entidad pública para la adecuada implementación del SGSI.
p) Asegurar y supervisar la adopción y uso de estándares, normas técnicas y mejores prácticas de seguridad de la información ampliamente reconocidos por parte de la unidad de organización de tecnologías de la información cuando ésta adquiera, tercerice o desarrolle *software* o implemente otro tipo de soluciones tecnológicas.
q) Coordinar con la unidad de organización responsable de las tecnologías de la información o la que haga sus veces en la entidad, cuando corresponda, en los temas relativos a sus responsabilidades.
r) Otras responsabilidades afines que le sean asignadas por el titular de la entidad o la máxima autoridad administrativa.

Especialista de Seguridad de la Información y Ciberseguridad

a) Proponer o actualizar documentos normativos o lineamientos que contribuyan a implementar la seguridad de la información.
b) Conducir el proceso de identificación de activos de información, así como de la identificación, análisis y evaluación de riesgos u oportunidades de seguridad de la información asociados a los mismos.

c) Efectuar seguimiento a la implementación del Plan tratamiento de riesgos, así como de los controles definidos en el SGSI.
d) Monitorear la gestión de eventos e incidentes de seguridad de la información.
e) Monitorear la infraestructura de TI del Ositrán, identificar y reportar vulnerabilidades en materia de ciberseguridad y seguridad informática.
f) Evaluar y efectuar seguimiento a la gestión de los riesgos de seguridad de la información de proyectos y requerimientos.
g) Brindar capacitación requerida por los equipos de trabajo a cargo de los proyectos o el personal de las unidades de organización que correspondan en la gestión de riesgos de seguridad de la información.
h) Supervisar y/o ejecutar las revisiones de seguridad de los dominios de seguridad en recursos humanos, seguridad en desarrollo y/o adquisición de sistemas y seguridad en las redes y comunicaciones.

Titulares de las unidades de organización

a) Participar de las actividades de identificación de activos de información, así como de la identificación, análisis y evaluación de riesgos de los procesos bajo el ámbito de sus competencias. Asimismo, aprobar los documentos resultantes de dichas actividades.
b) Brindar facilidades para las actividades periódicas de verificación del cumplimiento de las políticas y procedimientos de seguridad de la información en los procesos bajo el ámbito de sus competencias, a ser ejecutadas por el OSCD.
c) Comunicar requerimientos de control y protección de la información al OSCD y asegurar que la información y activos bajo su control estén debidamente protegidos.
d) Apoyar en la difusión de la(s) política(s) y procedimiento(s) de seguridad de la información a los colaboradores bajo su cargo.
e) Determinar los niveles de acceso de los colaboradores a su cargo a la información, sistemas de información y servicios tecnológicos bajo el ámbito de sus competencias. Así como, notificar la modificación o cancelación de los accesos asignados.
f) Reportar inmediatamente el incumplimiento o infracciones a las políticas y normas de seguridad de la información a través del canal establecido para dicho fin.
g) Revisar y validar todos los procedimientos y formatos del SGSI que le correspondan.

Propietario de riesgos de seguridad de la información

a) Participar y/o designar a los miembros del equipo de trabajo para el proceso de identificación, análisis y evaluación de los riesgos y oportunidades de seguridad de la información.
b) Aprobar las acciones del plan de tratamiento de riesgos y riesgo residual correspondiente, en el ámbito de sus competencias y gestionar su implementación oportuna.
c) Informar al OSCD respecto del nivel de implementación de las acciones de tratamiento de riesgos bajo su competencia.

Propietario de activos de información

a) Valorizar los activos de información bajo su competencia.
b) Definir la clasificación de la información bajo su competencia, con el propósito de garantizar su adecuado tratamiento conforme a su naturaleza.

c) Apoyar activamente en las actividades de identificación, análisis, evaluación y tratamientos de riesgos de seguridad de la información.
d) Autorizar la asignación de accesos sobre la información bajo el alcance de sus competencias en coordinación con el titular de la unidad de organización.
e) Autorizar los cambios sobre los activos de información bajo el alcance de sus competencias en coordinación con el titular de la unidad de organización.
f) Contribuir a la implementación de los controles de seguridad que estén relacionados con sus funciones.
g) Revisar y dar la conformidad a los resultados de la gestión de riesgos, el plan de tratamiento de riesgos y los riesgos residuales.
h) Brindar información oportuna y pertinente para la elaboración de indicadores y métricas, auditoría, revisión y mejora continua del SGSI, respecto a los activos de información a su cargo.

Colaboradores del Ositrán

a) Conocer, comprender y dar cumplimiento a las políticas, directivas, procedimientos o lineamientos en materia de seguridad de la información de la entidad.
b) Reportar debilidades, eventos, incidentes y riesgos de seguridad de la información identificados durante el desempeño de sus funciones; a las instancias pertinentes, a través de los canales correspondientes.
c) Participar en las actividades relacionadas a la gestión de riesgos de seguridad de la información.
d) Utilizar la información, activos, sistemas y servicios tecnológicos de la entidad únicamente para los propósitos autorizados e inherentes a sus funciones o actividades.
e) Proteger los recursos informáticos a fin de mantener y preservar la disponibilidad, confidencialidad e integridad de la información a la que tienen acceso, evitando, además, su divulgación fuera de los canales formales establecidos.

7.1.2. Segregación de funciones

El OSCD, con el fin de reducir el riesgo de uso incorrecto de los activos de la entidad, ya sea accidental o intencionado, debe gestionar la segregación de las funciones o roles en las unidades de organización que presentan conflicto en sus actividades dentro del SGSI.

7.1.3. Contacto con autoridades y grupos especiales de interés

a) El OSCD debe mantener activamente comunicación con autoridades y grupos de interés relacionados con la seguridad de la información, pudiendo estas ser instancias técnicas de apoyo o asesoría en dicha materia u otras a quienes se podrá recurrir en el caso de un incidente que pusiera en riesgo la confidencialidad, integridad y disponibilidad de la información de la entidad.
b) El listado de dichas autoridades o grupos de interés debe ser registrada en una matriz, la cual debe ser actualizada por el OSCD o por quien este designe, de manera periódica o cuando ocurran cambios significativos en el contexto externo y/o interno en la entidad.
c) En el caso de un incidente mayor, que requiera el pronunciamiento institucional ante la sociedad, autoridades o grupos de interesados, esta comunicación podrá ser efectuada por la Alta Dirección o por quien ésta designe.

7.1.4. Inteligencia de amenazas

a) La JTI debe establecer objetivos para la producción de inteligencia sobre amenazas a la seguridad de la información con la finalidad de generar la conciencia del entorno de amenazas y facilitar acciones de mitigación adecuadas.
b) La JTI debe establecer y ejecutar actividades para identificar y seleccionar fuentes de información internas y externas necesarias para la producción de inteligencia de amenazas, recopilar datos, procesarlos, analizar la información para comprender su significado y relevancia, y comunicar los resultados a las partes relevantes de manera comprensible.

7.1.5. Seguridad de la información en la gestión de proyectos

Las unidades de organización son responsables de considerar aspectos de seguridad de la información descritos en la presente directiva o en los otros documentos normativos del SGSI, en cada uno de los proyectos que ejecuten en la entidad. Para ello, deben solicitar asistencia al OSCD para asegurar que los riesgos de seguridad de la información se identifican y se contemplan en el marco del proyecto.

7.1.6. Seguridad de la Información en la Gestión de Activos

7.1.6.1. **Inventario y uso aceptable de la información y activos asociados**

a) El OSCD debe gestionar la identificación de los activos de información de los procesos del alcance del SGSI y de su correspondiente propietario, de acuerdo con lo establecido en los roles y responsabilidades de la presente directiva.
b) El OSCD es responsable de mantener actualizado el inventario de activos de información de los procesos bajo al alcance del SGSI.
c) El OSCD es responsable de establecer las reglas para el uso aceptable de la información y otros activos asociados.
d) El propietario del activo, en coordinación con el OSCD, debe revisar periódicamente las restricciones de acceso y las clasificaciones de activos importantes, teniendo en cuenta las políticas aplicables.
e) De la misma manera, el propietario de los activos de información debe velar por el tratamiento adecuado de los mismos, garantizando la protección de la información cuando el activo es devuelto, eliminado o destruido.

7.1.6.2. **Clasificación y etiquetado de la información**

a) El propietario de los activos de información debe clasificar los mismos según su naturaleza durante el proceso de identificación de activos, con la asistencia del OSCD.
b) El propietario de cada activo debe asegurar que la información reciba un nivel adecuado de protección de acuerdo con su naturaleza y clasificación.
c) Todo activo de tipo información debe ser clasificado según las siguientes categorías:
   - **Confidencial:** Información que no debe estar disponible o no debe ser divulgada a personas, entidades o procesos de negocio no autorizados y que se encuentre dentro de los supuestos establecidos en el artículo 17 del Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, aprobado por Decreto Supremo N° 021-2019-JUS, o norma que los modifique, complemente o sustituya.
   - **Uso interno:** información que puede ser accesible únicamente para los colaboradores de la entidad a través de los sistemas, aplicativos, portales o

cualquier medio de almacenamiento o publicación, y cuyo acceso excepcional por parte de personal externo (auditores, entidades reguladoras, consultores externos) puede darse, pero se encuentra regulado y sujeto a condiciones específicas de acceso.

- **Público:** Información que puede ser accesible o ser divulgada a todo el personal y público en general, sin reservas o consideraciones. Ej: boletines de noticias, comunicados, informes de prensa, memoria institucional, entre otros.

d) Cuando se estime que la naturaleza de un activo de tipo información ha cambiado, el propietario del activo de información debe revisar su clasificación, modificar de corresponder e informar al OSCD.
e) Todo documento generado en el marco de los actuaciones y procesos de la entidad, así como todo documento externo recibido mediante los canales establecidos, se constituye en un activo de tipo información y, por ende, debe ser clasificado para recibir el tratamiento adecuado conforme a su naturaleza.
f) Es responsabilidad de cada unidad de organización como propietaria del activo, la adecuada clasificación de los documentos emitidos o gestionados por la misma en el marco de sus competencias, a fin de garantizar su tratamiento adecuado y la preservación de su contenido.
g) La clasificación de los documentos deberá efectuarse tomando en cuenta lo dispuesto en el numeral c) del presente acápite, así como las disposiciones establecidas en la Directiva de Gestión Documental sobre seguridad y acceso de documentos.
h) El Comité de Gobierno Digital, en su calidad de responsable directivo del Modelo de Gestión Documental, debe aprobar los criterios para el control del acceso y seguridad de los documentos institucionales, teniendo como marco las definiciones de la presente directiva.
i) En el caso de documentos físicos y digitales el etiquetado y su tratamiento debe realizarse según lo dispuesto en la Directiva de Gestión Documental o documentos relacionados.

7.1.6.3. **Transferencia de información**

La JTI debe mantener la seguridad en la información que se transfiere dentro de la entidad y con cualquier organización externa. Para ello debe:

a) Establecer lineamientos, procedimientos y/o controles formales que protejan el intercambio de información.
b) Velar por la implementación de mecanismos de seguridad de la información en los canales digitales o mensajería electrónica que se implementen para el intercambio de información entre el Ositrán y otras entidades, así como con usuarios externos.

7.1.7. Seguridad de la Información para el Acceso, Identidades y Autenticación

La JTI debe establecer lineamientos y medidas de seguridad apropiadas para el control de acceso físicos y lógicos en la entidad.

7.1.7.1. **Requisitos para el control de acceso**

a) La JTI debe limitar el acceso a los recursos y servicios de consulta, manejo y procesamiento de información y activos de información.
b) La JTI debe establecer, documentar y revisar lineamientos de control de accesos basados en los requisitos de negocio y de seguridad de la información.

c) El control de acceso a los activos de información, sistemas, red de datos y servicios tecnológicos debe realizarse por medio de cuentas de usuario y contraseñas únicas para cada colaborador.
d) La JTI debe establecer parámetros para el uso de contraseñas robustas para el acceso a los activos de información y servicios tecnológicos. Asimismo, establecerá parámetros para el vencimiento periódico de las contraseñas.
e) La JTI debe mantener un registro actualizado de los niveles de accesos a la red de datos, sistemas y servicios tecnológicos, considerando los perfiles establecidos para los colaboradores.
f) Los usuarios solo podrán acceder a los recursos de información que han sido autorizados.

7.1.7.2. **Gestión de identidades**

La JTI debe garantizar la identificación única de los colaboradores y sistemas que accedan a la información de la entidad y otros activos asociados y permitir la asignación adecuada de los accesos. Para ello, debe:

a) Establecer procedimientos para el control de accesos:
   - De alta y baja de usuarios basado en las autorizaciones correspondientes y generando los registros necesarios.
   - De asignación o revocación de accesos a la red de datos, sistemas y servicios tecnológicos, basado en las autorizaciones correspondientes y generando los registros necesarios.
   - De asignación o revocación de accesos privilegiados a la red de datos, sistemas y servicios tecnológicos, basado en las autorizaciones correspondientes y generando los registros necesarios.
b) Mantener un registro del colaborador que cumple el rol de administrador con accesos privilegiados a los sistemas y/o aplicativos, así como de los servicios tecnológicos.
c) Revisar periódicamente que los accesos de las cuentas de usuario de los colaboradores desvinculados hayan sido deshabilitados.
d) Revisar periódicamente que los accesos concedidos a los usuarios sean los autorizados y según los lineamientos de control de accesos establecidos.
e) Actualizar, deshabilitar o remover todas las credenciales y los accesos del colaborador a los recursos de información, la red de datos, servicios tecnológicos y los sistemas de la entidad, una vez que haya tomado conocimiento del cambio o desvinculación correspondiente.
f) Asimismo, puede reiniciar las contraseñas en los sistemas de información y/o servicios tecnológicos únicamente a solicitud del usuario.

Los usuarios deben considerar que los accesos que superen tres (3) intentos fallidos generan automáticamente el bloqueo de la cuenta de usuario.

7.1.7.3. **Responsabilidades del usuario respecto a la gestión de accesos y autenticación**

a) Los usuarios son responsables de proteger su información de autenticación.
b) Las cuentas de usuario y contraseñas son de uso exclusivo del colaborador y no deben ser compartidas. Está prohibido el acceso a la red de datos, sistemas y servicios tecnológicos con la cuenta de usuario de otro colaborador.

c) El usuario debe establecer contraseñas robustas que brinden un adecuado nivel de seguridad, cumpliendo con los parámetros establecidos en los lineamientos de control de acceso.
d) Es responsabilidad del usuario mantener la confidencialidad de su credencial de acceso (usuario y contraseña), debiendo hacer uso adecuado de la misma y asumir la responsabilidad por las actividades realizadas desde dicha cuenta.
e) Es responsabilidad del usuario mantener actualizadas sus contraseñas conforme a la periodicidad establecida en los lineamientos de control de acceso.
f) Es responsabilidad del usuario cerrar la sesión activa en la computadora o emplear el mecanismo de bloqueo de pantalla, cuando finalice sus actividades o cuando ya no esté en uso del equipo.
g) Todo usuario que identifique cualquier indicio de que su contraseña de autenticación se encuentre vulnerada, deberá proceder al cambio inmediato de contraseña e informar a la mesa de ayuda de la JTI.

7.1.7.4. **Derechos de acceso a sistemas y aplicaciones**

a) La JTI debe prevenir el acceso no autorizado a los sistemas y aplicaciones.
b) Los accesos deben ser solicitados y autorizados por el titular de la unidad de organización
c) Los usuarios solo podrán acceder a las aplicaciones y sistemas que han sido autorizados según los lineamientos de control de acceso.
d) La JTI debe establecer mecanismos y procedimientos seguros de inicio de sesión a los sistemas y aplicaciones de acuerdo con los lineamientos de control de acceso.
e) La JTI debe restringir y controlar rigurosamente el uso de programas utilitarios privilegiados que puedan ser capaces de invalidar los controles del sistema y de la aplicación.
f) El acceso a los repositorios que contengan código fuente de las aplicaciones y software de la entidad debe ser controlado únicamente por personal de la JTI autorizado.

7.1.8. Seguridad de la Información para Proveedores

7.1.8.1. **Seguridad de la información en las relaciones con los proveedores**

a) La política o lineamientos de seguridad de la información con proveedores deben ser definidos y documentados por el OSCD, en coordinación con la JLCP para su comunicación.
b) La unidad de organización responsable del servicio a contratar debe incluir en los documentos de la contratación cláusulas de confidencialidad respecto de la información que va a ser intercambiada con el proveedor en el marco del servicio y/o cadena de suministro.
c) La JLCP debe hacer de conocimiento del proveedor la política o lineamientos de seguridad de la información con proveedores que se encuentre vigente.
d) Los titulares de las unidades de organización responsables de la gestión de los servicios del proveedor deben coordinar con las unidades de organización competentes los niveles y el periodo de acceso físicos y lógicos que el proveedor requiere para el cumplimiento de su servicio.
e) Los titulares de las unidades de organización responsables de los servicios deben asegurar la protección de los activos de la entidad que sean accesibles a los proveedores de los servicios bajo el ámbito de sus competencias.
f) La unidad de organización responsable del servicio debe supervisar que la información y los recursos que la entidad le proporcione al proveedor, sean utilizados

únicamente para cumplir con las actividades del servicio en cuestión y durante el plazo establecido del servicio.

7.1.8.2. **Seguridad de la Información en la ejecución de los servicios del proveedor**

a) El OSCD debe definir acciones para gestionar riesgos de seguridad de la información en la cadena de suministros en tecnología de la información y comunicaciones.
b) La unidad de organización responsable del servicio realizará la supervisión y la revisión del servicio, con el fin de asegurar que los términos y las condiciones de seguridad de la información de las cláusulas contractuales se están cumpliendo.
c) En el caso de que se realicen cambios en el equipo de trabajo del proveedor de un servicio contratado, la unidad de organización responsable del servicio deberá gestionar ante las unidades de organización correspondientes las medidas pertinentes respecto de los accesos físicos y lógicos.

7.1.9. Seguridad de la información para el uso de servicios en la nube

La JTI debe implementar y mantener medidas de seguridad para proteger la información almacenada, procesada o transmitida a través de servicios en la nube. Para ello debe:

a) Establecer los requisitos de seguridad de la información, los criterios de selección y el alcance del uso de servicios en la nube.
b) Determinar funciones y responsabilidades de los administradores, con relación al uso y gestión de servicios en la nube.
c) Gestionar los controles y capacidades de seguridad de los servicios en nube con el proveedor; como el monitoreo, la revisión y evaluación del uso de servicios en la nube.
d) Establecer acciones para la culminación de los servicios en la nube.

7.1.10. Gestión de incidentes de seguridad de la información

a) La JTI debe definir las responsabilidades y procedimientos para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.
b) La JTI debe evaluar los eventos reportados mediante los canales pertinentes para determinar si corresponde su clasificación como incidentes de seguridad de la información y darle el tratamiento adecuado, según el procedimiento vigente.
c) La JTI debe mantener una bitácora donde se registrarán y analizarán los eventos e incidentes de seguridad de la información, para aprender de los mismos.
d) La JTI debe responder a los incidentes de seguridad de la información de acuerdo con los métodos establecidos.
e) El OSCD, en coordinación con los especialistas de la JTI, debe evaluar la eficacia de los controles implementados como respuesta a incidentes de seguridad de la información ocurridos, a fin de reducir la probabilidad de recurrencia y sus impactos.
f) Ante la ocurrencia de un incidente de seguridad de la información que pudiera tener un impacto legal, se debe de identificar y preservar la información que pueda servir como evidencia.
g) Los colaboradores deben reportar a través de los canales establecidos para este fin; todo tipo de eventos, incidentes y/o debilidades relacionadas con la seguridad de la información y seguridad digital.

7.1.11. Seguridad de la información durante una disrupción

En el Ositrán la continuidad de la seguridad de la información debe formar parte de los requisitos para mantener la continuidad de negocio de la entidad. Para ello:

a) El OSCD, en coordinación con las unidades de organización, debe establecer los requisitos de seguridad de la información durante una disrupción.
b) La JTI, en coordinación con el OSCD, debe asegurar la implementación de los mecanismos y controles que permitan el cumplimiento de los requisitos de seguridad de la información establecidos durante una disrupción.
c) El OSCD debe de verificar los controles implementados como parte de mejora continua por lo menos una vez al año o cuando se requiera comprobando su validez y eficacia durante una disrupción.

7.1.12. Preparación de las TIC para la continuidad del negocio

La JTI debe establecer mecanismos para que la entidad pueda responder eficazmente ante interrupciones, mantener las actividades prioritarias y detectar anticipadamente incidentes que puedan afectar los servicios TIC. Para ello debe:

a) Planificar las acciones para la continuidad de las TIC considerando escenarios pre, durante y post interrupción.
b) Establecer una estructura adecuada para preparación, mitigación y respuesta; así como contar con personal competente, con el nivel de responsabilidad y autoridad necesaria.
c) Establecer actividades de respuesta y recuperación; así como realizar evaluaciones periódicas mediante ejercicios y pruebas.

7.1.13. Cumplimiento de requisitos legales, contractuales, de propiedad intelectual, información personal y protección de registros

El OSCD debe velar por el cumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.

a) El OSCD debe identificar, implementar y mantener en el alcance del SGSI las disposiciones normativas legales, regulatorias y contractuales relevantes relacionadas con seguridad de la información.
b) El OSCD debe velar por el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.
c) La JTI debe garantizar que toda adquisición de software que realice la entidad bajo licencia privativa (“copyright”) se debe realizar a través de proveedores autorizados. Asimismo, debe de mantenerse un registro y evidencias que sustenten su adquisición.
d) La JTI debe asegurar que los registros deben estar protegidos contra la pérdida, destrucción, falsificación, divulgación o acceso no autorizados de acuerdo con disposiciones legales, regulatorias, contractuales aplicables.
e) La JTI debe llevar un registro de licencias y suscripciones de software instaladas en los equipos informáticos de Ositrán y llevar un adecuado control de su vigencia.

f) La Gerencia de Asesoría Jurídica o la unidad de organización que corresponda, debe establecer y/o mantener vigentes los lineamientos orientados a la privacidad y protección de los datos personales que se gestionen dentro de la entidad.

7.1.14. Revisiones de seguridad de la información

El OSCD debe monitorear y controlar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la entidad. Para ello, debe:

a) Programar y realizar revisiones independientes y/o auditorías internas y/o externas, según corresponda de acuerdo con el procedimiento establecido.
b) Reportar y registrar los resultados de las revisiones y/o auditorías a los interesados para la atención de los hallazgos encontrados.
c) Comprobar periódicamente que los sistemas de información cumplan con las políticas y normas de seguridad de la información de la entidad.

7.1.15. Procedimientos operativos documentados

La JTI debe elaborar y mantener actualizada la documentación de los procedimientos operativos para las instalaciones de procesamiento de información.

7.2. CONTROLES DE PERSONAL

7.2.1. Antes del empleo

La JGRH, en el marco de sus funciones y conforme a lo definido en sus documentos internos de gestión o normativa vigente en la materia, debe:

a) Asegurar que todos los servidores civiles cumplan con los requisitos necesarios para el desempeño de las funciones que se le sean asignadas, así como entiendan sus responsabilidades.
b) Durante el proceso de selección, comprobar los antecedentes del personal que ingresa a laborar en la entidad, de acuerdo con las leyes y regulaciones vigentes, independientemente de su modalidad de contrato con la entidad.
c) Al inicio del vínculo laboral, entregar al nuevo servidor civil un ejemplar de la política y objetivos de seguridad de la información, dejando evidencia de su recepción.
d) Asimismo, gestionar la suscripción por parte del servidor civil de una declaración jurada referida al cumplimiento de la política, directiva y demás lineamientos establecidos de seguridad de la información; así como de un acuerdo de confidencialidad y no divulgación de la información a la cual tendrá acceso en el ejercicio de sus funciones.

7.2.2. Durante el empleo

La JGRH, conforme con lo definido en sus documentos internos de gestión o normativa vigente en la materia, debe garantizar que todos los servidores civiles conozcan y entiendan sus responsabilidades en seguridad de la información. Para ello, debe:

a) Planificar y asegurar la ejecución de actividades de inducción y capacitación en materia de seguridad de la información en coordinación con JTI, así como la participación de los servidores civiles en las mismas; a fin de lograr un nivel de concientización y conocimiento de las funciones y responsabilidades que desempeñe el servidor acorde con los objetivos de seguridad de la información.

b) Ante algún incumplimiento de la directiva, procedimiento o lineamiento relacionado a la seguridad de la información en concordancia con el Reglamento Interno de Servidores Civiles del Ositrán, poner en conocimiento del órgano competente para que se evalúe el inicio de un procedimiento administrativo disciplinario.

7.2.3. Término del empleo o cambio de puesto de trabajo

a) La JGRH debe proteger los intereses de la entidad como parte del proceso de cambio o finalización del vínculo laboral.
b) Cuando el servidor civil cambie de puesto de trabajo o se dé el término del vínculo laboral con la entidad, debe poner a disposición del titular de la unidad de organización o a quien este designe, todos los activos de información que correspondan y/o documentos (físicos y digitales) que representen valor para los procesos y funciones de la entidad, que fueron generados durante su vínculo laboral en el marco del desempeño de sus funciones.
c) La JTI procederá a actualizar, deshabilitar o remover todas las credenciales y los accesos del servidor civil a los recursos de información, la red de datos, servicios tecnológicos y los sistemas de la entidad, una vez que haya tomado conocimiento formal del cambio o desvinculación correspondiente.
d) La JTI procederá con el *backup* y resguardo de la información contenida en el buzón de correo electrónico asignado al servidor civil, una vez que haya tomado conocimiento del cambio o desvinculación, cuando corresponda. Dicha información podrá ser entregada al titular de la unidad de organización, de solicitarlo.
e) En caso de producirse un cambio de puesto de trabajo, el titular del órgano correspondiente debe solicitar a la JTI mediante el formulario respectivo, la actualización de los accesos a los servicios tecnológicos del servidor civil según el perfil del nuevo puesto de trabajo.

7.2.4. Seguridad de la información para el trabajo remoto

a) El OSCD debe disponer y/o gestionar el establecimiento de un lineamiento que defina las condiciones y restricciones para acceder, tratar o almacenar la información durante el teletrabajo en la entidad.
b) El acceso a la red de datos y sistemas de la entidad en el teletrabajo debe efectuarse, vía un servicio de internet, empleando obligatoriamente la VPN (Red Privada Virtual por sus siglas en inglés) o mecanismos equivalentes y las correspondientes credenciales de red (usuario y contraseña) previamente asignadas al colaborador.
c) El acceso remoto a la red de datos y sistemas de la entidad se debe realizar únicamente a través de equipos informáticos asignados por la entidad, los mismos que cuentan con los mecanismos de seguridad necesarios.
d) El uso de un equipo de propiedad del usuario está permitido de manera excepcional, previa autorización del titular de la unidad de organización correspondiente. El acceso a los sistemas, aplicativos y páginas de internet desde equipos de propiedad de los usuarios estará sujeto a los lineamientos y restricciones que la JTI defina en los documentos pertinentes.
e) El usuario es responsable de mantener el equipo de su propiedad con un software de seguridad informática (antivirus o antimalware) y sistema operativo actualizado y vigente, así como cualquier otro requisito que sea definido por la JTI. Asimismo, deberá permitir a la JTI efectuar las verificaciones periódicas que resulten pertinentes.

f) En caso de los servidores civiles que no puedan mantener el equipo de su propiedad con los requisitos correspondientes, éstos deberán necesariamente emplear un equipo de la entidad.

7.3 CONTROLES FÍSICOS

7.3.1 Seguridad de la información en áreas seguras

a) El OSCD debe definir y revisar los controles de seguridad física en los perímetros de las áreas que contienen información.
b) El OSCD debe evaluar los riesgos asociados al acceso físico no autorizado a las áreas seguras y proponer mecanismos y controles.
c) El OSCD debe identificar cómo áreas seguras al centro de datos de la entidad y a todos aquellos espacios que contienen información sensible o crítica.
d) El OSCD, en coordinación con la JLCP y/o con los responsables de las áreas seguras, debe implementar los mecanismos de control para prevenir el acceso físico no autorizado a las áreas seguras y a los recursos de tratamiento de la información.
e) El OSCD, en coordinación con la JLCP y/o con los responsables de las áreas seguras y la JLCP, debe implementar mecanismos físicos y/o lógicos para proteger y prevenir daños por causales externas o ambientales en las áreas identificadas como seguras.
f) El acceso a las diferentes áreas seguras del Ositrán debe estar manejado a través de mecanismos de control de acceso y de la asignación de las autorizaciones de ingreso correspondientes, supervisadas por los responsables de las áreas seguras o instancias correspondientes.
g) Cualquier personal externo sólo tendrá acceso al centro de datos de la entidad para fines específicos y debe ser autorizado por el responsable del centro de datos.
h) Todo ingreso que se efectúe por parte de personal externo o visitantes a las áreas identificadas como seguras, debe ser registrada en el formato correspondiente por parte del responsable del área segura. Durante dicho periodo, el personal externo que no pertenece a la entidad debe ser acompañado por un responsable encargado.
i) Los responsables de las áreas seguras deben evitar el trabajo no supervisado de proveedores en dichas áreas.
j) Los responsables de las áreas seguras deben controlar el ingreso de computadoras portátiles, equipos fotográficos, de video, audio o cualquier otro tipo de equipamiento que registre información, salvo previa autorización formal por correo electrónico o documento.
k) La JLCP debe establecer actividades de monitoreo a las instalaciones para detectar y disuadir el acceso físico no autorizado.

7.3.2 Seguridad en los equipos informáticos y medios de almacenamiento

La JTI debe prevenir la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la entidad. Para tal fin debe:

a) Asegurar que los equipos informáticos estén ubicados en lugares con las condiciones técnicas adecuadas, con el fin de prevenir daños ante posibles riesgos del ambiente.
b) Realizar o gestionar el mantenimiento preventivo y/o correctivo a los equipos informáticos de los usuarios y a la infraestructura tecnológica de la entidad.

c) El OSCD debe implementar mecanismos que eviten la revelación, modificación, eliminación o destrucción no autorizada de la información almacenada en medios de soportes removibles.
d) Asegurar que todo traslado de un equipo fuera de las instalaciones de la entidad sea coordinado con la JLCP y se realice con las debidas precauciones para su protección contra posibles daños y robos.
e) Velar que todo equipo desplazado para el teletrabajo cuente con la autorización de la Gerencia de Administración.
f) Adoptar una política de escritorio limpio y pantalla limpia en los equipos de la red de datos de la entidad.
g) Verificar que la información confidencial y/o restringida; así como el software con licencia se haya eliminado o sobre escrito en los equipos antes de su eliminación o reasignación.

Los usuarios deben:

a) Asegurar que el equipo desatendido tenga la protección adecuada, evitando el acceso no autorizado en ausencia del usuario.
b) En ausencia del usuario, evitar dejar papeles de trabajo expuestos sobre el escritorio. Asimismo, guardar preferiblemente en mobiliario bajo llave los medios de almacenamiento que contengan información confidencial de la entidad.
c) Evitar dejar en fotocopiadoras o impresoras documentos con información clasificada como confidencial. Asimismo, evitar el uso de papel que contenga información confidencial como papel reciclado.
d) Eliminar de manera segura la información impresa confidencial a fin de que no sea posible su reconstrucción total o parcial.
e) Cuando el usuario se ausente de su puesto de trabajo debe quitar toda la información sensible de la pantalla del equipo de cómputo, bloqueando, cerrando sesión o apagando el equipo de cómputo.

7.3.3. Suministro de apoyo y seguridad en el cableado

a) La JTI debe asegurar que los equipos informáticos, comunicaciones y de seguridad perimetral, sean protegidos contra cortes de energía u otras interrupciones causadas por fallas de los servicios públicos de apoyo (fluido eléctrico, telecomunicaciones, suministro de agua, entre otros).
b) La JTI debe efectuar las gestiones pertinentes para asegurar que el cableado eléctrico y de red de datos se encuentren separados, ordenados, etiquetados, y protegidos contra intercepciones, interferencias o daños.

7.4 CONTROLES TECNOLÓGICOS

7.4.1. Seguridad de la información para uso de dispositivos de usuario.

a) El OSCD debe proponer los lineamientos y medidas de seguridad apropiadas para la protección contra los riesgos asociados al uso de dispositivos terminales de usuario en la entidad.
b) El uso y asignación de dispositivos terminales de usuario deben ser autorizados y solicitados por el titular de la unidad de organización.
c) La JTI activará en los dispositivos terminales asignados, las configuraciones y herramientas de seguridad para su uso.

d) Todos los dispositivos terminales de usuario asignados deben contar con la última o la más segura actualización de los sistemas operativos y aplicativos obtenidos de fuentes originales y seguras.
e) No está permitido la utilización del dispositivo terminal de usuario para divulgar información no autorizada de la entidad, o para un uso diferente para el que fue asignado.
f) En caso de pérdida o robo del dispositivo terminal asignado por la entidad, el servidor civil debe reportarlo inmediatamente a la mesa de ayuda de JTI.
g) Todo dispositivo terminal provisto por la entidad debe contar con controles de acceso, controles contra fuga de datos, cifrado de dispositivo de almacenamiento y protección contra *malware*.

7.4.2. Derechos de acceso privilegiados

a) La JTI debe establecer lineamientos y mecanismos para restringir y administrar la asignación y uso de derechos de acceso privilegiado.

7.4.3. Control y restricción de acceso a la información

a) La JTI debe establecer lineamientos para evitar el acceso no autorizado a la información y otros activos asociados, de acuerdo con los lineamientos de seguridad de la información para el acceso, identidades y autenticación.
b) La JTI debe implementar mecanismos para controlar el acceso a la información en sistemas, aplicaciones y servicios.

7.4.4. Control de acceso al código fuente

a) La JTI deberá controlar el acceso a los repositorios que contengan código fuente de las aplicaciones y *software* de la entidad, herramientas de desarrollo y las bibliotecas de *software*.

7.4.5. Autenticación segura

a) La JTI debe implementar mecanismos de autenticación segura, en función de las restricciones de acceso a la información y lineamientos de seguridad de la información para el acceso, identidades y autenticación.

7.4.6. Gestión de capacidad

a) La JTI debe monitorear el uso de los recursos informáticos y prever necesidades futuras de capacidad, a fin de garantizar la disponibilidad y continuidad de los servicios de la entidad.

7.4.7. Protección contra programas maliciosos

a) La JTI debe asegurar que los recursos y servicios de consulta, manejo y procesamiento de información y la información están protegidos contra el *malware*.
b) La JTI debe asegurar que todos los equipos que se asignen a los usuarios del Ositrán cuenten con software contra códigos maliciosos.

7.4.8. Gestión de vulnerabilidades técnicas

La JTI debe mitigar los riesgos resultantes de la explotación de las vulnerabilidades técnicas. Para ello, debe:

a) Evaluar periódicamente la identificación de nuevas vulnerabilidades en los sistemas de información, aplicativos o plataformas tecnológicas que se encuentren en producción.

b) Implementar las acciones correspondientes para mitigar los riesgos asociados a las vulnerabilidades identificadas.
c) Asimismo, la instalación de software en los sistemas operacionales se encuentra restringida y puede ser únicamente ejecutada por personal de la JTI, debiendo los usuarios solicitar a dicha jefatura los softwares que requieran para el cumplimiento de sus funciones.

7.4.9. Gestión de la configuración

La JTI debe monitorear y controlar que las configuraciones funcionen de acuerdo con los requisitos de seguridad y que no se vea alterada por cambios no autorizados o incorrectos. Para ello, debe:

a) Establecer, documentar e implementar configuraciones seguras para hardware, software, servicios y redes.
b) Establecer roles, responsabilidades y actividades para gestionar todos los cambios de configuración. Mantener un registro seguro de las configuraciones establecidas y sus modificaciones, siguiendo las acciones para la gestión de cambios.
c) Establecer actividades para monitorear, revisar y actualizar regularmente las plantillas de configuración para abordar nuevas amenazas o vulnerabilidades.
d) Proteger la información sensible registrada en las plantillas y objetivos de configuración contra accesos no autorizados.

7.4.10. Eliminación de la información

a) La JTI debe establecer lineamientos para la eliminación de información cuando ya no sea necesaria, considerando requisitos legales, normativos y contractuales. Estos lineamientos deben definir plazos de retención, técnicas apropiadas y métodos de eliminación seguros para diferentes tipos de información y medios de almacenamiento.

7.4.11. Enmascaramiento de datos

a) La JTI debe definir técnicas de enmascaramiento de datos a fin de limitar la exposición de datos confidenciales y/o restringidos, incluida la información de identificación personal, para cumplir con los requisitos legales, normativos y contractuales.
b) La JTI debe establecer la técnica de seudonimización o anonimización que aplicará para ocultar la data de carácter confidencial.
c) El OSCD debe verificar que los datos hayan sido adecuadamente seudonimizados o anonimizados, considerando todos los elementos de la información sensible para prevenir la identificación indirecta de los usuarios.

7.4.12. Prevención de fuga de datos

a) La JTI debe establecer medidas de prevención de fuga de datos en todos los sistemas, redes y dispositivos que procesen, almacenen o transmitan información confidencial y/o restringida, con el fin de detectar y prevenir la divulgación y extracción no autorizada de información.
b) La JTI debe monitorear los canales potenciales de fuga y actuar preventivamente mediante el uso de herramientas especializadas para controlar, detectar y bloquear posibles fugas de datos.

7.4.13. Copia de seguridad de la información

La JTI debe establecer medidas o mecanismos para evitar la pérdida de datos. Para ello, debe:

a) Identificar los sistemas de información, servicios informáticos y la información que sean considerados críticos para la continuidad de las operaciones, con el fin de programar la ejecución, pruebas y restauración de las copias de respaldo.
b) Mantener registros exactos y completos de las copias de respaldo y de las pruebas de restauración.
c) Respaldar la información que se encuentre almacenada en los servidores del Ositrán de acuerdo con la programación de copias de respaldo establecida.
d) Ejecutar pruebas de restauración de la información relevante, con el fin de asegurar la integridad de los respaldos de información existentes.
e) Almacenar los medios que contienen las copias de respaldo en una localización remota con los niveles de protección apropiados y las condiciones físicas y ambientales de seguridad adecuadas.
f) Efectuar a solicitud del usuario, las copias de respaldo de la información almacenada en sus equipos informáticos o las restauraciones requeridas.

De la misma manera, todos los usuarios deben almacenar su información en los repositorios de información institucionales (Sharepoint), para asegurar su respaldo.

7.4.14. Redundancia de las instalaciones de procesamiento de información

La JTI debe asegurar el funcionamiento continuo de las instalaciones de procesamiento de información y servicios tecnológicos, para lo cual, debe procurar contar con infraestructura tecnológica redundante y ambientes alternos que contribuyan a garantizar la continuidad de los sistemas y servicios de tecnologías de información críticos de la entidad.

7.4.15. Registro de actividades, excepciones, fallas y eventos relevantes

La JTI debe registrar eventos y generar evidencias sobre las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información. En ese sentido debe:

a) Monitorear los sistemas de información y/o servicios informáticos que se encuentran en producción a través del personal responsable de su administración y/o servicios especializados tercerizados.
b) Almacenar y custodiar la información del registro de eventos con las medidas de seguridad que permitan asegurar su confidencialidad, integridad, disponibilidad y trazabilidad.

7.4.16. Actividades de monitoreo

a) La JTI debe monitorear las redes, sistemas y aplicaciones para detectar comportamientos anómalos y posibles incidentes de seguridad.
b) La JTI debe establecer una línea base de comportamiento normal considerando patrones de uso y acceso.
c) La JTI debe comunicar eventos anormales a las partes relevantes y establecer actividades de respuesta oportuna.

7.4.17. Sincronización de reloj

a) La JTI debe sincronizar los sistemas de información, los servicios informáticos y de comunicaciones con una fuente de referencia y de tiempo exactos con la hora oficial nacional.

7.4.18. Uso de programas de utilidad privilegiados e instalación de software en sistemas operativos

La JTI debe garantizar la integridad del software en sistemas operativos. Para ello, debe:

a) Controlar el uso de programas utilitarios privilegiados que puedan anular los controles de seguridad de los sistemas y de las aplicaciones.
b) Implementar procedimientos para controlar la instalación del software de sistemas operativos.
c) Mantener un registro de la instalación y/o desinstalación de los softwares en los sistemas operacionales.

7.4.19. Gestión de la seguridad de redes

La JTI debe proteger la información en las redes, los recursos y servicios de consulta, manejo y procesamiento de información. Para ello, debe:

a) Otorgar accesos a la red de datos a los usuarios que hayan sido debidamente autorizados por el titular de la unidad de organización correspondiente.
b) Asegurar la adecuada segregación de la responsabilidad operacional de las redes y de los sistemas informáticos.
c) Asegurar que se utilicen aplicaciones con protocolos seguros para la administración de los equipos de comunicaciones de la red cambiando las configuraciones por defecto.
d) Implementar sobre la red de datos de la entidad equipos de seguridad perimetral que permitan responder ante posibles ataques internos y externos de la red.
e) Asegurar que los identificadores de las redes inalámbricas del Ositrán no divulguen información relacionada con la entidad o alguna de sus unidades de organización.
f) Mantener el registro de eventos y monitorización para lograr el registro y detección de acciones que podrían afectar la seguridad de la información.
g) Definir los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red, los que se deben incluir en las condiciones de servicios, tanto si estos servicios se prestan dentro de la entidad como si se subcontratan.
h) Establecer segregación de redes para los segmentos de usuarios, de servidores, de acceso público (zona desmilitarizada) como mínimo.

7.4.20. Filtrado de la web

a) La JTI debe establecer mecanismos para bloquear el acceso a sitios web maliciosos, no autorizados o que contengan contenido ilegal.
b) La JTI debe establecer y mantener actualizados los lineamientos para el uso seguro y apropiado de recursos en línea, incluyendo restricciones específicas sobre sitios web y aplicaciones web inapropiadas.

7.4.21. Uso de Criptografía

a) La JTI debe asegurar un uso adecuado y eficaz de los controles criptográficos para proteger la confidencialidad, autenticidad y/o integridad de la información de la entidad, así como para el no repudio y la autentificación de usuarios en operaciones efectuadas por medios digitales.
b) La JTI debe implementar métodos criptográficos que permitan una conexión segura, en el caso que los sistemas de información requieran autenticación de los usuarios.
c) La JTI debe gestionar ante los entes correspondientes la revocación y/o cancelación de los certificados digitales, ante el cese del personal, o en caso de que estos hayan sido comprometidos o dejaron de usarse.
d) La JTI debe asegurar la confidencialidad, integridad y disponibilidad de la información que se procesa y/o transmite en los sistemas de información y/o aplicativos del Ositrán, mediante el cifrado de los canales de transmisión correspondientes.

7.4.22. Seguridad en el ciclo de vida de desarrollo de los sistemas de información y software

La JTI debe garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de sistemas de información. Para ello, debe:

a) Establecer lineamientos y requisitos sobre el desarrollo seguro de aplicaciones y sistemas, para los desarrollos internos y tercerizados.
b) Establecer, mantener y aplicar a cualquier actividad de desarrollo de sistemas de información, principios para diseñar sistemas seguros.
c) Aplicar al desarrollo y/o mantenimiento de sistemas de información y/o aplicaciones, los principios de codificación segura.
d) Ejecutar las pruebas unitarias y de seguridad informática, esta última de corresponder, así como las pruebas de aceptación con el usuario final como parte del proceso del desarrollo del software.
e) Establecer un procedimiento para el control de los cambios en el desarrollo y/o mantenimiento de sistemas de información y/o aplicaciones, dentro del ciclo de vida del software.
f) Separar los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.
g) Supervisar y monitorear en el caso de tercerización de las actividades de desarrollo de sistemas de información y/o aplicativos, que cumplan con los lineamientos establecidos de desarrollo seguro.
h) Seleccionar, proteger y gestionar adecuadamente la información de prueba.

7.4.23. Protección de los Sistemas de Información durante las pruebas de Auditoría

El OSCD debe planificar las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas y aplicaciones, en coordinación con el titular de la organización correspondiente.

VIII. Disposiciones complementarias

8.1. Los aspectos no contemplados en la presente directiva serán resueltos por la Jefatura de Tecnologías de la Información.

IX. Responsabilidades

9.1. La Jefatura de Tecnologías de la Información es la responsable de verificar la implementación y/o cumplimiento de las disposiciones de la presente directiva.

9.2. El Oficial de Seguridad y Confianza Digital es el responsable de realizar el seguimiento al cumplimiento y/o implementación de las disposiciones establecidas en la presente directiva.

9.3. El Oficial de Seguridad y Confianza Digital del Ositrán es responsable de revisar el presente documento, así como otras políticas y documentos normativos institucionales en materia de seguridad de la información con periodicidad anual o cuando ocurran cambios significativos, a fin de asegurar la vigencia de sus disposiciones y su efectividad continua.

Cuadro de Control de Cambios de la Directiva de Seguridad de la Información del Ositrán

Versión : 03

Elaborado por : **Américo Abreu Hidalgo**
Jefe de Tecnologías de la Información (e)

Revisado por : **Ricardo Mercado Toledo**
Jefe de la Gerencia de Planeamiento y Presupuesto

Javier Chocano Portillo
Jefe de la Gerencia de Asesoría Jurídica

Aprobado por : **Juan Carlos Mejía Cornejo**
Gerente General

Control de Cambios :

Referencia	Identificación del cambio
Versión 02	✓ Se actualizó la Directiva, de acuerdo con los requisitos y controles de la versión vigente de la norma ISO 27001:2022 ✓ Se actualizó el acápite III. Base legal. ✓ En el acápite V. Glosario de términos y acrónimos, se incorporaron los términos: Áreas seguras, confianza digital, dispositivos de usuario, técnicas de seudonimización o anonimización. Se incorporó el acrónimo CSCD. ✓ Se reorganizó el contenido de las disposiciones específicas en función de la nueva estructura de la norma vigente. ✓ Se incorporó la disposición general 6.12, relacionada a la restricción de divulgación de información. ✓ Se incorporó la sección 7.1 Controles Organizacionales ✓ Se actualizó el nombre del control 7.1.1 a Roles y responsabilidades. ✓ Se modificó en el numeral 7.1.1. el nombre de Analista en Seguridad de la Información por Especialista de Seguridad de la Información y Ciberseguridad. ✓ Se modificó el numeral 7.1.1. la función b) del rol Titulares de las unidades de organización. ✓ Se modificó el nombre del numeral 7.1.3 a Contacto con autoridades y grupos especiales de interés. ✓ Se incorporó el control 7.1.4. Inteligencia de amenazas, el cual contiene el desarrollo de los literales a) y b). ✓ Se modificó el nombre del numeral 7.1.6.1. Inventario y uso aceptable de la información y activos asociados. En esta sección se incorporó el literal c) y se modifica el literal e). ✓ Se modificó el nombre del numeral 7.1.6.2. Clasificación y etiquetado de la información. En esta sección de modifican los literales b), c), e), f), g) y h) ✓ Se modificó el nombre del numeral 7.1.7. Seguridad de la Información para el Accesos, Identidades y Autenticación. ✓ Se modificaron los literales b) y f) de la sección 7.1.7.1. Requisitos para el control de acceso. ✓ Se modificó el nombre del numeral 7.1.7.2. Gestión de identidades. Se modifica el literal d), de este numeral. ✓ Se modificó el nombre del numeral 7.1.7.3. Responsabilidades del usuario respecto a la gestión de accesos y autenticación. ✓ Se modificó el nombre del numeral 7.1.7.4. Derechos de acceso a sistemas y aplicaciones, en esta sección se modifica el literal b).

	✓ Se modificaron los literales d), e) y f) de la sección 7.1.8.1. Seguridad de la información en las relaciones con los proveedores. ✓ Se modificaron el nombre del numeral 7.1.8.2. Seguridad de la información en la ejecución de los servicios del proveedor, en esta sección se modifican los literales a) y b). ✓ Se incorporó el numeral 7.1.9. Seguridad de la información para el uso de servicio en la nube. Esta sección contiene los literales a), b), c) y d). ✓ Se modificaron los literales a), b) y c) y se incorpora el literal g) del numeral 7.1.10. Gestión de incidentes de seguridad de la información. ✓ Se incorporaron el numeral 7.1.11. Seguridad de la información durante una disrupción. Esta sección contiene los literales a) y b) y c. ✓ Se incorporaron el numeral 7.1.12. Preparación de las TIC para la continuidad del negocio, el cual contiene el desarrollo de los literales a) y b). ✓ Se actualizó el numeral 7.1.13. Cumplimiento de requisitos legales y contractuales, de propiedad intelectual, información personal y protección de registros. En esta sección se modifica el literal e). ✓ Se modificó la parte introductoria del numeral 7.1.14. Revisiones de seguridad de la información. ✓ Se incorporó el numeral 7.1.15. Procedimientos operativos documentados. ✓ Se incorporó la sección 7.2. Controles de personal. ✓ Se modificó el literal d) del numeral 7.2.3 Termino del empleo o cambio de puesto de trabajo. ✓ Se incorporó el numeral 7.2.4. Seguridad de la información para el trabajo remoto, en el cual se modifican los literales b), d) y e). ✓ Se incorporó la sección 7.3. Controles físicos. ✓ En el numeral 7.3.1. Seguridad de la información en áreas seguras, se incorporan los literales a) y k). ✓ Se incorporó el numeral 7.3.2. Seguridad en los equipos informáticos y medios de almacenamiento, el cual contiene el desarrollo de los literales a), b), c), d), e), f) y g). ✓ Se incorporó el numeral 7.3.3. Suministro de apoyo y seguridad en el cableado, el cual contiene los literales a) y b). ✓ Se incorporó la sección 7.4. Controles tecnológicos. ✓ Se incorporó el numeral 7.4.1. Seguridad de la información para uso de dispositivos de usuario. Se modifican los literales a), b), c), d), e), f) y g). ✓ Se incorporó el numeral 7.4.2. Derecho de accesos privilegiados. El cual cuenta con el literal a). ✓ Se incorporó el numeral 7.4.3. Control y restricción de acceso a la información. El cual cuenta con los literales a) y b). ✓ Se incorporó el numeral 7.4.4. Control de acceso al código fuente. El cual cuenta con el literal a). ✓ Se incorporó el numeral 7.4.5. Autenticación segura. El cual cuenta con el literal a). ✓ Se incorporó el numeral 7.4.6. Gestión de capacidad. El cual cuenta con el literal a). ✓ Se incorporó el numeral 7.4.7. Protección contra programas maliciosos, el cual contiene el desarrollo de los literales a) y b). ✓ Se incorporó el numeral 7.4.8. Gestión de vulnerabilidades técnicas, el cual contiene los literales a), b) y c). ✓ Se incorporó el numeral 7.4.9. Gestión de la configuración, el cual contiene los literales a), b), c) y d).

	✓ Se incorporó el numeral 7.4.10. Eliminación de la información, el cual contiene el literal a). ✓ Se incorporó el numeral 7.4.11. Enmascaramiento de datos, el cual contiene los literales a), b) y c). ✓ Se incorporó el numeral 7.4.12. Prevención de fuga de datos, el cual contiene los literales a) y b). ✓ Se modificó la parte introductoria y el literal d) del numeral 7.4.13. Copia de seguridad de la información. ✓ Se incorporó el numeral 7.4.14. Redundancia de las instalaciones de procesamiento de información. ✓ Se modificó el nombre del numeral 7.4.15. Registro de actividades, excepciones fallas y eventos relevantes. Además, se modifican los literales a) y b). ✓ Se incorporó el nombre del numeral 7.4.16. Actividades de monitoreo. Además, se modifican los literales a), b) y c). ✓ Se reubica el numeral 7.4.17. Sincronización de reloj. ✓ Se modificó el nombre del numeral 7.4.18. Uso de programas de utilidad privilegiados e instalación de software en sistemas operativos. En esta sección se modificó la introducción, y los literales a) y b). ✓ Se modificó el nombre del numeral 7.4.19. Gestión de la seguridad de redes. Se adecúa la introducción de esta sección. ✓ Se incorporó el numeral 7.4.20 Filtrado de la web, el cual contiene los literales a) y b). ✓ Se modificó el nombre del numeral 7.4.21 Uso de Criptografía. Adicionalmente se modifican los literales a). b) y c) ✓ Se modificó el nombre del numeral 7.4.22. Seguridad en el ciclo de vida de desarrollo de los sistemas de información y software. Adicionalmente se modifican el literal a) y se incorporan los literales b), c), f) y h). ✓ Se modificó el numeral 7.4.23. Protección de los sistemas de información durante las pruebas de auditoría.

Visado por:
AMÉRICO ABREU HIDALGO
Jefe de Tecnologías de la Información (e)
Jefatura de Tecnologías de la Información

Firmado por: ESCOBAR BEDOYA Christian Milovan FAU 20420248645 soft
Motivo: Firma Digital
Fecha: 14/03/2024 12:06:59 -0500

Firmado por: TORRES CASTILLO Luis Miguel FAU 20420248645 hard
Motivo: Firma Digital
Fecha: 18/03/2024 12:56:28 -0500

Firmado por: CARRION OLAZABAL Rosemiere Vicenta FAU 20420248645 soft
Motivo: Firma Digital
Fecha: 18/03/2024 13:01:37 -0500

Firmado por: ESCALANTE MELCHIORS Maria Cristina FAU 20420248645 hard
Motivo: Firma Digital
Fecha: 18/03/2024 15:44:11 -0500

Firmado por: CHEN CHEN Thou Su FAU 20420248645 soft
Motivo: Firma Digital
Fecha: 19/03/2024 14:45:07 -0500

Firmado por: JORDAN LIZA Zulema FAU 20420248645 hard
Motivo: Firma Digital
Fecha: 19/03/2024 14:51:15 -0500

PLAN PARA LA VIGILANCIA, PREVENCIÓN Y CONTROL DEL COVID-19 EN EL OSITRÁN

I. DATOS DEL EMPLEADOR

Organismo Supervisor de la Inversión en Infraestructura de Transporte de Uso Público– Ositrán.
Registro Único de Contribuyente – RUC: Nº 20420248645
Dirección: Calle Los Negocios N°182, 2do. Piso, distrito de Surquillo, provincia y departamento de Lima.

II. DATOS DEL LUGAR DE TRABAJO

SEDE CENTRAL
Calle Los Negocios N°182, distrito de Surquillo, provincia y departamento de Lima.

OFICINAS DESCONCENTRADAS – SEDES
Cusco: Av. El Sol N° 614, Sub-fracción A-5 (primer nivel) – distrito de Cusco, provincia y departamento de Cusco.
Iquitos: Jr. Sargento Fernando Lores N° 254 – Iquitos, provincia de Maynas, departamento de Loreto.
Arequipa: Av. Aeropuerto S/N Cerro Colorado (Hall principal del terminal de pasajeros frente a la zona de Check in) – Provincia y departamento de Arequipa.

CENTROS DE ORIENTACIÓN

Línea 1 del Metro de Lima y Callao: Estación La Cultura, Stand N° 14 Cruce de la Av. Aviación con Av. Javier Prado, distrito de San Borja, provincia y departamento de Lima.
Línea 2 del Metro de Lima y Callao: Av. Nicolás Ayllón 2018, distrito de Ate Vitarte, provincia y departamento de Lima.
Terminal Norte Multipropósito del Callao – Edificio Público de APM Terminals Callao S.A. (2do piso): Av. Contraalmirante Raygada N° 111, distrito y provincia del Callao.

III. DATOS DEL SERVICIO DE SEGURIDAD Y SALUD DE LOS SERVIDORES

Las responsabilidades vinculadas a la seguridad y salud de los servidores serán según detalle:

PUESTO	SITUACION
Médico	Dr. Rafael Berrio Carmelino
Enfermera	Lic. Claudia Sumari Chang

IV. INTRODUCCIÓN

Con fecha 11 de marzo del 2020, la Organización Mundial de la Salud – OMS, declaró la pandemia del nuevo coronavirus, denominado COVID-19, reportándose el primer caso en el Perú el 06 de marzo. En dicho contexto, el Estado Peruano tomó las correspondientes medidas, tales como la vigilancia epidemiológica que abarca desde la búsqueda de casos sospechosos por contacto, hasta el aislamiento domiciliario de los casos confirmados y procedimientos de laboratorio(serológicos y moleculares) para el diagnóstico de casos COVID-19, manejo clínico de casos positivos y su comunicación para investigación epidemiológica, y medidas básicas de prevención y control del contagio en centros hospitalarios y no hospitalarios.

Por ello, y siendo que está demostrado que la exposición al virus coronavirus que produce la enfermedad COVID-19, representa un riesgo biológico por su comportamiento epidémico y alta transmisibilidad, se ha dispuesto que todos los centros laborales, por cuanto constituyen espacios de exposición y contagio, deben considerar medidas para su vigilancia, prevención y control, a partir de lineamientos generales que para estos efectos ha emitido el Ministerio de Salud.

Además, es necesario considerar los principios definidos por la Organización Mundial de la Salud – OMS, a tener en cuenta al momento de plantear el desconfinamiento, siendo uno de ellos *"Establecer medidas preventivas en los lugares de trabajo y promover medidas como teletrabajo, el escalonamiento de turnos y cualesquiera otras que reduzcan los contactos personales".*

Asimismo, la Ley Nº 29783, Ley de Seguridad y Salud en el Trabajo tiene como objeto promover una cultura de prevención de riesgos laborales en el país; para ello, cuenta con el deber de prevención de los empleadores, el rol de fiscalización y control del Estado y la participación de los servidores y sus organizaciones sindicales, quienes a través del diálogo social velan por la promoción, difusión y cumplimiento de la normativa sobre la materia.

En este marco, el Ositrán, con la intención de prevenir el contagio del virus COVID- 19 en sus instalaciones; establece los procedimientos para la vigilancia de la salud de los servidores a través del presente Plan para la Vigilancia, Prevención y Control de COVID – 19 en el Trabajo – Ositrán.

El presente Plan contribuye a la disminución de riesgo de transmisión de la COVID-19 en el ámbito laboral.

V. BASE LEGAL

- Ley N° 26842, Ley General de Salud, y sus modificatorias.
- Ley N° 29733, Ley de protección de datos personales, y su modificatoria.
- Ley N° 29783, Ley de Seguridad y Salud en el Trabajo, y sus modificatorias.
- Ley N° 31572, Ley del Teletrabajo**.**
- Decreto Supremo N° 005-2012-TR, que aprueba el Reglamento de la Ley N° 29783, Ley de Seguridad y Salud en el Trabajo, y sus modificatorias.
- Directiva Administrativa N° 349-MINSA-DGIESP-2024, de fecha 13 de enero del 2014, Directiva Administrativa que establece las disposiciones para la vigilancia, prevención y control de la salud de los servidores con riesgo de exposición a SARS-CoV-2.

VI. DISPOSICIONES GENERALES

6.1 DEFINICIONES OPERATIVAS

6.1.1 Aislamiento respiratorio en la comunidad:

Es el procedimiento por el cual, previa evaluación médica y bajo criterio del médico tratante, una persona considerada como caso sospechoso, probable o confirmado de COVID-19, y que no requiere hospitalización, deberá seguir pautas para reducir la transmisión en otros servidores de los centros de labores.

En el caso de los servidores de salud es necesario reducir el contacto con pacientes en establecimientos de salud, centros residenciales y casas de reposo.

6.1.2 Caso sospechoso de COVID-19:

Persona que cumpla con cualquiera de los siguientes criterios clínicos:

a) Paciente con síntomas de infección respiratoria aguda, que presente tos y/o dolorde garganta y además uno o más de los siguientes signos/síntomas:

- Malestar general
- Fiebre
- Cefalea
- Congestión nasal
- Dolor de garganta

- Diarrea
- Dificultad para respirar (señal de alarma).

b) Persona con inicio reciente de anosmia (pérdida del olfato) o ageusia (pérdida del gusto), en ausencia de cualquier otra causa identificada.
c) Paciente con infección respiratoria aguda grave (IRAG: infección respiratoria aguda con fiebre o temperatura actual > o igual a 38º C, y tos; con inicio dentro de los últimos diez (10) días; y que requiere hospitalización).

El caso sospechoso de COVID-19 no requiere de confirmación de laboratorio para su clasificación.

6.1.3 Caso probable de COVID-19:

Quienes cumplan con cualquiera de los siguientes criterios:

a) Caso sospechoso con antecedente epidemiológico de contacto directo con un caso confirmado, o epidemiológicamente relacionado a un conglomerado de casos, los cuales han tenido al menos un caso confirmado dentro de ese conglomerado, catorce (14) días previos al inicio de los síntomas

b) Caso sospechoso con imágenes de tórax que muestran hallazgos sugestivos de COVID-19, en cualquiera de los siguientes exámenes de apoyo:

- Radiografía de tórax: Opacidades nebulosas, de morfología a menudo redondeadas, con distribución pulmonar periférica e inferior.
- Tomografía computarizada de tórax: Múltiples opacidades bilaterales en vidrio esmerilado, a menudo de morfología redondeada, con distribución pulmonar periférica e inferior.
- Ecografía pulmonar: Líneas pleurales engrosadas, líneas B (multifocales, aisladaso confluentes), patrones de consolidación con o sin broncogramas aéreos.
- Resonancia magnética con imágenes compatibles a afección pulmonar.

6.1.4 Caso confirmado de COVID-19:

Toda persona que cumpla con alguno de los siguientes criterios:

- Caso sospechoso o probable con prueba molecular positiva para detección del virus SARS-COV-2.
- Caso sospechoso o probable con prueba antigénica positiva para SARS COV-2.
- Persona asintomática con prueba molecular o antigénica positiva para SARS- CoV-2.

6.1.5 Caso de infección asintomática de COVID-19:

Toda persona asintomática identificada a través de la estrategia de búsqueda activa que no presenta signos ni síntomas compatibles con COVID-19, con resultado positivo de prueba molecular para SARS-COV-2 o que presenta prueba antigénica positiva.

6.1.6 Centro de trabajo:

Lugar o lugares en el (los) que se desarrolla la actividad laboral, con la presencia de servidores.

6.1.7 Descanso Médico:

Periodo de reposo físico que se indica al paciente mediante el procedimiento a cargo de médico tratante asignado por el centro de labores o por el médico tratante del paciente, como medida complementaria para el manejo de SARS-CoV-2, requiriendo monitoreo para detectar progresión de enfermedad. Se debe contemplar los siguientes procesos:

- Todo servidor con síntomas gripales debe usar mascarilla y buscar atención médica (medico ocupacional o especialista).
- En caso de ser un caso sospechoso de COVID-19 y hubiese disponibilidad de insumos para hacerse la prueba diagnóstica, debe proceder a realizarse.
- El médico puede determinar si es un caso sospechoso de COVID-19 y puede realizar el diagnóstico presuntivo a partir del cuadro clínico e indicar el descanso médico según la evaluación clínica independientemente de no disponer de confirmación de laboratorio.

6.1.8 Distanciamiento físico:

Es medida para el control de infecciones. El objetivo del distanciamiento físico es reducir las posibilidades de contacto entre las personas infectadas y no infectadas, con la finalidad de minimizar la transmisión del virus SARS-CoV-2.

6.1.9 Empleador/a:

Toda persona natural o jurídica, privada o pública, que emplea a uno o varios servidores.

6.1.10 Equipos de Protección Personal (EPP):

Son dispositivos, materiales e indumentaria personal destinados a cada servidor para protegerlo de uno o varios riesgos presentes en el trabajo y que puedan amenazar su seguridad y salud. Los EPP son una alternativa temporal y complementaria a las medidas preventivas de carácter colectivo (control administrativo y ambiental).

6.1.11 Factores de riesgo para COVID-19:

Se ha identificado factores de riesgo individuales asociados al desarrollo de complicaciones relacionadas a la COVID-19, que son los siguientes:

- Personas de 60 años a más.
- Diabetes Mellitus
- Obesidad (IMC > 30)
- EPOC (Enfermedad Pulmonar Obstructiva Crónica)
- Enfermedad o tratamiento Inmunosupresor (Inmunodeficiencias congénitas o adquirida) incluido VIH.
- Pacientes oncológicos (Cáncer)
- Enfermedades cardiovasculares (incluye Hipertensión arterial)
- Enfermedad renal crónica
- Asma moderada o grave
- Gestantes y puérperas.
- Enfermedad hepática crónica.

6.1.12 Lista de Chequeo de Vigilancia de la COVID-19:

Instrumento que se utiliza para vigilar el riesgo de exposición al SARS-CoV-2 en el lugar de trabajo (Ver Anexo N°4).

6.1.13 Lugar de trabajo:

Todo espacio o área donde los servidores permanecen y desarrollan su labor o donde tienen que acudir para desarrollarlo.

6.1.14 Profesional de la Salud del Servicio de Seguridad y Salud en el Trabajo (SST):

Para el presente documento técnico, aquel quien cumple la función de gestionar o realizar la vigilancia de salud de los servidores por exposición al SARS-CoV2, de acuerdo con el tamaño del centro de trabajo.

6.1.15 Puestos de trabajo con riesgo de exposición a SARS-CoV-2:

Son aquellos puestoscon diferente nivel de riesgo de exposición a SARS-CoV-2, que dependen del tipo de actividad que realizan.

Los niveles de riesgo de los puestos de trabajo se clasifican en:

- **Riesgo Bajo de Exposición:** Los trabajos con un riesgo bajo de exposición son aquellos que no requieren contacto con personas, que se conozca o se sospeche que están infectados con SARS-CoV-2, así como, en el que no se tiene contacto cercano y frecuente a menos de 1.5 metros de distancia con el público en general; o en el que se puedan usar o establecer barreras físicas para el desarrollo de la actividad laboral.

- **Riesgo Mediano de Exposición:** Los trabajos con riesgo mediano de la exposición, son aquellos que requieren contacto cercano y frecuente a menos de 1.5 metros de distancia con el público en general; y que, por las condiciones en el que se realizan no se puedan usar o establecer barreras físicas para el trabajo. En este grupo se incluyen algunos puestos de trabajo en educación presencial, comerciantes minoristas, vigilantes con contacto con el público.

- **Riesgo Alto de Exposición:** Trabajo con riesgo potencial de exposición a casos sospechosos o confirmados de COVID-19 u otro personal que debe ingresar a los ambientes o lugares de atención de pacientes con la COVID-19, pero que no se encuentran expuestos a procedimientos generadores de aerosoles en el ambiente de trabajo. Este grupo incluye a los servidores de ambulancias y servidores de funerarias.

- **Riesgo Muy Alto de Exposición:** Trabajo en el que se tiene contacto con casos sospechosos y/o confirmados de COVID-19, expuesto a procedimientos generadores de aerosoles, en el ambiente de trabajo, durante procedimientos médicos específicos o procedimientos de laboratorio (manipulación de muestras de casos sospechosos o confirmados). Incluye a los servidores de morgues que realizan necropsias.

6.1.16 Pruebas de Diagnóstico para la COVID-19:

Son aquellas pruebas de ayuda diagnóstica realizada por personal entrenado, cumpliendo con requerimientos técnicos, de bioseguridad y manejo correcto manejo de residuos biocontaminados:

a) Detección del material genético del virus (prueba molecular).
b) Detección del virus como entidad individual, mediante la detección de antígenos virales (prueba rápida de detección de antígeno del SARS- CoV 2).

6.1.17 Reincorporación al trabajo:

Proceso de retorno al trabajo presencial cuando el servidor fue diagnosticado de COVID-19, estuvo en descanso médico y está de alta por el médico tratante

6.1.18 Responsable del Servicio de Seguridad y Salud de los Servidores:

Profesional de la Salud u otro, que cumple la función de gestionar o realizar el Plan para la vigilancia de salud de los servidores en el marco de la Ley N° 29783,Ley de Seguridad y Salud en el Trabajo. Tiene entre sus funciones prevenir, vigilary controlar el riesgo de exposición laboral por el SARS-CoV-2.

6.1.19 Servidor:

Toda persona natural que desempeña una actividad laboral subordinada o autónoma, para un empleador del Estado.

6.1.20Teletrabajo:

Es una modalidad para desarrollar la fuerza laboral acorde a los nuevos tiempos, optimizando el trabajo desde casa, lugar de aislamiento o lugar habitual, reduciendo el espacio físico de las empresas o entidades públicas, fortaleciendo los lazos familiares, y conllevando a un ahorro y mejora económica y prevención ante el contagio contra la COVID-19.

6.1.21 Valoración de la aptitud para la reincorporación a labores presenciales:

Consiste en la evaluación médica, del estado vacunal y riesgo de exposición al SARS-CoV-2, realizada por el médico del servicio de seguridad y salud en el trabajo o el que haga sus veces, en el marco de la emergencia sanitaria. Esta no se refiere a la evaluación de la aptitud laboral referida en el Documento Técnico "Protocolos de Exámenes Médicos Ocupacionales y Guías de Diagnóstico de los Exámenes Médicos Obligatorios por Actividad", aprobado con Resolución Ministerial N° 312- 2011- MINSA.

6.2 Los empleadores deben garantizar un ambiente seguro de trabajo, verificando que de preferencia todos los empleados estén debidamente vacunados para la COVID-19.

6.3 Todo empleador debe garantizar la seguridad y salud en el trabajo de sus servidores en el marco de la Ley Nº 29783, Ley de Seguridad y Salud en el Trabajo.

6.4 Todo empleador garantiza la organización de un servicio de seguridad y salud en el trabajo, cuya finalidad es esencialmente preventiva, con sus profesionales de salud registrados de acuerdo con la normativa vigente.

6.5 En todo centro laboral, a través del Servicio de Seguridad y Salud en el Trabajo en el centro de trabajo, se debe elaborar el "Plan para la vigilancia, prevención

y control de la COVID-19 en el trabajo", el mismo que debe ser remitido al Comité de Seguridad y Salud en el Trabajo o al Supervisor de Seguridad y Salud en el Trabajo, según corresponda, para su aprobación en un plazo máximo de cuarenta y ocho (48) horas a partir de su recepción.

6.6 Las disposiciones contempladas en el presente Plan, es de aplicación por todo empleador, independientemente que esté comprendido en el ámbito del Decreto Supremo N°003-98-SA, que aprueba Normas Técnicas del Seguro Complementario de Trabajo de Riesgo.

VII. DISPOSICIONES ESPECIFICAS

Dadas las recientes modificaciones normativas, el Ositrán está en la obligación de adecuar e implementar medidas acordes a la normativa vigente, garantizando con ello la seguridad y salud en el trabajo, cuya finalidad es esencialmente preventiva y de control en la disminución de riesgo de transmisión de la COVID-19 en el ámbito laboral. Por tal motivo, el Ositrán, garantiza un ambiente seguro de trabajo, verificando que de preferencia todos los servidores estén debidamente vacunados contra COVID-19.

Los profesionales de la salud del Ositrán, están a cargo del monitoreo del estricto cumplimiento de los implementos de seguridad sanitaria relacionado a los servicios de mantenimiento, limpieza, seguridad y otros; para ello contarán con el apoyo del personal de la Jefatura de Logística y Control Patrimonial-JLCP.

Asimismo, la entidad ha reevaluado el aforo de la sede central (Anexo 05) y de las áreas destinadas a las oficinas; así como de las Oficinas Desconcentradas y Centros de Orientación, en el marco de las disposiciones sanitarias establecidas por el Ministerio de Salud por el COVID-19 para las entidades públicas.

Los empleadores del personal de mantenimiento, limpieza y seguridad (intermediación o tercerización laboral), así como los proveedores frecuentes identificados, que se encuentren en las instalaciones del Ositrán, deberán cumplir con las disposiciones establecidas en el presente plan, conforme a la normativa vigente.

En el Ositrán, el Servicio de Seguridad y Salud en el Trabajo, elaboró el "Plan para la vigilancia, prevención y control del COVI0-19 en el trabajo", el mismo que fue remitido al Comité de Seguridad y Salud en el Trabajo para su aprobación.

Todos los servidores, al retornar a la prestación de servicios en sus puestos de trabajo de forma presencial, han tomado conocimiento de los Procedimientos Obligatorios de Prevención del COVID-19, que forman parte del Plan para la Vigilancia, Prevención y Control de COVID-19 en el Trabajo del Ositrán, cuya actualización se les hará llegar de manera virtual y debiendo llenar un formato electrónico con sus datos personales, bajo la observancia de los lineamientos, acciones y responsables por cada temática; esta disposición incluye a los proveedores frecuentes identificados y personal de las empresas de tercerización

e intermediación laboral, quienes a través de sus empleadores o directamente se les hará llegar la información, según corresponda.

La entidad ha identificado a los servidores que presenten factores de riesgo, considerando las definiciones vigentes de la Autoridad Sanitaria y criterios epidemiológicos establecidos por el Centro Nacional de Epidemiología Prevención y Control de Enfermedades (CDC):

- Edad mayor igual a 60 años a más.
- Diabetes Mellitus.
- Obesidad (IMC > 30).
- EPOC (Enfermedad Pulmonar Obstructiva Crónica).
- Enfermedad o tratamiento Inmunosupresor (Inmunodeficiencias congénitas o adquirida incluido VIH.
- Pacientes oncológicos (Cáncer).
- Enfermedades cardiovasculares (incluye Hipertensión arterial).
- Enfermedad renal crónica.
- Asma moderada o grave.
- Gestantes y puérperas.
- Enfermedad hepática crónica.

Cabe precisar que, para el caso de las personas en grupos de riesgo que laboran, se prioriza su prestación de servicios bajo la modalidad de teletrabajo. En caso los servidores identificados dentro del referido grupo, que sus funciones no les permitan realizar actividades remotas y/o deseen concurrir a trabajar en modalidad presencial, deberán seguir las siguientes disposiciones:

1. Los servidores nuevos mediante DJ de buena salud (Anexo 03), que presenten alguna comorbilidad y/o que sean mayor o igual de 60 años de edad, será el área usuaria quien evalúa la necesidad de servicio en modalidad presencial y/o mixta, debiendo informar a la JGRH las funciones que cada servidor del grupo de riesgo realizará.

2. El profesional de la salud solicitará al servidor del grupo de riesgo que haya sido designado para trabajo en modalidad presencial y/o mixta, los siguientes documentos de salud:

    - Carnet de vacunación contra COVID-19 (De preferencia con dosis Completa – Según lo indique el calendario de vacunación del MINSA).
    - Informe o certificado médico actualizado, de la especialidad correspondiente.

3. Una vez recepcionados los documentos de salud, el profesional de la salud procederá a su revisión e informará al área que lo requiera, la aptitud de cada servidor que pertenece al grupo de riesgo y que permita realizar trabajo en modalidad presencial y/ɵ mixta.

El presente Plan es de alcance a todos los servidores del Ositrán sin excepción,tanto a los que laboran en las instalaciones de la entidad, como no, en lo que les compete, así como para todas las personas que ingresen a esta (proveedores, proveedores frecuentes identificados, personal de seguridad, mantenimiento y limpieza).

Para el caso de los servidores que se encuentran en los Centros de Orientación del Ositrán deberán adherirse de manera complementaria a los lineamientos establecidos por las entidades prestadoras respectivas; para el caso del personal en campo, además del procedimiento contenido en el presente Plan deberán cumplir los planes o disposiciones establecidos por las Entidades Prestadoras dentro del área concesionada materia de supervisión, bajo responsabilidad, para lo cual el Ositrán podrá prestar las facilidades que requieran (pruebas de descarte, equipos especializados, desinfección área de trabajo, etc.).

VIII. OBJETIVO

Establecer las disposiciones para la vigilancia, prevención y control de la salud de los servidores con riesgo de exposición a SARS-CoV-2.

IX. NÓMINA DE SERVIDORES POR RIESGO DE EXPOSICIÓN AL COVID-19

Producto de la evaluación respecto al riesgo de exposición al COVID-19 de los puestos y servicios entregados por la entidad a la ciudadanía o beneficiarios, se presenta la siguiente nómina (Anexo 01).

X. DISPOSICIONES PARA LA PREVENCIÓN Y CONTROL DE COVID-19 EN EL TRABAJO

Para la vigilancia de la salud de los servidores, en el contexto de la pandemia por la COVID-19, se han considerado siete (7) disposiciones para aplicación por el empleador, basados en criterios técnicos y epidemiológicos.

10.1 DISPOSICIÓN 1: VACUNACIÓN CONTRA LA COVID-19.

La medida de prevención más efectiva es la vacunación contra la COVID-19. Se recomienda que todos los servidores tengan sus vacunas de acuerdo al esquema nacional de vacunación contra COVID-19, en la medida que ello aumenta las posibilidades de protección individual y poblacional.

La JGRG y el servicio de seguridad y salud en el trabajo promueven la vacunación completa para el SARS-CoV-2 de todos los servidores.

10.2 DISPOSICIÓN 2: ASEGURAR LA VENTILACIÓN DE LOS CENTROS DE TRABAJO

Establecer controles para disminuir el riesgo de exposición en el centro de

trabajo:

- En el Ositrán, por intermedio de la Jefatura de Logística y Control Patrimonial y el personal del servicio de seguridad y salud en el trabajo, evaluaron las características físicas de cada uno de los ambientes de la entidad, considerando entradas y salidas de aire, flujos de aire, fuentes de ventilación natural y artificial, entre otros.
- Todos los ambientes donde se realizan actividades presenciales deben mantener abiertas las puertas y ventanas, de este modo, se evitará el recurrente contacto con las perillas o manija de las puertas y se permitirá el ingreso de aire nuevo al ambiente.
- En el Ositrán, se estableció el Teletrabajo como una modalidad laboral permanente, encontrándose más del 82% de servidores bajo esta modalidad, el restante de servidores que son los que realizan actividades en modalidad presencial, mantienen todas las medidas preventivas para evitar la difusión de la enfermedad, siguiendo las disposiciones establecidas en el presente plan.
- El Ositrán, por intermedio de la Jefatura de Logística y Control Patrimonial, verificará por intermedio de una empresa proveedora de servicio, si los ambientes de trabajo cuentan con niveles de CO2 en el aire libre, por debajo de la concentración adecuada (400 ppm), para lo cual utilizará la Guía para el uso de medidores de CO2 en ambientes de trabajo. (Anexo N° 11).

10.3 DISPOSICIÓN 3: EVALUACIÓN DEL NIVEL DE RIESGO Y VALORACIÓN DE LA APTITUD DEL SERVIDOR PREVIO AL REGRESO AL CENTRO DE TRABAJO.

Al ingreso de los servidores, el personal del servicio de seguridad y salud en el trabajo estará a cargo de:

- De la identificación del riesgo de exposición a SARS-CoV-2 (COVID-19) de cada puesto de trabajo según el numeral 6.1. "Definiciones Operativas – Puestos de Trabajo con Riesgo de Exposición a COVID-19" conforme a la DIRECTIVA ADMINISTRATIVA N° 349 -MINSA/DGIESP-2024, (la lista está anexa al presente Plan).
- Verificar que los servidores que se reincorporen al trabajo completen la ficha de evaluación de la aptitud para el regreso o reincorporación al trabajo (ficha sintomatológica), conforme al (Anexo 02), que serán entregadas en el tópico institucional y en cada centro de trabajo. Se podrán usar medios digitales para emitir y recibir ambos documentos, en caso algún servidor declare síntomas vinculados a la COVID-19 o declara ser contacto directo u otro, la ficha de evaluación de la aptitud para el regreso o reincorporación al trabajo (ficha sintomatológica) (Anexo 02) deberá ser remitida en el día a los profesionales de la salud de la Sede Central a los correos electrónicos rberrio@ositran.gob.pe y csumari@ositran.gob.pe, dejando constancia del

estado de salud del servidor o servidores, además, deberán acudir a un centro asistencial para evaluación, diagnóstico, tratamiento y emisión del descanso médico si lo amerita.

De corresponder el alta médica del servidor y su reincorporación a sus labores,el profesional de la salud de la empresa emitirá la Ficha de Alta Epidemiológica al área médica del Ositrán.

- De acuerdo a la evaluación de la aptitud del servidor el profesional del servicio de seguridad y salud en el trabajo realiza las recomendaciones para la ubicación del servidor en un puesto de trabajo con riesgo bajo o mediano de exposición al SARS-CoV-2 de corresponder, para proteger la salud del servidor.

- El servidor tiene la obligación de reportar al Servicio de Seguridad y Salud en el Trabajo del Ositrán, si presenta signos y síntomas relacionados a las definiciones de caso COVID-19, en función de las actualizaciones que brinde el Centro Nacional de Epidemiología, Prevención y Control de Enfermedades. Según Flujograma de Comunicación (Anexo 07).

- A todo servidor que cumpla criterios de caso sospechoso, identificado en el centro de trabajo, se indica el aislamiento domiciliario, o es referido al establecimiento de salud de su jurisdicción según corresponda (EsSalud, EPS, MINSA u otro correspondiente). El empleador procede a la identificación de contactos laborales, salvaguardando la identidad del caso, y respetando en todo momento la normativa referida a protección de datos personales.

- Las pruebas de diagnóstico laboratorial las indica sólo el Servicio de Seguridad y Salud en el Trabajo, con el fin de detectar posibles casos o contactos. Para el diagnóstico definitivo, el servidor debe ser evaluado en un centro asistencial donde el médico que atienda el caso brindará tratamiento y la emisión del descanso médico si lo amerita.

- No se recomienda la aplicación de pruebas de laboratorio diagnósticas para vigilancia de síntomas y de contactos de infección por SARS-CoV-2. Su indicación debe hacerse únicamente para aquellos servidores que presentan síntomas compatibles con la COVID-19.

- No deben realizarse pruebas diagnósticas de laboratorio, como PCR o pruebas de detección de antígeno, para definir el alta del paciente. La valoración de las acciones realizadas en el marco de esta Disposición permite al Médico ocupacional del Servicio de Seguridad y Salud en el Trabajo, determinar si el servidor puede reincorporarse a su puesto de trabajo.

- De identificarse un caso sospechoso o de tomar conocimiento de ser contacto directo de un caso confirmado, se procede con las siguientes medidas por parte del profesional de la salud o quien haga sus veces en el centro de

trabajo:

a) El caso sospechoso recibe la indicación de acudir a un establecimiento de salud para su manejo de acuerdo con lo establecido en el Documento Técnico: Manejo ambulatorio de personas afectadas por la COVID-19 en el Perú, aprobado con Resolución Ministerial N° 834-2021/MINSA, o el que haga sus veces.
b) El profesional de la salud realiza el monitoreo de salud de los servidores con diagnóstico confirmado o sospecha que se encuentren en aislamiento domiciliario, por teléfono o sistemas de telemedicina. El seguimiento clínico es registrado en la Ficha F300 (Ficha de seguimiento) del SICOVID-19 del Ministerio de Salud.
c) Para garantizar la vigilancia epidemiológica del servidor en el contexto de la COVID -19, los empleadores que realicen el diagnòstico por pruebas de laboratorio para la infección por SARS -CoV -2 en sus servidores, en sus respectivos tópicos de medicina, salud ocupacional, entre otros, con insumos directamente adquiridos por ellos, deben registrar sus resultados a través del aplicativo de la vigilancia de COVID -19 (Noti web), disponible en: https://app7 .dge.gob.pe/noticovid/ a través del personal de salud encargado.
d) Los profesionales de la salud, del Servicio de Seguridad y Salud en el Trabajo cumple funciones administrativas y preventivo asistenciales especializadas, es el responsable de hacer el seguimiento clínico remoto a los pacientes sospechosos, probables o confirmados de la COVID -19 que cumplan aislamiento domiciliario, y debe hacer el registro correspondiente en la Ficha F300 del SICOVID - 19. Para tal fin el Servicio de Seguridad y Salud en el Trabajo debe solicitar los accesos respectivos a la Oficina General de Tecnologías de la Información del Ministerio de Salud. Esta labor puede ser realizada por personal médico especialista de Infectología, Neumología o quien haga sus veces del establecimiento de salud más cercano al centro de trabajo.
e) El tiempo de descanso médico de casos sospechosos, probables o confirmados de la COVID-19 será definido por el médico tratante de acuerdo a la condición clínica del paciente, pudiendo extenderse excepcionalmente, de acuerdo a evaluación médica debidamente certificada (Certificado de Incapacidad Temporal para el Trabajo (CITT), Certificado Médico del Colegio Médico del Perú o certificado de una IPRESS pública o privada).
f) El alta de los servidores sospechosos o confirmados por la COVID -19 debe hacerse a través del formato de ALTA de la Ficha F300 del SICOVID-19.
g) En el caso de pacientes moderados o graves (hospitalizados), con diagnóstico confirmado de la COVID-19, el alta la establece el Médico tratante. Su reincorporación se realiza de acuerdo con la evaluación realizada por el Servicio de Seguridad y Salud en el Trabajo, de acuerdo con las normas vigentes.
h) En caso de servidores hospitalizados es pertinente contar con información del familiar a través del área de bienestar social del centro de trabajo, no es necesario el seguimiento clínico. Los accesos a la

Ficha F300 (Ficha de seguimiento) se proporcionan a través de la Mesa de Ayuda del Ministerio de Salud.

i) Ositrán brinda material e información sobre la prevención del contagio de la COVID-19, sobre medidas de higiene y cuidado que debe llevar en casa.

j) Ante un caso sospechoso o probable de la COVID-19, el establecimiento de salud o empleador procede con otorgar el certificado médico o certificado de incapacidad temporal, con indicación firmada por el Médico tratante, Médico ocupacional o Médico a cargo de la vigilancia de la salud, por el tiempo considerado para el aislamiento, para proteger y resguardar la salud e integridad del servidor, así como del resto de los servidores de la institución.

10.4 DISPOSICIÓN 4: PUNTOS DE LAVADO O DESINFECCIÓN DE MANOS

Antes, durante y después de la jornada laboral, los servidores de las instalaciones de la sede central, centros de orientación y oficinas desconcentradas de la entidad, deberán acercarse a los servicios higiénicos, los cuales están equipados con lavadero, caño con conexión a agua potable, jabón líquido o jabóndesinfectante, papel toalla y alcohol en gel al 70%, para el uso libre de lavado y desinfección de manos.

Los servidores que asisten a las instalaciones de Sede Central, deberán realizar el lavado y desinfección de manos en el lavadero más cercano, siguiendo las recomendaciones descritas en la presente disposición.

El lavado de manos y desinfección debe realizarse:

- Al llegar de casa, al centro de trabajo, antes de empezar sus actividades y viceversa.
- Luego de toser, estornudar o limpiarse la nariz.
- Antes y después de comer o manipular alimentos.
- Antes y después de cambiarse una mascarilla.
- Después de tocar objetos o superficies contaminadas (residuos sólidos, dinero, pasamanos de las unidades de servicio de transporte, botones del ascensor, cajeros, barandas, manijas de puertas, entre otros).
- Antes de retirarse del centro de trabajo.

Se cuenta con carteles sobre la ejecución adecuada del método de lavado correcto o uso del alcohol para la higiene de manos. Se debe tener en cuenta que el uso de alcohol en gel/líquido no reemplaza al lavado de manos.

Los servidores deberán lavarse las manos hasta el antebrazo con agua y jabón por lo menos **durante 20 segundos**. Asimismo, deberán utilizar gel desinfectante (ubicado en lugares estratégicos en cada piso); tomándose en cuenta que esto no debe reemplazar al lavado de manos.

Al utilizar papel higiénico o pañuelos descartables, los servidores deberán

asegurarse de desecharlos dentro del basurero de los servicios higiénicos y luego lavarse las manos **durante 20 segundos**.

10.5 DISPOSICIÓN 5: SENSIBILIZACIÓN DE LA PREVENCIÓN DEL CONTAGIO EN EL CENTRO DE TRABAJO

Como medida para asegurar ambientes saludables frente a la COVID-19, el Ositrán asegura las siguientes actividades para la sensibilización a los servidores:

- Realizar capacitaciones sobre COVID-19 y las medidas de disminución del riesgo de infectarse por SARS-CoV-2 en el centro de trabajo, en la comunidad y en el hogar
- Sensibilizar en la importancia de reportar tempranamente la presencia de sintomatología de la COVID-19 y el auto reporte de casos intradomiciliarios o intrafamiliar de la COVID 19 constatado por un profesional de la salud.
- Informar de los beneficios de la vacunación en la prevención de formas graves de la enfermedad y la disminución de probabilidades de morir por la infección del virus SARS- CoV-2.
- Dichas actividades deben darse a la totalidad de los servidores, en adición al marco del cumplimiento de capacitación mínima establecida porla Ley N° 29783, Ley de Seguridad y Salud en el Trabajo.

Medios y acciones:

El Plan para la Vigilancia, Prevención y Control del COVID-19 en el Ositrán será enviado por correo electrónico, mediante comunicado interno, a todos los servidores, para su conocimiento y aplicación.

Los servidores podrán realizar consultas respecto al COVID-19, a los profesionales de salud de manera presencial en el tópico de la entidad o por medios electrónicos (rberrio@ositran.gob.pe, csumari@ositran.gob.pe).

Todos los servidores tienen a su disposición, información sobre el COVID-19 y los medios de protección personal, a través de los comunicados internos virtuales y carteles en lugares visibles.

Discriminación y prejuicios

La entidad protegerá la privacidad de los servidores, así como la vigilancia de que su salud no sea utilizada con fines discriminatorios, ni de cualquier otra índole.

Evitar el estigma y discriminación y, sobre todo, evitar la propagación del pánico en el ambiente de trabajo, por cualquier medio de comunicación.

10.6 DISPOSICIÓN 6: MEDIDAS PREVENTIVAS DE APLICACIÓN COLECTIVA

Ositrán desarrollará acciones dirigidas a reducir el riesgo de transmisión del SARS-

CoV-2 en el ambiente laboral, las cuales se implementarán teniendo en cuenta los siguientes aspectos enfocados en la jerarquía de controles.

10.6.1 Evitar la exposición a SARS-CoV-2, en el puesto de trabajo:

a) Las reuniones de trabajo o capacitación deben ser preferentemente virtuales, cuando sea posible.
b) Se recomienda, la protección de los servidores con factores de riesgo en puestos de atención al cliente, mediante el empleo de mascarilla correspondiente cuando el servidor no pueda ser reubicado en un puesto de menor riesgo.

10.6.2 Establecer controles administrativos:

a) Controlar el aforo convencional no se sobrepase durante toda la jornada laboral.

10.6.2 Establecer el uso de equipos de protección personal:

a) El uso de los Equipos de Protección Personal (EPP) en el puesto de trabajo es de acuerdo con el nivel de riesgo, debiéndose garantizar su uso correcto y seguro, así como su disponibilidad.
b) Se sugiere el uso de una mascarilla KN95, en los puestos de trabajo de atención al cliente y oficinas desconcentradas, de acuerdo con las indicaciones y recomendaciones del Ministerio de Salud.
c) En sede central del Ositrán, el uso de la mascarilla KN95, **no es obligatorio, por lo que cada servidor podrá utilizarla a voluntad propia**.
d) El tópico de salud ocupacional cuenta con tachos de basura con bolsa roja para el acopio de Equipos de Protección Personal (EPP) usados, material descartable posiblemente contaminado (mascarillas u otros), para un manejo adecuado, como material contaminado, conforme lo establecido en la normativa vigente aprobada por la Resolución Ministerial N° 456-2020-MINSA sobre la Norma Técnica de Salud N° 161-MINSA/2020/DGAIN o la que haga sus veces.

Durante las labores en campo:

Durante las labores en campo, además del procedimiento establecido en el presente Plan, los servidores deberán alinearse a los protocolos y procedimientos que, de ser el caso, las Entidades Prestadoras de las Concesiones hayan establecido, para lo cual deberán informar a la JLCP y a los profesionales de la salud del Ositrán a fin de que puedan gestionar las atenciones de los requerimientos especiales, si los hubiera.

Asimismo, la “ficha de evaluación de la aptitud para el regreso o reincorporación al trabajo (ficha sintomatológica) (Anexo 02)”, deberá ser

remitida al profesional de la Salud al retorno o reincorporación laboral de cada servidor, sin perjuicio de ello, en caso algún servidor presente síntomas vinculados a COVID-19 o haya tenido contacto directo u otro con personas diagnosticadas con COVID-19, deberán remitir la mencionada Ficha en el día a los profesionales de la salud de la Sede Central a los correos electrónicos (rberrio@ositran.gob.pe y csumari@ositran.gob.pe), dejando constancia de su estado de salud, para el seguimiento, apoyo y adopción de medidas correspondientes.

Traslado a la Sede Central del Ositrán:

El "personal en campo" deberá cumplir los protocolos de sanidad establecidos para la Sede Central del Ositrán, en caso se requiera su presencia en la misma.

Otras acciones:

Acciones e implementación de medidas para la protección en espacios en los cuales se brinde atención al ciudadano:

- Uso de mascarilla KN95 durante la jornada laboral que implique atención al público.
- Desinfección permanente de teléfonos y equipos puestos a disposición de la ciudadanía.
- Se ubicará señalética visible para la atención de servicios de atención preferente y servicios a personas con discapacidad, dentro del grupo de vulnerabilidad y de riesgo establecidos por el MINSA.

Otras acciones adoptadas en los ambientes de las instalaciones del Ositrán.

El servidor y todo aquel que vaya a ingresar a las instalaciones del Ositrán, deberá lavarse las manos en el lavadero más cercano, asimismo, podrá hacer uso de los dispensadores de alcohol en gel para proceder a la desinfección.

Para el caso del ingreso a las instalaciones del Ositrán por parte de visitas y proveedores de bienes y servicios ya sea como peatones o con vehículos, estos deberán ceñirse a los procedimientos sanitarios del presente Plan. Siendo responsable de hacer cumplir esta disposición, una vez que la visita o proveedor ingresó a las instalaciones, el servidor o unidad de organización que atenderá la visita, proveedor o servicio.

10.6 DISPOSICIÒN 7: MEDIDAS DE PROTECCIÓN PERSONAL

El Ositrán asegura la disponibilidad de los equipos de protección personal para COVID-19 e implementa las medidas para su uso correcto, en coordinación y según lo determine el profesional de salud, estableciendo como mínimo las medidas recomendadas por organismos nacionales e internacionales tomando encuenta el riesgo de los puestos de trabajo para exposición ocupacional al SARS CoV-2, cumpliendo los principios de la Ley de Seguridad y Salud en el Trabajo (Anexo 06).

El uso de equipo de protección respiratoria (FFP2, N95 o equivalentes) es de uso exclusivo para servidores de salud que trabajan en ambientes con muy alto y alto riesgo de exposición biológica al virus SARS-CoV-2 que causa la COVID-19.

De acuerdo con el nivel de riesgo de los puestos de trabajo, se deben considerar los mínimos estándares de protección respiratoria. Los servidores de los puestos de atención al cliente y oficinas desconcentradas, deben cumplir con el mínimo estándar de una mascarilla KN95, el Ositrán debe asegurarse de brindarle las mascarillas necesarias que cumplan el criterio establecido por la Autoridad Nacional de Salud y en la cantidad y frecuencia necesaria.

XI. DISPOSICIONES INTERNAS:

Todo Servidor deberá identificarse con su DNI y/o su fotocheck, lo cual facilitaráel control de ingreso.

a. HORARIO DE TRABAJO: la Gerencia de Administración con el propósito de mitigar el posible contagio del COVID-19 y evitar la aglomeración de personal que realice trabajo presencial, el Ositrán ha propuesto los siguientes horarios de lunes a viernes, **los cuales serán flexibles y movibles:**

- Ingreso de 8:00 am. y salida 5:00 pm.
- Ingreso de 9:00 am. y salida 6:00 pm.

b. CONTROL DE ASISTENCIA:

En el caso de los servidores que desarrollan actividades presenciales: Las computadoras tendrán acceso a un portal de marcación por el cual el servidor registrará el inicio y término de sus labores diarias.

Los gerentes o jefes de unidades de organización determinarán las siguientes modalidades de trabajo aplicables a las funciones y actividades de la entidad, de acuerdo con la priorización que realicen:

- **Teletrabajo** es la prestación de servicios sujeto a subordinación, con la presencia física del servidor en su domicilio o lugar de aislamiento domiciliario. Aplica preferentemente al servidor que pertenece a los grupos de riesgo, evitando su presencia en las instalaciones de la entidad, así como a los servidores que la entidad establezca para realizar su labor desde casa o lugar de aislamiento.

- **Trabajo presencial**, implica la asistencia física del servidor durante la jornada de trabajo.

- **Trabajo en modalidades mixtas**, implica la combinación de días en trabajo presencial, en trabajo remoto, teletrabajo y/o licencia con goce de haber compensable, alternando las modalidades en atención a las necesidades de la entidad.

c. HORARIO DE REFRIGERIO

El horario de refrigerio se encuentra establecido en el Reglamento Interno deServidores Civiles del Ositrán, el cual consiste en una (01) hora, entre la 1:00 p.m. y las 3:00 p.m.

Los servidores podrán hacer uso de las instalaciones del comedor, respetando el aforo.

d. ACTUACIÓN SANITARIA PARA LABORES DEL PERSONAL EN CAMPO

- En caso que el "personal en campo" presente síntomas del COVID-19 o declara ser contacto directo u otro, la ficha de evaluación de la aptitud para el regreso o reincorporación al trabajo (ficha sintomatológica) (Anexo 02) deberá ser remitida en el día a los profesionales de la salud de la Sede Central a los correos electrónicos rberrio@ositran.gob.pe y csumari@ositran.gob.pe.
- De ser necesario el traslado del "personal en campo", se deberá seguir las indicaciones del profesional de la salud del Ositrán.
- En el caso de personal que presente síntomas del COVID-19**,** se procederá a la identificación de las personas que hayan estado próximas al supuesto afectado, si se confirma que el servidor sospechoso ha sido diagnosticado con COVID-19, todos los servidores que mantuvieron contacto directo serán monitoreados por el profesional de la salud del Ositrán, quien evaluará su condición.

e. MEDIDAS DE PROTECCIÓN A LA SALIDA DE LABORAR (FIN DE JORNADA LABORAL)

Al final de la jornada los servidores deberán retirarse de forma ordenada, evitando aglomeraciones en las áreas comunes.

f. OCURRENCIAS DURANTE LA JORNADA DE TRABAJO

Si dentro de las instalaciones de la entidad algún servidor presentase síntomas relacionados al COVID-19, deberá llamar vía telefónica al profesional de la salud,a su jefe inmediato o a un superior, o a la JGRH, quienes coordinarán con el profesional de la salud a fin de realizar las acciones correspondientes para la atención y su retiro inmediato de la entidad.

En el caso que una persona se encuentre mal de salud y no pueda movilizarse por sus propios medios, esperará en el lugar donde se encuentra hasta ser atendido por el profesional de la salud, quien deberá aislar la zona y brindará la atención primaria debiendo llamar a una ambulancia. El profesional de la salud deberá de usar los EPP para tratar pacientes sospechosos con COVID-19.

Una vez que la persona se retire de la entidad**,** se procederá a la identificación de lsas personas que hayan estado próximas al supuesto afectado, y toda el área deberá ser totalmente desinfectada. Si se confirma que la persona ha sido diagnosticada con COVID-19, todas las personas que se encontraban en el entorno del puesto de trabajo del servidor del Ositrán serán monitoreadas debiendo utilizar mascarilla KN95 para realizar sus labores y comunicando de manera inmediata a los profesionales de la salud, si presentasen algún síntoma sugestivo a Covid-19.

XII. DISPOSICIÓN COMPLEMENTARIA

Para el caso de aspectos no contemplados en el presente Plan, deberán remitirse a las normas específicas sobre la materia, accesorias o conexas, a fin de determinar la absolución o resolver alguna duda o controversia.

XIII. RESPONSABILIDADES DEL CUMPLIMIENTO DEL PLAN

El Ositrán, a través de la Gerencia General y la Gerencia de Administración, es responsable de implementar y supervisar el cumplimiento del presente Plan.

Todos los servidores son responsables del cumplimiento de las disposiciones contenidas en el presente Plan, independientemente del régimen laboral o contractual, así como las modalidades formativas, bajo responsabilidad funcional.

Los profesionales de la Salud son los responsables de realizar el seguimiento y gestionar la notificación del servidor positivo a la entidad de salud correspondiente (MINSA, EsSalud, EPS, aseguradoras de salud o IAFAS) para elmanejo del paciente infectado.

ACCIÓN	RESPONSABILIDAD	RESPONSABLE
Planificación	Gestionará y otorgará el presupuesto a fin de cumplir con la implementación del presente plan.	GPP
Adquisiciones	Se encargará de la compra y adquisición de los bienes y servicios necesarios para la implementación del presente plan.	GA – JLCP
Prevención	Se encargará de la vigilancia y aplicación de las medidas de limpieza, desinfección y otras, a fin de prevenir el contagio y la propagación del COVID-19.	GA-JGRH-JLCP
Monitoreo	Se encargará de monitorear el cumplimiento de lo establecido en el presente Plan	CSST
Control	Se encargará de controlar que se cumpla con lo dispuesto en las disposiciones establecidas en el plan.	GA-JGRH
Gestión y vigilancia	Se encargará de la gestión y vigilancia de la salud de los servidores y personas.	Profesionales de la salud – Médico y enfermera

XIV. PRESUPUESTO Y PROCESO DE ADQUISICIÓN DE INSUMOS PARA EL CUMPLIMIENTO DEL PLAN

En base a lo descrito en el presente Plan, se detallan los aspectos relevantes respecto a la adquisición de insumos y de servicios que permitan el cumplimiento del mismo.

PRESUPUESTO
PLAN DE VIGILANCIA, PREVENCIÓN Y CONTROL DEL COVID-19 EN EL OSITRÁN

N°	CONCEPTO	PRECIO UNITARIO	CANT.	UNIDAD DE MEDIDA	PRECIO TOTAL INC IGV S/	COMENTARIOS
1	Mascarillas KN95	1.0	2500	Unidad	2,950	Para la entrega a los servidores que pertenecen a los siguientes puestos de trabajo: Atención al cliente y servidores de las oficinas descentralizadas que realizan su trabajo a nivel nacional
				TOTAL	**2,950**	
Precios referenciales. Presupuesto sujeto a la disponibilidad de los recursos financieros.						

XV. DOCUMENTO DE APROBACIÓN DEL COMITÉ DE SEGURIDAD Y SALUD EN EL TRABAJO

El Comité de Seguridad y Salud en el Trabajo del Ositrán es responsable de la aprobación del presente Plan para la Vigilancia, Prevención y Control del COVID – 19 en el Ositrán. Dicha aprobación quedará materializada en el Acta de la sesión correspondiente, debidamente suscrita por los miembros del mencionado Comité.

ANEXO 01

NÓMINA DE SERVIDORES POR RIESGO DE EXPOSICIÓN AL COVID-19

REGISTRO DE PERSONAL ACTIVO RIESGO BAJO DE EXPOSICIÒN			
Nº	**PERSONAL**	**CARGO**	**UNIDAD ORGANICA**
1	ABANTO LIMO GONZALO ALEJANDRO	PRACTICANTE	JEFATURA DE ASUNTOS JURÍDICO REGULATORIOS Y ADMINISTRATIVOS
2	ABREU HIDALGO AMERICO OMAR	COORDINADOR DE SISTEMAS DE INFORMACIÓN	JEFATURA DE TECNOLOGÍAS DE LA INFORMACIÓN
3	ACOSTA ARBILDO NELVI	SECRETARIA	GERENCIA DE SUPERVISIÓN Y FISCALIZACIÓN
4	AGUILAR GAMIO FIDEL EVERTH	SUPERVISOR IN SITU	JEFATURA DE CONTRATOS PORTUARIOS
5	AGURTO ACUÑA MAICKY NOELIA	APOYO EN TESORERIA	JEFATURA DE TESORERÍA
6	ALARCON DIAZ WALTER	ESPECIALISTA EN CONTRATACIONES	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
7	ALARCON IBARGUEN JULIO CESAR	SUPERVISOR IN SITU DEL CONTRATO DE CONCESIÓN DEL TRAMO VIAL: OVALO CHANCAY / DV. VARIANTE PASAMAYO - HUARAL - ACOS	JEFATURA DE CONTRATOS DE LA RED VIAL
8	ALARCON MORALES ANDRE JESUS	ANALISTA EN GESTIÓN DE PROYECTOS DE DESARROLLO DE SOFTWARE	JEFATURA DE TECNOLOGÍAS DE LA INFORMACIÓN
9	ALCALDE POMA SOFIA EMPERATRIZ	ESPECIALISTA AMBIENTAL	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
10	ALEGRE BUSTAMANTE SANDY ANEL	ANALISTA LEGAL	GERENCIA DE ATENCIÓN AL USUARIO
11	ALFERES FLORES RUBY DARA	PRACTICANTE	GERENCIA DE SUPERVISIÓN Y FISCALIZACIÓN
12	ALIAGA CALDERON CARLOS RICARDO	JEFE DE CONTRATOS PORTUARIOS	JEFATURA DE CONTRATOS PORTUARIOS
13	ALVARADO CARMEN MANUEL IGNASIO	AUXILIAR EN CAPTURA DE IMÁGENES DIGITALIZADAS	OFICINA DE GESTIÓN DOCUMENTARIA
14	ALVARADO ROJAS ITALO ALBUCAR	SUPERVISOR CONTRACTUAL	JEFATURA DE CONTRATOS DE LA RED VIAL
15	ALVAREZ ESTRADA LUIS EDUARDO	SUPERVISOR DE INVERSIONES PORTUARIAS I	JEFATURA DE CONTRATOS PORTUARIOS
16	ALVAREZ GUILLEN JOANA PATRICIA	ESPECIALISTA EN GOBIERNO DIGITAL Y GESTIÓN DE PROYECTOS	JEFATURA DE TECNOLOGÍAS DE LA INFORMACIÓN
17	ALVAREZ HUAMAN JUNIOR MISSAEL	ANALISTA DE ESTUDIOS ECONÓMICOS II	JEFATURA DE ESTUDIOS ECONÓMICOS
18	ALVAREZ LUQUE IRIS SARITA	ASISTENTE SECRETARIAL	JEFATURA DE FISCALIZACIÓN
19	ALVAREZ SUAREZ PIERO RIQUIER	ASISTENTE TÉCNICO	JEFATURA DE CONTRATOS DE LA RED VIAL
20	AMES SANTILLAN JUAN CARLOS	ANALISTA SENIOR REGULATORIO FINANCIERO	GERENCIA DE REGULACIÓN Y ESTUDIOS ECONÓMICOS
21	ANGELES LIZA ANA PATRICIA	ANALISTA EN GESTIÓN DEL TRÁMITE DOCUMENTARIO	OFICINA DE GESTIÓN DOCUMENTARIA
22	APARICIO YAMASHIRO BERTHA	Jefe de Atención al Usuario Intermedio (e)	GERENCIA DE ATENCIÓN AL USUARIO
23	ARAMBURU GARCIA ROSA MARIELA	ASESOR TÉCNICO	GERENCIA GENERAL
24	ARANDA CHAVEZ WILSON	SUPERVISOR IN SITU PARA EL SEGUNDO GRUPO DE AEROPUERTOS DE PROVINCIA PARA AREQUIPA, JULIACA Y TACNA	JEFATURA DE CONTRATOS AEROPORTUARIOS
25	AREQUIPEÑO BUSTOS DIEGO ALONSO	PRACTICANTE	JEFATURA DE GESTIÓN DE RECURSOS HUMANOS
26	ARRESCURRENAGA SANTISTEBAN ANGELA	GERENTE DE ATENCIÓN AL USUARIO (E)	GERENCIA DE ATENCIÓN AL USUARIO
27	ARTOLA GRADOS JORGE HERNAN	ABOGADO SENIOR	GERENCIA DE SUPERVISIÓN Y FISCALIZACIÓN
28	ASCURRA ZUÑIGA CESAR DAVID	AUDITOR I	ÓRGANO DE CONTROL INSTITUCIONAL
29	ASPILCUETA RUBIO MELISSA MARINA	JEFE DE LA OFICINA DESCONCENTRADA DE AREQUIPA	OFICINA DESCONCENTRADA DE AREQUIPA
30	ASTUDILLO HURTADO ANA DEL ROSARIO	ESPECIALISTA LEGAL EN MATERIA ADMINISTRATIVA	PROCURADURÍA PÚBLICA

31	AVENDAÑO VARIAS DANIEL MARTIN	SUPERVISOR DE INVERSIONES DE LA RED VIAL I	JEFATURA DE CONTRATOS DE LA RED VIAL
32	AYALA FIGUEROA WALTHER ENRIQUE	ABOGADO SENIOR	JEFATURA DE FISCALIZACIÓN
33	BALLADARES SANDOVAL JESUS JAVIER	ESPECIALISTA EN CONTROL PREVIO I	JEFATURA DE CONTABILIDAD
34	BALLARTA FUENTES KERLY NORMA	ASISTENTE LEGAL EN MATERIA ADMINISTRATIVA Y GESTIÓN PÚBLICA	PROCURADURÍA PÚBLICA
35	BARRERA CHAVEZ JUANA LUISA	SECRETARIA	JEFATURA DE CONTRATOS DE LA RED VIAL
36	BARRIA RODRIGUEZ LUPE ENITH	SUPERVISOR ECONÓMICO FINANCIERO DE LA RED VIAL II	JEFATURA DE CONTRATOS DE LA RED VIAL
37	BARROSO CARRILLO VANESSA ERIKA	ESPECIALISTA EN TRÁMITE DOCUMENTARIO	OFICINA DE GESTIÓN DOCUMENTARIA
38	BAZALAR HUAMAN MARIA DEL ROSARIO	COORDINADOR DE LA OFICINA DE COMUNICACIÓN CORPORATIVA	OFICINA DE COMUNICACIÓN CORPORATIVA
39	BECERRA SILVA WILFREDO	ANALISTA DE CONTRATO DE LA RED VIAL I	JEFATURA DE CONTRATOS DE LA RED VIAL
40	BEJAR PEZO ALICE KARINA	ABOGADO	PROCURADURÍA PÚBLICA
41	BELLIDO PASTOR MARIA EUGENIA	ESPECIALISTA EN COMUNICACIÓN EXTERNA	OFICINA DE COMUNICACIÓN CORPORATIVA
42	BELLO MASIAS LUIS ALBERTO	SUPERVISOR(A) IN SITU DE LOS AEROPUERTOS DE TUMBES, PIURA, TALARA Y CHICLAYO	JEFATURA DE CONTRATOS AEROPORTUARIOS
43	BENGOA ACHATA JUAN CARLOS	ANALISTA PROGRAMADOR DE SISTEMAS SENIOR	JEFATURA DE TECNOLOGÍAS DE LA INFORMACIÓN
44	BENITES RUIZ PAOLA MONICA	ESPECIALISTA EN MEJORA CONTINUA	GERENCIA DE PLANEAMIENTO Y PRESUPUESTO
45	BERRIO CARMELINO DARWIN RAFAEL	MÉDICO	JEFATURA DE GESTIÓN DE RECURSOS HUMANOS
46	BRAVO SAAVEDRA CARLOS ALBERTO	APOYO ESPECIALIZADO DE PRESUPUESTO	GERENCIA DE PLANEAMIENTO Y PRESUPUESTO
47	BRICEÑO AGURTO LUIS ALBERTO	COORDINADOR IN SITU DE LA CONCESIÓN DEL AEROPUERTO INTERNACIONAL JORGE CHAVEZ (AIJC)	JEFATURA DE CONTRATOS AEROPORTUARIOS
48	BRICEÑO SALVADOR DIANA CAROLINA	ANALISTA EN CONTRATACIONES	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
49	BRINGAS CALDERON OSCAR EDUARDO	ANALISTA EN PROGRAMACIÓN	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
50	BROUSSET MENDOZA RICARDO ALBERTO	ESPECIALISTA LEGAL EN MATERIA SANCIONADORA	JEFATURA DE FISCALIZACIÓN
51	BUSTAMANTE CHAVEZ RICHARD	ANALISTA ECONÓMICO	JEFATURA DE CONTRATOS PORTUARIOS
52	CABRERA CARRILLO MIGUEL ANGEL	SUPERVISOR DE INVERSIONES DE LA RED VIAL I	JEFATURA DE CONTRATOS DE LA RED VIAL
53	CABRERA MENDOZA ALFREDO IDELBERTO	AUXILIAR DE TRANSPORTE	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
54	CACERES TAPIA NANCY ISABEL	RECEPCIONISTA	PROCURADURÍA PÚBLICA
55	CADILLO ANGELES GLORIA ZOILA	ASESOR EN DIRECCIÓN ESTRATÉGICA	PRESIDENCIA EJECUTIVA
56	CAIPO TRUJILLO CESAR ALFREDO	SUPERVISOR PORTUARIO	JEFATURA DE CONTRATOS PORTUARIOS
57	CALDAS CABRERA DAYSI MELINA	JEFE DE REGULACIÓN	GERENCIA DE REGULACIÓN Y ESTUDIOS ECONÓMICOS
58	CALDERON MARQUEZ JORGE LUIS	ANALISTA EN ECONOMÍA	GERENCIA DE ATENCIÓN AL USUARIO
59	CALLE ESPINOZA ROSSMERY	ESPECIALISTA EN OPERACIONES FINANCIERAS I	JEFATURA DE GESTIÓN DE RECURSOS HUMANOS
60	CALLE MORALES KATHERIN AYDE	ASISTENTE DE PRENSA	OFICINA DE COMUNICACIÓN CORPORATIVA
61	CALVO JAUREGUI JHOEL	ESPECIALISTA AMBIENTAL	JEFATURA DE CONTRATOS DE LA RED VIAL
62	CAMPOS FLORES FLOR NOELIA	AUXILIAR ADMINISTRATIVO	JEFATURA DE CONTRATOS AEROPORTUARIOS
63	CAMPOS FLORES LUIS DANILO	JEFE DE CONTRATOS AEROPORTUARIOS	JEFATURA DE CONTRATOS AEROPORTUARIOS
64	CAMPOS VALDIVIEZO JORGE ANTONIO	ASISTENTE DE ALMACÉN Y CONTROL PATRIMONIAL	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
65	CANDELA TEPE JULIO MARTIN	ASISTENTE DE OPERACIONES PORTUARIAS	JEFATURA DE CONTRATOS PORTUARIOS
66	CANTA VENTURA HARDY LUIS	SUPERVISOR Y COORDINADOR IN SITU PARA LA CONSTRUCCIÓN DE OBRAS PORTUARIAS DEL TERMINAL PORTUARIO DE MATARANI	JEFATURA DE CONTRATOS PORTUARIOS
67	CANTILLO ATALITO ELIEM PATRICIA	ANALISTA DE CENTRO DE ORIENTACIÓN DE LA LÍNEA 1	GERENCIA DE ATENCIÓN AL USUARIO
68	CÁRDENAS PARI FERNANDO JOSÉ	PRACTICANTE	PROCURADURÍA PÚBLICA
69	CARRILLO REATEGUI JACKELINE	ABOGADO	SECRETARÍA TECNICA DE LOS TRIBUNALES DEL OSITRAN

70	CARRION OLAZABAL ROSEMIERE VICENTA	ASISTENTA SOCIAL	JEFATURA DE GESTIÓN DE RECURSOS HUMANOS
71	CASTAÑEDA CHAVARRY ZOILA ROSA	ESPECIALISTA TRIBUTARIO II	GERENCIA DE SUPERVISIÓN Y FISCALIZACIÓN
72	CASTILLO MAR RUTH ELIANA	ABOGADO SENIOR	GERENCIA DE REGULACIÓN Y ESTUDIOS ECONÓMICOS
73	CASTILLO ORMEÑO GIULIANA PATRICIA	ESPECIALISTA LEGAL PARA CONTRATOS DE CONCESIÓN DE LA RED VIAL	JEFATURA DE CONTRATOS DE LA RED VIAL
74	CASTILLO ROMERO ELMER ANDRES	ANALISTA EN CONTRATACIONES	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
75	CASTILLO SIFUENTES ISABEL FABIOLA	ABOGADO	GERENCIA DE PLANEAMIENTO Y PRESUPUESTO
76	CASTILLON FAJARDO NATALIA SOLEDAD	ASISTENTE TÉCNICO DEL CONSEJO DIRECTIVO	GERENCIA DE PLANEAMIENTO Y PRESUPUESTO
77	CASTRO CUBA LEON JAVIER ERNESTO	JEFE DE LA OFICINA DESCONCENTRADA DE CUSCO	OFICINA DESCONCENTRADA DE CUSCO
78	CASTRO HORNA ALEXANDER MITCHELL	ESPECIALISTA EN BIBLIOTECA Y CENTRO DE DOCUMENTACIÓN	OFICINA DE GESTIÓN DOCUMENTARIA
79	CASTRO RUIZ ERIKA	APOYO ADMINISTRATIVO	SECRETARÍA TECNICA DE LOS TRIBUNALES DEL OSITRAN
80	CCALLO CCARI JHONATAN JOSE DAVID	PRACTICANTE	GERENCIA DE REGULACIÓN Y ESTUDIOS ECONÓMICOS
81	CERDA HERNANDEZ ROSA MARIA	ESPECIALISTA LEGAL TRIBUTARIO II	GERENCIA DE SUPERVISIÓN Y FISCALIZACIÓN
82	CHACON ARELLANO OSWALDO ALBERTO	ASISTENTE TÉCNICO DE ESTACIONES Y TRENES	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
83	CHARAPAQUI PAITAN KAREN LEIDY	Auditor III	ÓRGANO DE CONTROL INSTITUCIONAL
84	CHAUPIS RODRIGUEZ ADA VANESSA	ESPECIALISTA EN INTEGRACIÓN CONTABLE I	JEFATURA DE CONTABILIDAD
85	CHAVARRIA MENDOZA OSCAR ROBERTO	SUPERVISOR IN SITU	JEFATURA DE CONTRATOS DE LA RED VIAL
86	CHAVESTA TITO LUIS ANGEL	PRACTICANTE	OFICINA DE GESTIÓN DOCUMENTARIA
87	CHAVEZ ARAUJO JAIME ENRIQUE	SUPERVISOR IN SITU II TRAMO 4: INAMBARI - AZÁNGARO	JEFATURA DE CONTRATOS DE LA RED VIAL
88	CHAVEZ MANRRIQUE DAVID ANTONIO	ESPECIALISTA DE OPERACIONES PORTUARIAS	JEFATURA DE CONTRATOS PORTUARIOS
89	CHAVEZ MONTOYA CARLA GABRIELA	ANALISTA LEGAL	GERENCIA DE ATENCIÓN AL USUARIO
90	CHAVEZ QUIROZ FELIPE GUSTAVO	COORDINADOR EN PRESUPUESTO	GERENCIA DE PLANEAMIENTO Y PRESUPUESTO
91	CHEN CHEN THOU SU	GERENTE DE ADMINISTRACIÓN	GERENCIA DE ADMINISTRACIÓN
92	CHERO GRANADOS ALISSON GABRIELA	PRACTICANTE	JEFATURA DE TESORERÍA
93	CHERO LOPEZ ANNIE YULEYDY	ANALISTA LEGAL	JEFATURA DE ASUNTOS JURÍDICO CONTRACTUALES
94	CHINCHA CAMPRUBI BORIS MARIO	COORDINADOR DE INFRAESTRUCTURA TECNOLÓGICA	JEFATURA DE TECNOLOGÍAS DE LA INFORMACIÓN
95	CHOCANO PORTILLO JAVIER EUGENIO MANUEL JOS	JEFE/A DE LA GERENCIA DE ASESORÍA JURÍDICA	GERENCIA DE ASESORÍA JURÍDICA
96	CHUMACERO ASENCION EVELYN EDITH	COORDINADORA DEL EQUIPO FUNCIONAL DE HIDROVÍAS	GERENCIA DE SUPERVISIÓN Y FISCALIZACIÓN
97	CIURLIZZA VILLAR NADIA NAIR	APOYO ADMINISTRATIVO	JEFATURA DE TESORERÍA
98	CONDORI CAPIA KEVIN	ANALISTA LEGAL	SECRETARÍA TECNICA DE LOS TRIBUNALES DEL OSITRAN
99	COPAJA CHAMBILLA MAURICIO RAFAEL	PRACTICANTE	SECRETARÍA TECNICA DE LOS TRIBUNALES DEL OSITRAN
100	CORDOVA CHUQUIVAL BORIS ANDRE	SUPERVISOR ECONÓMICO FINANCIERO FERROVIARIO I	JEFATURA DE CONTRATOS PORTUARIOS
101	CORILLOCLLA GUTARRA LILIANA GIOVANNA	ESPECIALISTA LEGAL TRIBUTARIO I	GERENCIA DE SUPERVISIÓN Y FISCALIZACIÓN
102	CORNEJO AMEZAGA CLAUDIA BEATRIZ	ESPECIALISTA LEGAL	GERENCIA DE REGULACIÓN Y ESTUDIOS ECONÓMICOS
103	CORONADO SANCHEZ JUAN ANTONIO	ESPECIALISTA DE BASE DE DATOS Y PROGRAMACIÓN II	JEFATURA DE TECNOLOGÍAS DE LA INFORMACIÓN
104	CORRALES DURAND MIGUEL ANGEL	SUPERVISOR IN SITU TRAMO 1-A - SAN JUAN DE MARCONA - CHALHUANCA	JEFATURA DE CONTRATOS DE LA RED VIAL
105	COSSÍO CHÁVEZ SARA BETSABÉ	ASISTENTE EN ADMIISTRACIÓN DE PERSONAL	JEFATURA DE GESTIÓN DE RECURSOS HUMANOS
106	COSSIO TAPIA MARCO ANTONIO LEONCIO	SUPERVISOR IN SITU II - IIRSA SUR, TRAMO 2: URCOS - INAMBARI	JEFATURA DE CONTRATOS DE LA RED VIAL

107	COVEÑAS ASCURRA FREDDY FERNANDO	CHOFER	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
108	DAGA LAZARO ROBERTO CARLOS	ANALISTA DE REGULACIÓN EN MATERIA DE PUERTOS I	JEFATURA DE REGULACIÓN
109	DAVILA ROSALES ROSARIO DEL PILAR	SUPERVISOR DE INVERSIONES	JEFATURA DE CONTRATOS DE LA RED VIAL
110	DE LA CRUZ MUNIVE ROCIO EVELYN	ESPECIALISTA LEGAL EN MATERIA PENAL	PROCURADURÍA PÚBLICA
111	DELGADO FUENTES EDWIN	SUPERVISOR DE INVERSIONES DE LA RED VIAL I	JEFATURA DE CONTRATOS DE LA RED VIAL
112	DELGADO FUENTES YURI	SUPERVISOR IN SITU - RED VIAL 5	JEFATURA DE CONTRATOS DE LA RED VIAL
113	DOMINGUEZ ROSAS LUIGGI ROGER	PRACTICANTE	JEFATURA DE CONTRATOS PORTUARIOS
114	DUEÑAS RODRIGUEZ JUAN SEBASTIAN	ASISTENTE TÉCNICO EN INGENIERÍA	JEFATURA DE CONTRATOS DE LA RED VIAL
115	ENCISO ALVAREZ VANINA KATIUSKA	ESPECIALISTA EN GESTIÓN DOCUMENTARIA Y ACCESO A LA INFORMACIÓN PÚBLICA	OFICINA DE GESTIÓN DOCUMENTARIA
116	ENRIQUEZ HIDALGO KARLO CHRISTOPHER	ESPECIALISTA EN GESTIÓN DE LA CAPACITACIÓN	JEFATURA DE GESTIÓN DE RECURSOS HUMANOS
117	ESCALANTE MELCHIORS MARIA CRISTINA	ASESOR LEGAL	PRESIDENCIA EJECUTIVA
118	ESCARCINI ENCINAS MARIA ALESSANDRA	ANALISTA EN MANTENIMIENTO E INFRAESTRUCTURA	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
119	ESCOBAR BEDOYA CHRISTIAN MILOVAN	AUXILIAR DE ARCHIVO	GERENCIA DE SUPERVISIÓN Y FISCALIZACIÓN
120	ESPINOZA MONTESINOS FRANCISCO EDWARD	ASISTENTE EN INGENIERÍA	JEFATURA DE CONTRATOS PORTUARIOS
121	EXEBIO NARANJO MARIA SOLEDAD	SECRETARIA	JEFATURA DE CONTRATOS DE LA RED VIAL
122	EYZAGUIRRE EYZAGUIRRE MILAGROS GRACIELA	SECRETARIA	GERENCIA DE REGULACIÓN Y ESTUDIOS ECONÓMICOS
123	FAJARDO GUTIERREZ VALERIA ROSALIA JULIA	ANALISTA EN INGENIERÍA	ÓRGANO DE CONTROL INSTITUCIONAL
124	FALCON ARRIETA MARIA KARLA ALEJANDRA	ESPECIALISTA EN SEGUIMIENTO Y MONITOREO DE USUARIOS	GERENCIA DE ATENCIÓN AL USUARIO
125	FALCON QUISPE KATHERINE LIZET	SECRETARIA	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
126	FARFAN ALFARO LIZ NOEMI	ASISTENTE DE SOPORTE TÉCNICO A USUARIOS	JEFATURA DE TECNOLOGÍAS DE LA INFORMACIÓN
127	FARFAN RIOS DAVIS HERITRON	ANALISTA DE ATENCIÓN AL USUARIO DE LA OFICINA DESCONCENTRADA DE CUSCO	OFICINA DESCONCENTRADA DE CUSCO
128	FERNANDEZ CASTRO VLADIMIR	ASESOR EN GESTIÓN ADMINISTRATIVA	GERENCIA GENERAL
129	FIERRO LAUREANO ANDRES ALFONSO	APOYO EN SOPORTE TÉCNICO	JEFATURA DE TECNOLOGÍAS DE LA INFORMACIÓN
130	FIGUEROA GAYOSO RODRIGO JOAQUIN	PRACTICANTE	JEFATURA DE CONTRATOS DE LA RED VIAL
131	FLORES ASTORAYME WILMER ALEXANDER	SUPERVISOR IN SITU DEL AEROPUERTO INTERNACIONAL JORGE CHAVEZ	JEFATURA DE CONTRATOS AEROPORTUARIOS
132	FRANCIA VÁSQUEZ KELLY JANNET	ASISTENTE EN CONTABILIDAD	JEFATURA DE CONTABILIDAD
133	FRANCO PEBE PEDRO RENE	SUPERVISOR IN SITU DE LA CONCESIÓN AUTOPISTA DEL SOL TRAMO TRUJILLO - SULLANA	JEFATURA DE CONTRATOS DE LA RED VIAL
134	FUENTES ANDRADE YESSENIA PAOLA	ABOGADO - ESPECIALISTA EN LA DEFENSA DEL ÁREA CONSTITUCIONAL Y PENAL	PROCURADURÍA PÚBLICA
135	FUSTAMANTE GUTIERREZ MARIA DE LOS ANGELES	ASISTENTE LEGAL	JEFATURA DE ASUNTOS JURÍDICO CONTRACTUALES
136	GADEA TRUJILLO MAYTE ROCIO	SECRETARIA	GERENCIA DE ATENCIÓN AL USUARIO
137	GARCIA ADRIANZEN ARLETTE MILAGROS	SECRETARIA	JEFATURA DE TECNOLOGÍAS DE LA INFORMACIÓN
138	GARCIA BELTRAN SILVANA MARIELLA	ESPECIALISTA EN PLANEAMIENTO Y ESTADÍSTICA	GERENCIA DE SUPERVISIÓN Y FISCALIZACIÓN
139	GARCIA CAYCHO ABEL HERNAN	SUPERVISOR DE INVERSIONES DE LA RED VIAL I	JEFATURA DE CONTRATOS DE LA RED VIAL
140	GARCIA GOMEZ JORGE EDUARDO	ASISTENTE EN PAGOS	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
141	GARCIA LOLI RAUL MARCO	INGENIERO SUPERVISOR	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
142	GAVILAN CHIHUALA GUILLERMO JHON	PRACTICANTE	SECRETARÍA TECNICA DE LOS TRIBUNALES DEL OSITRAN
143	GOMEZ BACILIO EVERTH JESUS	ESPECIALISTA DE REDES Y TELECOMUNICACIONES II	JEFATURA DE TECNOLOGÍAS DE LA INFORMACIÓN
144	GOMEZ GALARZA DE CAMPOS ERICKA BRIGITTE	RECEPCIONISTA	OFICINA DE GESTIÓN DOCUMENTARIA

145	GONZALEZ BEDOYA MIGUEL JULIO	JEFE DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA (E)	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
146	GOYCOCHEA FLORES CECILIA DEL ROSARIO	ASISTENTE ADMINISTRATIVO	JEFATURA DE CONTRATOS PORTUARIOS
147	GRANDEZ VERGARA NICOLAS ALEJANDRO	PRACTICANTE	OFICINA DE GESTIÓN DOCUMENTARIA
148	GRONERT ALVA WILDORO	JEFE DE CONTABILIDAD	JEFATURA DE CONTABILIDAD
149	GUERRA RABANAL YAKELYN ANGÉLICA	ASISTENTE EN GESTIÓN	GERENCIA DE SUPERVISIÓN Y FISCALIZACIÓN
150	GUEVARA GUARDIA JOSE JORGE ERNESTO	ESPECIALISTA EN ORGANIZACIÓN DEL TRABAJO Y GESTIÓN DEL RENDIMIENTO	JEFATURA DE GESTIÓN DE RECURSOS HUMANOS
151	GUEVARA MARTINEZ FRANCISCO RAFAEL	COORDINADOR IN SITU	JEFATURA DE CONTRATOS AEROPORTUARIOS
152	GUILLEN BARBARAN KELLY	INGENIERO CIVIL	JEFATURA DE CONTRATOS PORTUARIOS
153	GUILLEN DELGADO HAYBI MICAELA	PRACTICANTE	GERENCIA DE REGULACIÓN Y ESTUDIOS ECONÓMICOS
154	GUTIERREZ CARPIO LUIS ROOSEMBERG	SUPERVISOR AMBIENTAL	JEFATURA DE CONTRATOS DE LA RED VIAL
155	GUTIERREZ DAMAZO JOSE ANTONIO	COORDINADOR DE ASUNTOS FINANCIEROS	JEFATURA DE REGULACIÓN
156	GUTIERREZ HANCCO HUGO	SUPEVISOR IN SITU II TRAMO VIAL DV.QUILCA - AREQUIPA, DV. MATARANI-DV. MOQUEGUA, DV. ILO-TACNA Y TACNA-LA CONCORDIA	JEFATURA DE CONTRATOS DE LA RED VIAL
157	GUTIERREZ INCA JHON MIGUEL	Jefe de Logística y Control Patrimonial (e)	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
158	HARO CORALES JORGE LUIS	ESPECIALISTA DE INVERSIONES	GERENCIA DE PLANEAMIENTO Y PRESUPUESTO
159	HERNANDEZ CAÑARI FRANCESCA AURORA	ASISTENTE ADMINISTRATIVO	GERENCIA DE ADMINISTRACIÓN
160	HERNANDEZ CHANDUVI JORGE LUIS	ESPECIALISTA LEGAL PARA CONTRATOS DE CONCESIÓN DE CARRETERAS	JEFATURA DE CONTRATOS DE LA RED VIAL
161	HIDALGO BRICEÑO SILVIA	ESPECIALISTA LEGAL	JEFATURA DE CONTRATOS DE LA RED VIAL
162	HINOJOSA VIGIL OSCAR BERARDO	ESPECIALISTA EN COMUNICACIÓN INTERNA III	OFICINA DE COMUNICACIÓN CORPORATIVA
163	HOLGUIN VALDIVIESO ANA LUCIA FABIOLA	ESPECIALISTA EN RELACIONES INSTITUCIONALES	JEFATURA DE GESTIÓN DE RECURSOS HUMANOS
164	HOLGUINO AROSQUIPA NAYELY ESTEFANY	PRACTICANTE	GERENCIA DE SUPERVISIÓN Y FISCALIZACIÓN
165	HOSPINAL P ESCAJADILLO SANDRO	SUPERVISOR DE OPERACIONES FERROVIARIAS I	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
166	HUAMAN PORRAS CESAR EDGARDO	CHOFER	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
167	HUAMAN VELASQUE MARISOL	PRACTICANTE	GERENCIA DE REGULACIÓN Y ESTUDIOS ECONÓMICOS
168	HUAMANI JIMENEZ MONICA LUISA	ASISTENTE DE CENTRO DE ORIENTACIÓN DEL OSITRÁN EN LA LÍNEA 1 DEL METRO DE LIMA Y CALLAO	GERENCIA DE ATENCIÓN AL USUARIO
169	HUANCAUQUI RODRIGUEZ DE SAEZ EDITH HELGA	ASESOR EN GESTIÓN DIRECTIVA	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
170	HUANQUI VALCARCEL PATRICIA FATIMA	ABOGADO SENIOR	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
171	HUAPAYA POMA LEISLY CAROL	ASISTENTE EN GESTIÓN DOCUMENTARIA	OFICINA DE GESTIÓN DOCUMENTARIA
172	HUARACA MOSCOSO KATHIA MIRTHA	ASISTENTE LEGAL	SECRETARÍA TECNICA DE LOS TRIBUNALES DEL OSITRAN
173	HUERTA OLIVAS KELLY VANESSA	ESPECIALISTA EN SEGUIMIENTO Y MONITOREO EN TEMAS ADMINISTRATIVOS	GERENCIA DE ADMINISTRACIÓN
174	ILLAHUAMAN CHIPANA CRISTIAN ELIAS	ESPECIALISTA EN CONTRATACIONES	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
175	JACOME BAUTISTA IVAN EDUARDO	PRACTICANTE	JEFATURA DE GESTIÓN DE RECURSOS HUMANOS
176	JARA MALPARTIDA MARCIAL YVAN	SUPERVISOR IN SITU PARA LA SUPERVISIÓN DE AEROPUERTOS DEL PERÚ - ADP EN LOS AEROPUERTOS DE CAJAMARCA, TRUJILLO, ANTA - HUARAZ Y PISCO	JEFATURA DE CONTRATOS AEROPORTUARIOS
177	JARAMILLO TARAZONA FRANCISCO	GERENTE DE SUPERVISIÓN Y FISCALIZACIÓN (E)	GERENCIA DE SUPERVISIÓN Y FISCALIZACIÓN
178	JIMENEZ CERRON TITO FERNANDO	JEFE DE ASUNTOS JURÍDICO CONTRACTUALES	JEFATURA DE ASUNTOS JURÍDICO CONTRACTUALES
179	JIMENEZ MATUTE JULIO CESAR	SUPERVISOR DE OPERACIONES DE LA RED VIAL II	JEFATURA DE CONTRATOS DE LA RED VIAL
180	JORDAN LIZA ZULEMA	ANALISTA EN SELECCIÓN Y GESTIÓN DE PERSONAS	JEFATURA DE GESTIÓN DE RECURSOS HUMANOS

181	JOSEPH BARTRA GUSTAVO SALOMON	COORDINADOR IN SITU DE LA CONCESIÓN DE LOS TRAMOS VIALES DEL EJE MULTIMODAL AMAZONAS NORTE Y DE LA CONCESIÓN EMPALME 01B BUENOS AIRES CANCHAQUE	JEFATURA DE CONTRATOS DE LA RED VIAL
182	KATSUREN TOBARU JUAN CARLOS	COORDINADOR DE MANTENIMIENTO	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
183	LAZARO DULANTO RITA ANA	ANALISTA EN GESTIÓN DE CONTENIDOS ECONÓMICOS PARA LA DIFUSIÓN EN MEDIOS DE COMUNICACIÓN	OFICINA DE COMUNICACIÓN CORPORATIVA
184	LEA POMA CRISTIAN HUMBERTO	SUPERVISOR DE INVERSIONES DE LA RED VIAL I	JEFATURA DE CONTRATOS DE LA RED VIAL
185	LEON ROSALES KIMBERLY LUCERO	ANALISTA LEGAL	GERENCIA DE REGULACIÓN Y ESTUDIOS ECONÓMICOS
186	LEQQUE QUISPE WILDER	PRACTICANTE	JEFATURA DE CONTRATOS PORTUARIOS
187	LESCANO ECHAJAYA JOSE LUIS	ABOGADO	JEFATURA DE GESTIÓN DE RECURSOS HUMANOS
188	LI NING CHAMAN JORGE FRANCISCO	SUPERVISOR ECONÓMICO FINANCIERO PORTUARIO I	JEFATURA DE CONTRATOS PORTUARIOS
189	LINARES BARRANTES MARTHA CAROLINA	ANALISTA DE GESTIÓN I	PRESIDENCIA EJECUTIVA
190	LIVIAC ESPINOZA DANTE ROSALES	SUPERVISOR(A) DE MATERIAL RODANTE Y DE EQUIPAMIENTO ELECTROMECÁNICO	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
191	LOAYZA ALVAREZ MANUEL	CHOFER	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
192	LOLAY HUAMANYAURI INGRID VANESSA	ESPECIALISTA LEGAL	GERENCIA DE ATENCIÓN AL USUARIO
193	LOPEZ BELTRAN JULIO CESAR	INGENIERO MECÁNICO ELÉCTRICO PARA LA SUPERVISIÓN DEL EQUIPAMIENTO ELECTROMECÁNICO DEL METRO DE LIMA, LÍNEA 1	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
194	LOPEZ CARDENAS FRANCIS JACKELYN	SUPERVISOR DE INVERSIONES AEROPORTUARIAS I	JEFATURA DE CONTRATOS AEROPORTUARIOS
195	LOPEZ CATASUS CESAR SAMUEL	COORDINADOR DE SEGURIDAD Y DEFENSA NACIONAL	GERENCIA GENERAL
196	LOPEZ DONGO SANDRA JULISSA	ESPECIALISTA DE GESTIÓN DE LA INFORMACIÓN II	JEFATURA DE CONTRATOS PORTUARIOS
197	LOPEZ FLORES CARLA PAOLA	ESPECIALISTA EN GESTIÓN DE RIESGOS	GERENCIA DE PLANEAMIENTO Y PRESUPUESTO
198	LOPEZ GAYOSO HELENA DEL ROCIO	ASISTENTE ADMINISTRATIVO	JEFATURA DE CONTRATOS DE LA RED VIAL
199	LOPEZ VASQUEZ CINTHYA	ESPECIALISTA EN ESTUDIOS ECONÓMICOS	GERENCIA DE REGULACIÓN Y ESTUDIOS ECONÓMICOS
200	LUNA FLORES KENNETH AURELIO	SUPERVISOR IN SITU II TRAMO 5B: ILO-MOQUEGUA-PUNO-JULIACA	JEFATURA DE CONTRATOS DE LA RED VIAL
201	LUQUE RAMIREZ HANSEL BRUCEAMIEL	PRACTICANTE	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
202	MAGUIÑA CORTEZ JUAN JOSÉ	SUPERVISOR DE INVERSIONES AEROPORTUARIAS II	JEFATURA DE CONTRATOS AEROPORTUARIOS
203	MAGUIÑA MESTA MARIBEL NERAIDA	ESPECIALISTA LEGAL	JEFATURA DE CONTRATOS DE LA RED VIAL
204	MALLMA BERTINETTI JORGE LUIS	ASISTENTE PARA LA MESA DE PARTES VIRTUAL	OFICINA DE GESTIÓN DOCUMENTARIA
205	MALLQUI RODRIGUEZ OSCAR ENRIQUE	SUPERVISOR DE TELECOMUNICACIONES Y SEÑALIZACIÓN	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
206	MALPARTIDA DEL CARPIO CARMEN BEATRIZ	ASISTENTE EN GESTIÓN ADMINISTRATIVA	GERENCIA GENERAL
207	MAMANI OSORIO ERNESTO ALBERTO	SUPERVISOR ECONÓMICO FINANCIERO AEROPORTUARIO I	JEFATURA DE CONTRATOS AEROPORTUARIOS
208	MANCO OSORIO RICARDO ALEJANDRO	ESPECIALISTA CONTRACTUAL	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
209	MANCO TICONA MARCO ANTONIO	PRACTICANTE	GERENCIA DE REGULACIÓN Y ESTUDIOS ECONÓMICOS
210	MANDUJANO DAMIAN CAROLINE YVES	ESPECIALISTA LEGAL EN MATERIA SANCIONADORA	JEFATURA DE FISCALIZACIÓN
211	MANRIQUE MANRIQUE ELMER ANASTASIO	SUPERVISOR DE OPERACIONES	JEFATURA DE CONTRATOS DE LA RED VIAL
212	MARCELO POVIS GEAN PIERTH	PRACTICANTE	JEFATURA DE CONTRATOS AEROPORTUARIOS
213	MARCELO TORRE EDUARDO IVAN	PROFESIONAL EN TESORERÍA	JEFATURA DE TESORERÍA
214	MARINA AREVALO ALDO ROMAN	COORDINADOR IN SITU DE LA CONCESIÓN DE LOS TRAMOS VIALES DEL EJE MULTIMODAL AMAZONAS NORTE Y DE LA CONCESIÓN EMPALME 01B BUENOS AIRES CANCHAQUE	JEFATURA DE CONTRATOS DE LA RED VIAL
215	MARTINEZ QUINTO KATHERINA	ASISTENTE PARA LA ATENCIÓN DE CENTRAL TELEFÓNICA Y APOYO EN MESA DE PARTES	OFICINA DE GESTIÓN DOCUMENTARIA
216	MATAMOROS PAITAN CRISTIAN	ASISTENTE EN INGENIERÍA	JEFATURA DE CONTRATOS PORTUARIOS

217	MATOS SANCHEZ AMIRA ELENI	ASISTENTE DE SUPERVISIÓN	JEFATURA DE CONTRATOS DE LA RED VIAL
218	MATTA REYES GINA ISABEL	ABOGADO SENIOR EN MATERIA ADMINISTRATIVA	JEFATURA DE ASUNTOS JURÍDICO REGULATORIOS Y ADMINISTRATIVOS
219	MATUTE GONZALES ERIKA VANESSA	ABOGADO	GERENCIA DE ADMINISTRACIÓN
220	MEDINA RODRIGUEZ GERMAN FIDEL	SUPERVISOR IN SITU	JEFATURA DE CONTRATOS DE LA RED VIAL
221	MEDINA RUBIANES EDGARDO RAJMAN	ABOGADO SENIOR	JEFATURA DE ASUNTOS JURÍDICO CONTRACTUALES
222	MEGO SILVA JULIO CÉSAR	ANALISTA LEGAL	SECRETARÍA TECNICA DE LOS TRIBUNALES DEL OSITRAN
223	MEJIA CORNEJO JUAN CARLOS	GERENTE/A GENERAL	GERENCIA GENERAL
224	MELGAR PAJARES ZOILA JULIA DEL ROSARIO	AUXILIAR DE ARCHIVO	OFICINA DE GESTIÓN DOCUMENTARIA
225	MELGAREJO SANCHEZ AVITA MONICA	ANALISTA DE CONTRATOS AEROPORTUARIOS I	JEFATURA DE CONTRATOS AEROPORTUARIOS
226	MENDEZ VEGA MARIA ALEJANDRA	ESPECIALISTA EN ESTUDIOS ECONÓMICOS	JEFATURA DE ESTUDIOS ECONÓMICOS
227	MENDEZ ZEVALLOS JUAN JESUS	SUPERVISOR DE OPERACIONES FERROVIARIAS	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
228	MENDOZA GUZMAN ROCIO	ESPECIALISTA LEGAL EN MATERIA SANCIONADORA	JEFATURA DE CONTRATOS PORTUARIOS
229	MENDOZA MONTENEGRO JAIME GUSTAVO	ASISTENTE EN ARCHIVO	OFICINA DE GESTIÓN DOCUMENTARIA
230	MENENDEZ GAITAN SUSANA BEATRIZ	ANALISTA DE COMUNICACIÓN EXTERNA	OFICINA DE COMUNICACIÓN CORPORATIVA
231	MERCADO FLORES CRISTHIAN PAOLO	Procurador Público	PROCURADURÍA PÚBLICA
232	MERCADO QUIROZ JORGE ALBERTO ALESSANDRO	ANALISTA DE PAGOS	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
233	MERCADO TOLEDO RICARDO JAVIER	JEFE/A DE LA GERENCIA DE PLANEAMIENTO Y PRESUPUESTO	GERENCIA DE PLANEAMIENTO Y PRESUPUESTO
234	MESTANZA DONGO LUIS ANDRES	ANALISTA DE PROYECTOS DE SISTEMAS	JEFATURA DE TECNOLOGÍAS DE LA INFORMACIÓN
235	MIKI NINOMIYA JUAN JOSÉ	SUPERVISOR DE INVERSIONES AEROPORTUARIAS I	JEFATURA DE CONTRATOS AEROPORTUARIOS
236	MIO CORTEZ EDISON SEGUNDO	ASISTENTE DE ESTUDIOS ECONÓMICOS	GERENCIA DE REGULACIÓN Y ESTUDIOS ECONÓMICOS
237	MOLINA LUJAN JUAN CARLOS	COORDINADOR IN SITU DE LA CONCESIÓN DEL TRAMO 2 DE IIRSA CENTRO: PUENTE RICARDO PALMA - LA OROYA - HUANCAYO Y LA OROYA -DV CERRO DE PASCO	JEFATURA DE CONTRATOS DE LA RED VIAL
238	MONTENEGRO GARCIA KARLIN VALENTY	SUPERVISOR IN SITU - RED VIAL 6: PUCUSANA - CERRO AZUL -ICA	JEFATURA DE CONTRATOS DE LA RED VIAL
239	MONTOYA GUILLEN MAXIMO CASIMIRO	INGENIERO MECÁNICO ELÉCTRICO PARA LA SUPERVISIÓN DEL MATERIAL RODANTE DEL METRO DE LIMA - LÍNEA 1	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
240	MORALES DIOS INGRID YANET	APOYO ADMINISTRATIVO GENERAL	GERENCIA GENERAL
241	MORÁN CARDENAS FLAVIO	ASISTENTE EN SERVICIOS GENERALES	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
242	MORENO DELGADO HERNAN GONZALO	SUPERVISOR DE INVERSIONES FERROVIARIAS I	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
243	MORILLO BLAS MANUEL MARTÍN	ANALISTA DE ESTUDIOS ECONÓMICOS III	JEFATURA DE ESTUDIOS ECONÓMICOS
244	MORZAN SCERPELLA JORGE JAVIER	ESPECIALISTA EN ADMINISTRACIÓN DE BASE DE DATOS Y APLICACIONES	JEFATURA DE TECNOLOGÍAS DE LA INFORMACIÓN
245	MOSCOSO REATEGUI HUGO DISTEL	SUPERVISOR IN SITU II PARA EL TRAMO II DE LA IIRSA CENTRO	JEFATURA DE CONTRATOS DE LA RED VIAL
246	MOSCOSO VALENZUELA JULIO GIRALDO	SUPERVISOR IN SITU II PARA EL TRAMO 5 DE LA IIRSA SUR: MATARANI - JULIACA, ILO - PUNO - JULIACA - AZÁNGARO	JEFATURA DE CONTRATOS DE LA RED VIAL
247	MUNDACA MAYORGA JOSE MANUEL	SUPERVISOR DE OPERACIONES DE LA RED VIAL I	JEFATURA DE CONTRATOS DE LA RED VIAL
248	MUÑOZ MEDRANO ANGEL HIROSHI	PRACTICANTE	GERENCIA DE SUPERVISIÓN Y FISCALIZACIÓN
249	MUÑOZ RUIZ GLORIA VIVIANA	ABOGADO SENIOR EN MATERIA REGULATORIA	JEFATURA DE ASUNTOS JURÍDICO REGULATORIOS Y ADMINISTRATIVOS
250	NANFARO POMASONGO NORMA SOLANGE	ANALISTA EN CONTRATACIONES	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
251	NASSR SANDOVAL SALIM	ANALISTA EN FORMULACIÓN, SEGUIMIENTO Y EVALUACIÓN DE LOS PLANES INSTITUCIONALES	GERENCIA DE PLANEAMIENTO Y PRESUPUESTO
252	NEYRA GONZALES CESAR JEAN PAUL	GESTOR DOCUMENTARIO	GERENCIA DE SUPERVISIÓN Y FISCALIZACIÓN

253	NORIEGA QUIROZ EYLEEN CAROLINA	ESPECIALISTA SENIOR EN TRANSFORMACIÓN DIGITAL	JEFATURA DE TECNOLOGÍAS DE LA INFORMACIÓN
254	OCHOA CARBAJO YESSICA GUADALUPE	ANALISTA DE REGULACIÓN EN MATERIA DE CARRETERAS Y VÍAS FÉRREAS I	JEFATURA DE REGULACIÓN
255	OCHOA OCHOA OSCAR ISAAC	ESPECIALISTA LEGAL PARA CONTRATOS DE CONCESIÓN AEROPORTUARIOS	JEFATURA DE CONTRATOS AEROPORTUARIOS
256	ORDOÑEZ BENDEZU GERALDINE ISBETH	ASISTENTE DE REGULACIÓN	JEFATURA DE REGULACIÓN
257	ORTEGA MATUTE ELIZABETH MONICA	SUPERVISOR DE TECNOLOGÍAS PORTUARIAS I	JEFATURA DE CONTRATOS PORTUARIOS
258	ORTIZ CABREJOS CLAUDIA IVONNE	ESPECIALISTA LEGAL	JEFATURA DE ASUNTOS JURÍDICO CONTRACTUALES
259	ORTIZ NIETO MARY CARMEN	ANALISTA DE CENTRO DE ORIENTACIÓN DEL OSITRAN EN EL TERMINAL NORTE MULTIPROPÓSITO DEL CALLAO	GERENCIA DE ATENCIÓN AL USUARIO
260	ORTIZ RODRIGUEZ KARINA MAGALY	ASISTENTE DE SERVICIOS ARCHIVÍSTICOS	OFICINA DE GESTIÓN DOCUMENTARIA
261	ORTIZ VARIAS CRISTIAN RICARDO	SUPERVISOR ECONÓMICO FINANCIERO DE LA RED VIAL II	JEFATURA DE CONTRATOS AEROPORTUARIOS
262	ORUE MARTINEZ ADELA ROSARIO	ESPECIALISTA EN ALMACÉN III	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
263	OYOLA DEL AGUILA ANTONIO	SUPERVISOR IN SITU PARA LA SUPERVISIÓN DE AEROPUERTOS DEL PERÚ ADP EN LOS AEROPUERTOS DE IQUITOS, PUCALLPA, CHACHAPOYAS Y TARAPOTO	JEFATURA DE CONTRATOS AEROPORTUARIOS
264	PACHECO INGARUCA NOELIA DALILA	ABOGADO SENIOR DE LA GSF	GERENCIA DE SUPERVISIÓN Y FISCALIZACIÓN
265	PADILLA AGAMA WALTER KEVIN	ANALISTA EN CONTRATACIONES	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
266	PALACIOS CANALES CARLA MARCIA	PRACTICANTE	JEFATURA DE CONTRATOS AEROPORTUARIOS
267	PANEZ MATEO EDGAR GEORGE	PRACTICANTE	JEFATURA DE CONTRATOS AEROPORTUARIOS
268	PAREDES RAMIREZ LUIS ELEAZAR	SUPERVISOR DE INVERSIONES AEROPORTUARIAS II	JEFATURA DE CONTRATOS AEROPORTUARIOS
269	PARIASCA MANSILLA JOSE	ASISTENTE DE TRANSPORTE	JEFATURA DE GESTIÓN DE RECURSOS HUMANOS
270	PARIONA VEGA EDITH PILAR	ASISTENTE DE ALMACÉN DE EXISTENCIAS	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
271	PAZ PANIZO JORGE LUIS	ESPECIALISTA I	JEFATURA DE REGULACIÓN
272	PEREA MOSCOSO JORGE LUIS	ESPECIALISTA EN GESTIÓN DE DATOS	JEFATURA DE TECNOLOGÍAS DE LA INFORMACIÓN
273	PEREYRA MONTOYA LIDIA YANET	ESPECIALISTA EN CONTRATACIONES II	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
274	PEREZ ALATA WILBER JAVIER	JEFE DE FISCALIZACIÓN	JEFATURA DE FISCALIZACIÓN
275	PEREZ CUBAS TEODORO	COORDINADOR IN SITU DE LA CONCESIÓN DE LOS TRAMOS VIALES DEL EJE MULTIMODAL AMAZONAS NORTE Y DE LA CONCESIÓN EMPALME 01B BUENOS AIRES CANCHAQUE	JEFATURA DE CONTRATOS DE LA RED VIAL
276	PEREZ GOMEZ CESAR LUIS	SUPERVISOR ECONÓMICO FINANCIERO DE LA RED VIAL II	JEFATURA DE CONTRATOS DE LA RED VIAL
277	PEREZ LIRCOS LUIS	ECONOMISTA	JEFATURA DE CONTRATOS DE LA RED VIAL
278	PEREZ VELASQUEZ OSCAR WILLIAM	ESPECIALISTA EN LA DEFENSA DE PROCESOS CIVILES, PENALES Y LABORALES	PROCURADURÍA PÚBLICA
279	PINCHI CACERES GABRIELA NATALI	ASISTENTE LEGAL	GERENCIA DE REGULACIÓN Y ESTUDIOS ECONÓMICOS
280	PIZARRO BACA ANTONIO	INGENIERO CIVIL	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
281	POLANCO NORIEGA EMMANUEL ANTONIO	ANALISTA LEGAL	JEFATURA DE ASUNTOS JURÍDICO CONTRACTUALES
282	POLO VIVAR CHRISTIAN JOEL	SUPERVISOR IN SITU - NUEVO TERMINAL PORTUARIO DE YURIMAGUAS - NUEVA REFORMA	JEFATURA DE CONTRATOS PORTUARIOS
283	PORRAS CHANCA JIMMY	ASISTENTE TÉCNICO DE ESTACIONES Y TRENES	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
284	PORTUGAL VARGAS ANGEL EULOGIO	ABOGADO SENIOR	JEFATURA DE GESTIÓN DE RECURSOS HUMANOS
285	POZO CRUZ BETTY SAMANDA	APOYO ADMINISTRATIVO	GERENCIA DE ASESORÍA JURÍDICA
286	PRADO PANDO STEPHANIE	PRACTICANTE	SECRETARÍA TECNICA DE LOS TRIBUNALES DEL OSITRAN
287	PRECIADO JERONIMO EDGAR JAVIER	ANALISTA ADMINISTRATIVO	GERENCIA DE ATENCIÓN AL USUARIO
288	PRIETO BARRERA ALDO MARTIN	ESPECIALISTA	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO

289	PUCHOC RIOS LIZZETH	ASISTENTE DE ARCHIVO	OFICINA DE GESTIÓN DOCUMENTARIA
290	QUEIJA DE LA SOTTA SANDRA FIORELLA	Jefe de Estudios Económicos	JEFATURA DE ESTUDIOS ECONÓMICOS
291	QUESADA ORÉ LUIS RICARDO	GERENTE DE REGULACIÓN Y ESTUDIOS ECONÓMICOS	GERENCIA DE REGULACIÓN Y ESTUDIOS ECONÓMICOS
292	QUEVEDO BURNEO CARLOS ALBERTO	Asistente de Transporte	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
293	QUIÑONEZ QUISPE ELISVAN	ASISTENTE DE TRANSFERENCIA DE DOCUMENTOS	OFICINA DE GESTIÓN DOCUMENTARIA
294	QUIROZ GARAY HASSLEN	OPERADOR DE LA LÍNEA DE DIGITALIZACIÓN	OFICINA DE GESTIÓN DOCUMENTARIA
295	QUISPE DE LA CRUZ ELIAS TORIBIO	PROFESIONAL PARA QUE SE ENCARGUE DE LAS LABORES DE SUPERVISIÓN DEL PROYECTO Y DE LAS INVERSIONES EN EQUIPOS Y SISTEMAS FERROVIARIOS ELECTROMECÁNICOS	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
296	QUISPE TERRONES REYMER GRACIANO	AUXILIAR DE PRESIDENCIA	PRESIDENCIA EJECUTIVA
297	RAMIREZ CHUQUISPUMA CHRISTIAN EDSON	PRACTICANTE	OFICINA DE COMUNICACIÓN CORPORATIVA
298	RAMIREZ DIAZ ANITA LUZ	ANALISTA EN COMUNICACIÓN MULTIMEDIA	GERENCIA DE ATENCIÓN AL USUARIO
299	RAMIREZ RABINES VERONICA CARMEN	ABOGADO PARA LA SECRETARIA TÉCNICA DE LOS ÓRGANOS INSTRUCTORES DE LOS PROCEDIMIENTOS ADMINISTRATIVOS DISCIPLINARIOS	JEFATURA DE GESTIÓN DE RECURSOS HUMANOS
300	RAMIREZ VIZCARRA JOSE MANUEL	SUPERVISOR IN SITU II PARA EL TRAMO I DE LA IIRSA SUR	JEFATURA DE CONTRATOS DE LA RED VIAL
301	RAMOS VALDERRAMA JHONATAN	PRACTICANTE	JEFATURA DE CONTRATOS DE LA RED VIAL
302	REATEGUI RIOS JOSE ENRIQUE	JEFE DE OFICINA DESCONCENTRADA DE LORETO	OFICINA DESCONCENTRADA DE IQUITOS
303	REATEGUI SANCHEZ JESSICA	APOYO ADMINISTRATIVO	GERENCIA DE ASESORÍA JURÍDICA
304	REGALADO RAFAEL DORIS DELICIA	ASESOR TÉCNICO	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
305	REYES CABRERA VERONICA ROXANA	Auditor II	ÓRGANO DE CONTROL INSTITUCIONAL
306	REYES QUEZADA ISABEL JASMINE	AUXILIAR DE CONTROL DE CALIDAD EN MESA DE PARTES	OFICINA DE GESTIÓN DOCUMENTARIA
307	REYNAGA ALVARADO PATRICIA	GERENTE ADJUNTO DE LA GERENCIA GENERAL	GERENCIA GENERAL
308	RICALDI RODRIGUEZ MAGALY GLORIA	ESPECIALISTA LEGAL EN MATERIA SANCIONADORA	JEFATURA DE FISCALIZACIÓN
309	RIOS ARELLANO KARIN KATIA	ESPECIALISTA AMBIENTAL DE LA RED VIAL	JEFATURA DE CONTRATOS DE LA RED VIAL
310	RIOS DE LA CRUZ ISAAC	SUPERVISOR DE OPERACIONES DE LA RED VIAL I	JEFATURA DE CONTRATOS DE LA RED VIAL
311	RIOS RAMIREZ FERNANDO	ANALISTA LEGAL	GERENCIA DE ATENCIÓN AL USUARIO
312	ROBLADILLO QUISPILAY ENRIQUE ALBERTO	AUDITOR II	ÓRGANO DE CONTROL INSTITUCIONAL
313	RODRIGUEZ CHOCCARE ARTHUR	ESPECIALISTA EN ARCHIVO Y TRANSFORMACIÓN DIGITAL	OFICINA DE GESTIÓN DOCUMENTARIA
314	RODRIGUEZ HERNANDEZ ANA ISABEL	ESPECIALISTA EN GESTIÓN DE PERSONAS	JEFATURA DE GESTIÓN DE RECURSOS HUMANOS
315	RODRIGUEZ HERRERA OSWALDO JEHOSHUA	ASESOR LEGAL	JEFATURA DE ASUNTOS JURÍDICO REGULATORIOS Y ADMINISTRATIVOS
316	RODRIGUEZ MARTINEZ ANTONIO MICHAEL	SECRETARIO TÉCNICO DE LOS TRIBUNALES DEL OSITRAN	SECRETARÍA TECNICA DE LOS TRIBUNALES DEL OSITRAN
317	RODRIGUEZ ROMAN CINDY DIANE	ANALISTA ADMINISTRATIVO	JEFATURA DE TECNOLOGÍAS DE LA INFORMACIÓN
318	ROJAS REGALADO DANNA VALERY	ESPECIALISTA LEGAL	GERENCIA DE ATENCIÓN AL USUARIO
319	ROJAS ZEBALLOS JOSE CARLOS	ABOGADO SENIOR	SECRETARÍA TECNICA DE LOS TRIBUNALES DEL OSITRAN
320	ROSALES ALVARADO SUSANA DE LOS MILAGROS	SUPERVISOR AMBIENTAL I	GERENCIA DE SUPERVISIÓN Y FISCALIZACIÓN
321	ROSALES MAYO CHRISTIAN JUAN	Jefe de Asuntos Jurídicos Regulatorios y Administrativos (e)	JEFATURA DE ASUNTOS JURÍDICO REGULATORIOS Y ADMINISTRATIVOS
322	RUBIO BEDREGAL REYNA DE LOS ANGELES	Jefe de Tesorería (e)	JEFATURA DE TESORERÍA
323	RUPAY CERVANTES JENNY IRMA	ANALISTA EN GESTIÓN DEL EMPLEO Y COMPENSACIONES	JEFATURA DE GESTIÓN DE RECURSOS HUMANOS
324	SAAVEDRA CASTILLO LUIS EMILIO	Especialista en Presupuesto	GERENCIA DE PLANEAMIENTO Y PRESUPUESTO
325	SALAS PAICO HENRRI ANTONIO	SUPERVISOR DE INVERSIONES DE LA RED VIAL I	JEFATURA DE CONTRATOS DE LA RED VIAL
326	SALAZAR LEON MANUEL ALEJANDRO	ANALISTA DE PAGOS	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL

327	SALCEDO MOLINA ROXANA YVONE	SECRETARIA	GERENCIA DE PLANEAMIENTO Y PRESUPUESTO
328	SAMPLINI BECERRA MONICA PAOLA	ASISTENTE EN CONTRATACIONES	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
329	SANCHEZ AREVALO EVELING CARMELA	ANALISTA EN GESTIÓN DE TRÁMITES DIGITALES	OFICINA DE GESTIÓN DOCUMENTARIA
330	SANCHEZ BARRUETA ELVIS LULI	SUPERVISOR IN SITU DE INVERSIONES	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
331	SANCHEZ POZO HENRY LEONEL	ESPECIALISTA EN PROCESOS	GERENCIA DE PLANEAMIENTO Y PRESUPUESTO
332	SANDOVAL DIOSES BRENDA VANESSA	ANALISTA EN PLANEAMIENTO	GERENCIA DE PLANEAMIENTO Y PRESUPUESTO
333	SANTA CRUZ SANTA CRUZ MANUEL TEODOSIO	SECRETARIO TÉCNICO DE LOS CUERPOS COLEGIADOS	SECRETARÍA TECNICA DE LOS CUERPOS COLEGIADOS
334	SANTA MARIA CARLOS MARIANO JESUS	ASISTENTE TÉCNICO EN INGENIERÍA	JEFATURA DE CONTRATOS AEROPORTUARIOS
335	SANTILLAN ESPINOZA JESSICA VICTORIA	ASESOR LEGAL	JEFATURA DE ASUNTOS JURÍDICO REGULATORIOS Y ADMINISTRATIVOS
336	SARASI GUILLEN KATHERIN ELIZABETH	ASISTENTE EN CONTROL DE ARCHIVOS	OFICINA DE GESTIÓN DOCUMENTARIA
337	SAUCEDO DURAN MANUEL GUSTAVO ARTURO	APOYO EN SOPORTE TÉCNICO	JEFATURA DE TECNOLOGÍAS DE LA INFORMACIÓN
338	SHEPUT STUCCHI HUMBERTO LUIS	ASESOR LEGAL ESPECIALIZADO EN CONCESIONES Y APPS	GERENCIA GENERAL
339	SILVA CAMARGO WILLIAM ALBERTO	SUPERVISOR DE INVERSIONES AEROPORTUARIAS I	JEFATURA DE CONTRATOS AEROPORTUARIOS
340	SILVA GIL LENIN HENRRY	SUPERVISOR DE SEGURIDAD Y MEDIO AMBIENTE	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
341	SORIANO DE LA CRUZ JAQUELINE MAGALY	ESPECIALISTA TRIBUTARIO	GERENCIA DE SUPERVISIÓN Y FISCALIZACIÓN
342	SOTOMAYOR TEVES CESAR AUGUSTO	ASESOR LEGAL PARA LA CONCESIÓN DE LA LÍNEA 2 DE LA RED BÁSICA DEL METRO DE LIMA Y CALLAO	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
343	SOTOMAYOR VERIA ROLANDO ALFREDO	SUPERVISOR IN SITU II DE INVERSIONES PARA EL TRAMO 5 DE LA IIRSA SUR	JEFATURA DE CONTRATOS DE LA RED VIAL
344	SUAREZ SALINAS RENZO FERNANDO	SUPERVISOR DE OPERACIONES AEROPORTUARIAS I	JEFATURA DE CONTRATOS AEROPORTUARIOS
345	SUMARI CHANG CLAUDIA DEL ROCIO	ENFERMERA	JEFATURA DE GESTIÓN DE RECURSOS HUMANOS
346	TAIRO TAPIA ELVER BERNARDO	SUPERVISOR DE OPERACIONES	JEFATURA DE CONTRATOS DE LA RED VIAL
347	TALLEDO LEON CESAR ENRIQUE	JEFE DE TECNOLOGÍAS DE LA INFORMACIÓN	JEFATURA DE TECNOLOGÍAS DE LA INFORMACIÓN
348	TAMAYO PEREYRA PAUL GERSON	ABOGADO SENIOR	JEFATURA DE ASUNTOS JURÍDICO REGULATORIOS Y ADMINISTRATIVOS
349	TAPIA RAMOS CARMEN HAYDEE	SECRETARIA	PRESIDENCIA EJECUTIVA
350	TAVARA VASQUEZ ANGELA ESTHER	ESPECIALISTA LEGAL	GERENCIA DE ATENCIÓN AL USUARIO
351	TERRONES SANCHEZ CESAR FROILAN	ESPECIALISTA EN CONTABILIDAD	JEFATURA DE CONTABILIDAD
352	TINEO HUAMAN JENNY ROSAURA	ASISTENTE ADMINISTRATIVO	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
353	TINEO NAJARRO RODOLFO	SUPERVISOR IN SITU II	JEFATURA DE CONTRATOS DE LA RED VIAL
354	TITO FIGUEREDO MANUEL LORENZO	PRACTICANTE	JEFATURA DE TECNOLOGÍAS DE LA INFORMACIÓN
355	TOLEDO CALLA KENNY DANY	SUPERVISOR IN SITU DE LOS AEROPUERTOS DE AYACUCHO Y PUERTO MALDONADO	JEFATURA DE CONTRATOS AEROPORTUARIOS
356	TORRES CASTILLO LUIS MIGUEL	JEFE DE GESTIÓN DE RECURSOS HUMANOS	JEFATURA DE GESTIÓN DE RECURSOS HUMANOS
357	TORRES MARQUEZ ROLANDO ROQUE	SUPERVISOR DE INVERSIONES DE LA RED VIAL I	JEFATURA DE CONTRATOS DE LA RED VIAL
358	TORRES SAMOS WALTER FERMIN	CHOFER	PRESIDENCIA EJECUTIVA
359	TORRES SANCHEZ MARIA TESSY	ASESOR DE COORDINACIÓN TÉCNICA (E)	PRESIDENCIA EJECUTIVA
360	TORRES SOTO KHYRA DEL CHAYO	ANALISTA DE ATENCIÓN AL USUARIO DE LA OFICINA DESCONCENTRADA DE LORETO	OFICINA DESCONCENTRADA DE IQUITOS
361	TRUJILLO GONZALES ESTELA MELVA	ESPECIALISTA CONTABLE EN TRIBUTOS	GERENCIA DE SUPERVISIÓN Y FISCALIZACIÓN
362	TUPAYACHI BEISAGA GERARDO	PRACTICANTE	PROCURADURÍA PÚBLICA
363	URIARTE ESPEJO URSULA PAULINA	ESPECIALISTA EN CONTRATACIONES	JEFATURA DE LOGÍSTICA Y CONTROL PATRIMONIAL
364	VALDIVIA PAREDES GIULIANA GLADYS	ESPECIALISTA EN PLANEAMIENTO	GERENCIA DE PLANEAMIENTO Y PRESUPUESTO

365	VALDIVIA RODRIGUEZ ABEL ANTONIO	ANALISTA LEGAL	GERENCIA DE ATENCIÓN AL USUARIO
366	VALENCIA JULCA PEDRO MIGUEL	SUPERVISOR DE OPERACIONES	JEFATURA DE CONTRATOS DE LA RED VIAL
367	VALENZUELA CAVELLO ALINA AIMEE	COORDINADOR DE OFICINA DE GESTIÓN DOCUMENTARIA	OFICINA DE GESTIÓN DOCUMENTARIA
368	VALLE MANCHEGO TANIA BEATRIZ	ASESOR LEGAL PARA LA CONCESIÓN DE LA LÍNEA 2 DE LA RED BÁSICA DEL METRO DE LIMA Y CALLAO	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
369	VARGAS RODRIGUEZ FRANCIS HAROLD	SUPERVISOR DE VÍAS FÉRREAS Y OBRAS CIVILES	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
370	VARGAS ZAFRA GLADYS ELIZABETH	ASISTENTE DE PROCURADURÍA PÚBLICA	PRESIDENCIA EJECUTIVA
371	VASQUEZ PAZ LUIS ALBERTO	SUPERVISOR DE INVERSIONES FERROVIARIAS I	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
372	VASQUEZ PESANTES ELINA ELIZABETH	AUDITOR II	ÓRGANO DE CONTROL INSTITUCIONAL
373	VASQUEZ VELASQUEZ MAGDA FIORELLA	ESPECIALISTA EN ATENCIÓN AL USUARIO FINAL	SECRETARÍA TECNICA DE LOS TRIBUNALES DEL OSITRAN
374	VEGA VASQUEZ JOHN ALBERT	JEFE DE CONTRATOS DE LA RED VIAL	JEFATURA DE CONTRATOS DE LA RED VIAL
375	VELASQUEZ CORDOVA MARIA DEL ROSARIO	ESPECIALISTA EN INTEGRIDAD	JEFATURA DE GESTIÓN DE RECURSOS HUMANOS
376	VENEGAS DELGADO CLAUDIA ELIZABETH	ABOGADO SENIOR	JEFATURA DE ASUNTOS JURÍDICO CONTRACTUALES
377	VENTURI MOQUILLAZA ANGELA RITA	ABOGADO SENIOR PORTUARIO	JEFATURA DE CONTRATOS PORTUARIOS
378	VICENTE ROMERO DOMINGO	SUPERVISOR IN SITU - TRAMO 5-A- MATARANI-AREQUIPA-JULIACA-AZÁNGARO	JEFATURA DE CONTRATOS DE LA RED VIAL
379	VIDAL VILCATOMA DANIEL ANGEL	SUPERVISOR IN SITU II PARA LA LONGITUDINAL DE LA SIERRA TRAMO 2	JEFATURA DE CONTRATOS DE LA RED VIAL
380	VIGO RIVERA CINTIA ROSSEMARIE	ESPECIALISTA TRIBUTARIO II	GERENCIA DE SUPERVISIÓN Y FISCALIZACIÓN
381	VILA QUEREVALU EVELYNN ELENA	ANALISTA LEGAL	GERENCIA DE ATENCIÓN AL USUARIO
382	VILCAPOMA VIRRUETA HANZ JOEL	ANALISTA DE CONTRATOS PORTUARIOS I	JEFATURA DE CONTRATOS PORTUARIOS
383	VILLEGAS BALAREZO DAVID ALEJANDRO	ANALISTA DE CONTRATOS FERROVIARIOS I	JEFATURA DE CONTRATOS FERROVIARIOS Y DEL METRO DE LIMA Y CALLAO
384	VOLTA ALOMIA MARIO MARTIN	SUPERVISOR DE OPERACIONES DE LA RED VIAL I	JEFATURA DE CONTRATOS DE LA RED VIAL
385	VONTRAT LINO ERIC CHARLES RAPHAEL	GERENTE ADJUNTO DE LA GERENCIA DE ATENCIÓN AL USUARIO	GERENCIA DE ATENCIÓN AL USUARIO
386	YABAR SANTILLAN JOSE LUIS	ABOGADO SENIOR	JEFATURA DE FISCALIZACIÓN
387	YNCIO MUÑOZ SOFIA TERESA	COORDINADOR PARLAMENTARIO	PRESIDENCIA EJECUTIVA
388	YNGA CELEDONIO JOSE FAUSTINO	ASISTENTE DE INVERSIONES EN PUERTOS	JEFATURA DE CONTRATOS PORTUARIOS
389	YUPANQUI TORRES RUTH ELENA	PROCURADOR PÚBLICO ADJUNTO	PROCURADURÍA PÚBLICA
390	ZAMBRANO COPELLO ROSA VERONICA	PRESIDENTE DEL CONSEJO DIRECTIVO	PRESIDENCIA EJECUTIVA
391	ZAMORA BARBOZA MARTHA YSABEL	ABOGADO SENIOR	JEFATURA DE ASUNTOS JURÍDICO REGULATORIOS Y ADMINISTRATIVOS
392	ZAPATA CRUZ LUIS ENRIQUE	MOTORIZADO	OFICINA DE GESTIÓN DOCUMENTARIA
393	ZARATE SALAS CRISTHIAN EMANUEL	SUPERVISOR ESTADÍSTICO FINANCIERO II	JEFATURA DE CONTRATOS DE LA RED VIAL
394	ZAVALETA ALTAMIRANO JORGE LUIS	SUPERVISOR IN SITU - RED VIAL 6: PUCUSANA - CERRO AZUL -ICA	JEFATURA DE CONTRATOS DE LA RED VIAL
395	ZAVALETA MEDINA JOSUE MACK LINDER	ANALISTA DE REGULACIÓN EN MATERIA DE AEROPUERTOS III	JEFATURA DE REGULACIÓN
396	ZEA VEGA RAFAEL	SUPERVISOR IN SITU II PARA LOS TRAMOS DESVÍO OLMOS - LAMBAYEQUE, MOCUPE-CAYALTI-OYOTÚN Y EMPALME 1B - BUENOS AIRES-CANCHAQUE	JEFATURA DE CONTRATOS DE LA RED VIAL
397	ZEGARRA PELAEZ ISABEL CECILIA	ASISTENTE DEL ÓRGANO DE CONTROL INSTITUCIONAL	ÓRGANO DE CONTROL INSTITUCIONAL
398	ZEGARRA ROMERO JOSÉ HÉCTOR	ASESOR LEGAL	JEFATURA DE ASUNTOS JURÍDICO REGULATORIOS Y ADMINISTRATIVOS
399	ZELADA ASMAT WALTER ROLANDO	SUPERVISOR IN SITU II PARA EL TRAMO 3 DE LA IIRSA SUR: INAMBARI - IÑAPARI	JEFATURA DE CONTRATOS DE LA RED VIAL

REGISTRO DE PERSONAL ACTIVO RIESGO BAJO DE EXPOSICIÒN		
PERSONAL	**CARGO**	**UNIDAD ORGANICA**
ASPILCUETA RUBIO MELISSA MARINA	JEFE DE LA OFICINA DESCONCENTRADA DE AREQUIPA	OFICINA DESCONCENTRADA DE AREQUIPA
CASTRO CUBA LEON JAVIER ERNESTO	JEFE DE LA OFICINA DESCONCENTRADA DE CUSCO	OFICINA DESCONCENTRADA DE CUSCO
FARFAN RIOS DAVIS HERITRON	ANALISTA DE ATENCIÓN AL USUARIO DE LA OFICINA DESCONCENTRADA DE CUSCO	OFICINA DESCONCENTRADA DE CUSCO
REATEGUI RIOS JOSE ENRIQUE	JEFE DE OFICINA DESCONCENTRADA DE LORETO	OFICINA DESCONCENTRADA DE IQUITOS
TORRES SOTO KHYRA DEL CHAYO	ANALISTA DE ATENCIÓN AL USUARIO DE LA OFICINA DESCONCENTRADA DE LORETO	OFICINA DESCONCENTRADA DE IQUITOS
GOMEZ GALARZA DE CAMPOS ERICKA BRIGITTE	RECEPCIONISTA	OFICINA DE GESTIÓN DOCUMENTARIA
REYES QUEZADA ISABEL JASMINE	AUXILIAR DE CONTROL DE CALIDAD EN MESA DE PARTES	OFICINA DE GESTIÓN DOCUMENTARIA

ANEXO 02
EVALUACIÓN DE LA APTITUD PARA EL REGRESO O REINCORPORACIÓN AL TRABAJO
(FICHA SINTOMATOLÒGICA)
DECLARACIÓN JURADA

Evaluación de la aptitud para el regreso o reincorporación al trabajo **Declaración Jurada**			
Apellidos y nombres			
Área de trabajo	DNI		
Dirección	Número (celular)		
En los últimos 7 días calendario he tenido alguno de los síntomas siguientes:		SI	NO
1. Sensación de alza térmica, fiebre o malestar			
2. Dolor de garganta, tos, estornudos o dificultad para respirar			
3. Dolor de cabeza, diarrea o congestión nasal			
4. Pérdida del gusto y/o del olfato			
5. Contacto con un caso confirmado de COVID-19			
6. Está tomando alguna medicación (detallar cuál o cuáles): _			
He recibido explicación del objetivo de esta evaluación y he respondido con la verdad.			
Fecha: / /	Firma del Servidor		

ANEXO 03
DECLARACIÒN JURADA DE ESTADO DE SALUD

OSITRAN	ORGANISMO SUPERVISOR DE LA INVERSIÓN EN INFRAESTRUCTURA DE TRANSPORTE DE USO PÚBLICO – OSITRÁN
	JEFATURA DE LOGISTICA Y CONTROL PATRIMONIAL – GERENCIA DE ADMINISTRACIÓN

DECLARACIÓN JURADA DE ESTADO DE SALUD

DECLARO BAJO JURAMENTO lo siguiente:

I. IDENTIFICACIÓN DEL CONTRATISTA

Apellido paterno: _____ Apellido materno: _____ Nombres: _____

Fecha de nacimiento: ___ ___ ___ Edad: _____ Sexo: M | F DNI: _____

Residencia: Departamento: _____ Provincia: _____ Distrito: _____

Número de teléfono: _____ Correo Electrónico: _____

Número de Contrato u Orden: _____

II. GERENCIA DONDE PRESTARA SERVICIOS Y OTROS DATOS: *(Escribe con Letra Imprenta)*

Gerencia, Jefatura u Oficina donde brindara el servicio		Lugar de la prestación del servicio	
		Descripción breve del servicio	

III. FACTOR O CONDICION DE RIESGO:

Declaro bajo juramento que los datos consignados que sustenta mi estado de salud actual se basan en los factores de riesgo siguiente:

	Marcar con X en el recuadro			Marcar con X en el recuadro	
	SI	NO		SI	NO
Hipertensión Arterial			Enfermedad respiratoria crónica		
Cáncer			Enfermedad renal crónica		
Diabetes mellitus			Enfermedad inmunodepresora		
Obesidad			Enfermedad Cardiovascular		
Gestación			Otro:		

Especifique:

Declaro **NO** encontrarme en los factores o condiciones de riesgo descritos: ☐

IV. OTROS FACTORES:	SI	NO	Detalle *(Consignar información de los dos (02) últimos meses)*
1. ¿Tuvo una Fractura?			
2. ¿Fue Operado?			
3. ¿Estuvo Internado?			
4. ¿Alergias algún medicamento?			
5. ¿Padece de Anemia?			
6. ¿Usa Audífonos para escuchar?			
7. ¿Tiene alguna discapacidad?			
8. Otros, especifique:			

4.1.- ANTECEDENTES COVID -19:	SI	NO	Detalle
1. ¿Usted se encuentra en una zona identificada como de alto riego por el COVID-19 según información oficial del MINSA?			*¿Lugar?*
2. ¿Usted ha tenido contacto en los últimos 14 días con alguna persona enferma o sospechosa de Coronavirus (COVID-19)?			
3. ¿Actualmente, usted presenta alguno de estos síntomas?			*Fiebre ( ) Tos ( ) Dolor de garganta ( )Problemas para respirar ( ) ninguno ( ) perdida del gusto ( ) perdida del olfato ( )*
INFORMACION ADICIONAL:			

V. DOCUMENTOS QUE DEBERÀ ADJUNTAR:

En caso, presente algún factor de riesgo el o los documentos que acrediten dichos factores o condiciones de riesgo, deberán ser presentados dentro de las 24 horas de ingresar a prestar servicios o cuando sean requeridos por el Servicio de Salud Ocupacional.

VI. DECLARACION DE GOZAR BUENA SALUD:		
Declaro GOZAR DE UNA BUENA CONDICIÓN DE SALUD FÍSICA Y MENTAL a la fecha de la suscripción del presente documento, que me permitirán desarrollar los servicios para la cual sería contratado. De consignar (NO) fundamente las razones: _____	SI	NO
Asimismo, autorizo que todo acto administrativo derivado del presente procedimiento se me notifique en el correo electrónico (email) consignado en el presente Declaración Jurada:	SI	NO
DECLARO BAJO JURAMENTO QUE LOS DATOS EXPRESAN LA VERDAD		

Asumo las responsabilidades correspondientes ante mi empleador, por la veracidad de la presente declaración jurada.

Asimismo, autorizo a Ositrán, el uso confidencial de la información brindada, sólo y exclusivamente para los fines de salvaguardar la salud y bienestar que pudieran encontrarse dentro de los grupos de riesgos establecidos por la norma (RM 972-2020-MINSA) o la norma que la sustituya.

APELLIDOS Y NOMBRES: _____ DNI N° _____ FECHA ____/____/____ FIRMA _____	HUELLA DIGITAL

ANEXO 4 LISTA DE CHEQUEO DE VIGILANCIA DE LA COVID 19				
Razón Social: OSITRAN		**RUC:**		
Domicilio: Calle Los Negocios 182	**Distrito: Surquillo**	**Provincia: Lima**	**Departamento: Lima**	
ELEMENTO		**CUMPLE (SI/NO)**	**Detalles/Pendientes/Por Mejorar**	
Ventilación natural o mecánica de los ambientes del centro de labores.				
Uso de medidores de C02 (recomendable).				
Se evalúa las condiciones de salud de todos los servidores periódicamente.				
Ficha sintomatológica de la Covid-19				
CASOS SOSPECHOSOS				
Aplicación de la Ficha epidemiológica de la COVID 19 establecida por el MINSA a todos los casos sospechosos en servidores de bajo riesgo.				
Identificación de contactos de casos sospechosos.				
Se realiza el seguimiento clínico a distancia al servidor identificado como sospechoso.				
MEDIDAS DE HIGIENE				
Se aseguran los puntos de lavado de manos con agua potable, jabón líquido o jabón desinfectante y papel toalla o puntos de alcohol.				
Se colocan carteles en las partes superiores de los puntos de lavado para la ejecución adecuada del método de lavado correcto o el uso de alcohol para la higiene da manos.				
SENSIBILIZACIÓN DE LA PREVENCIÓN DEL CONTAGIO EN EL CENTRO DE TRABAJO				
Se difunde información sobre coronavirus y medios de protección laboral en lugares visibles				
Se difunde la importancia del lavado de manos, toser o estornudar cubriéndose la boca con la flexura del codo, no tocarse el rostro, entre otras prácticas de higiene.				
Los servidores de grupos de riesgo o con síntomas respiratorios agudos, utilizan mascarillas de acuerdo con el nivel de riesgo del puesto de trabajo.				
Se facilitan medios para responder las inquietudes de los servidores respecto al COVID-19.				
MEDIDAS PREVENTIVAS				
Existen medidas de protección a los servidores en puestos de atención al cliente, mediante el empleo de barreras físicas.				
Se establecen puntos estratégicos para el acopio y entrega de EPP.				
Se entrega EPP de acuerdo con el nivel de riesgo.				
El servidor utiliza correctamente el EPP				
El centro laboral promueve y facilita el esquema completo de vacunación para el Covid-19.				
SALUD DEL SERVIDOR				
Se indica evaluación médica de síntomas a todo servidor que presente temperatura corporal mayor a 37.5°C y/o síntomas respiratorios agudos.				
Se consideran medidas de salud mental (especificar)				
Se registra en el SISCOVID a todos los servidores que pasen por una prueba de la COVID 19				
El servidor será evaluado para determinar la continuidad de actividades en centro de labores o el otorgamiento de descanso mèdico				

ANEXO 05

AFORO MÁXIMO DE SEDE CENTRAL (*)

PISO	N° máximo de personas en cada ambiente	AREAS	OBSERVACIONES
1	8	RECEPCION	
	3	SERVICIOS GENERALES	
	5	TOPICO	
	5	POOL DE CHOFERES	
	40	COMEDOR	SIN MESAS
2	12	OGD-LINEA DE DIGITALIZACION	
	30	OGD	
	4	OGD TEMPORAL	25 PERSONAS COMO SALA DE REUNIONES-SIN MESA
	4	LACTARIO	
	12	KITCHENETTE	
	56	SALA - CARRETERAS SEGURAS	SIN MESAS
	30	SALA - AEROPUERTOS TECNOLOGICOS	SIN MESAS
	19	SALA - ESTACION OSITRAN	SIN MESAS
	18	SALA - PUERTOS SOSTENIBLES	SIN MESAS
	3	OP-01	OFICINAS PRIVADAS
	3	OP-02	OFICINAS PRIVADAS
	3	STPAD	
	3	OCC	
	18	MODULOS	
	12	RECEPCION	
3	8	RECEPCION	
	15	SALA DE EXPOSICION	SIN MESAS
	4	SALA - HIDROVIAS NAVEGABLES	CON MESAS
	4	SALA - METROS DEL FUTURO	CON MESAS
	10	SALA DE REUNIONES DE PD	CON MESA
	14	MODULOS	
	2	SECRETARIA DE GG	
	3	SECRETARIA DE PD	
	12	JEFATURA DE TECNOLOGIA DE LA INFO	
	13	PROCURADURIA	
	14	OCI	

(*) Información proporcionada por la JLCP

ANEXO 06

EQUIPOS DE PROTECCIÓN PERSONAL PARA PUESTO DE TRABAJO CON RIESGO DE EXPOSICIÓN A LA COVID-19 SEGÚN EL NIVEL DE RIESGO

Nivel de riesgo de protección biológica	Barreras de protección		Equipos de protección personal (****)					
	Mascarilla comunitaria (Tela)	Mascarilla quirúrgica	Respirador FFP2/N95 o equivalentes*	Careta Facial**	Gafas de protección	Guantes para protección biológica ***	Traje de protección biológica	Botas para la protección biológica
Riesgo muy alto de exposición			o	c	o	o	c	c
Riesgo alto de exposición			o	c	o	o	C (*)	
Riesgo medio de exposición	O*	o	c	c	c			
Riesgo bajo de exposición (de precaución)	C	C	c	c	c			

O-Obligatorio O (*) Uso de delantal o bata

C Condicional a personas de bajo o mediano riesgo cuando cumplan con actividades excepcionales de alto riesgo como campañas médicas, visitas a emergencias de hospitales o centros de salud, contacto cercano con personas sospechosas o con la COVID-19 positivo y otras actividades relacionadas a salud.

El uso de doble mascarilla puede ser reemplazado por el uso de una KN95 o su equivalente.

O* El uso de mascarilla comunitaria en servidores de mediano riesgo de exposición es permitido siempre y cuando se complemente con una mascarilla quirúrgica adicional.

*El uso de equipo de protección respiratoria específica (FFP2, N95 o equivalentes) es de uso exclusivo para servidores de salud con muy alto y alto riesgo de exposición biológica al virus SARS-CoV-2 que causa la COVID-19.

**Se recomienda el uso de careta facial, de acuerdo con la comodidad del servidor en actividades con alta conglomeración de personas, pero su uso no es obligatorio. Cuando se usan lentes de protección ocular no es necesario el uso de careta facial.

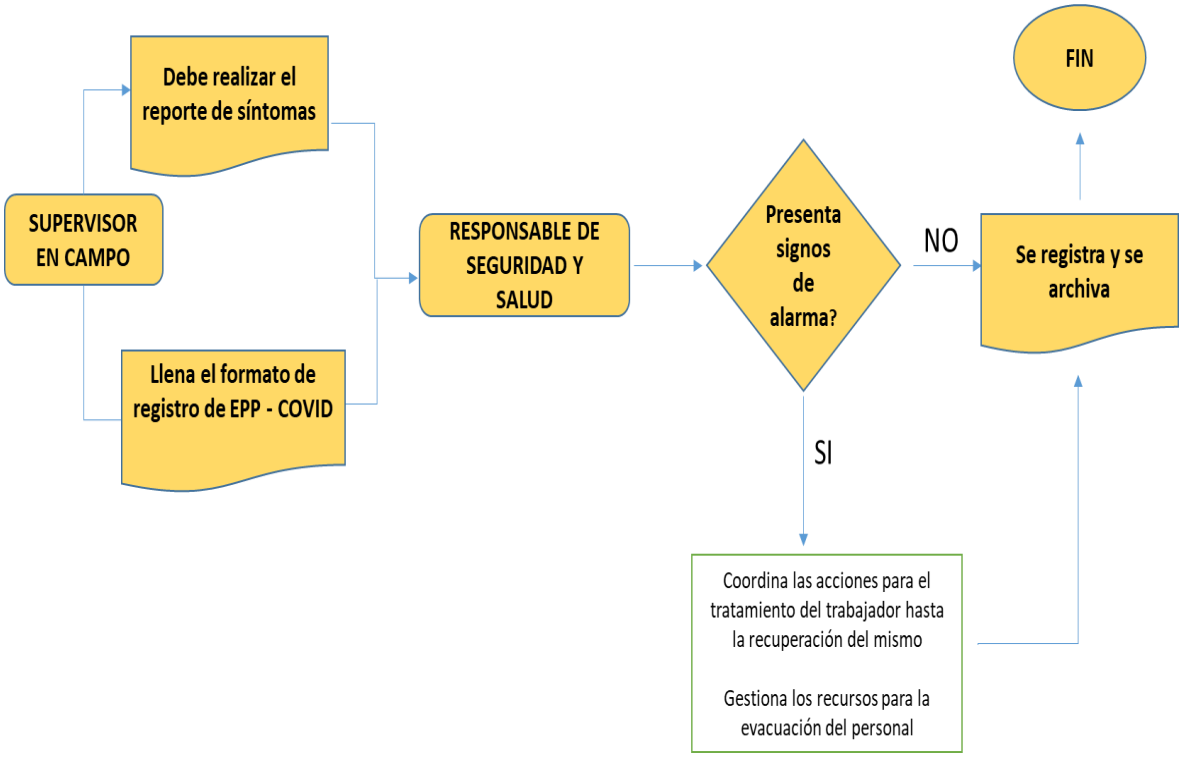
* La evidencia ha demostrado que el uso de guantes no es una forma eficiente para protegerse del virus, genera un falso sentimiento de seguridad y de no ser bien utilizados pueden convertirse en un agente transportador del virus por lo que puede ser perjudicial e incrementa el riesgo de contaminación cruzada. Por lo que NO es recomendable el uso de guantes, salvo por personal entrenado como el personal de salud para procedimientos con el paciente y/o en casos puntuales como personal de limpieza u otros que apruebe el personal de Salud y Seguridad en el Trabajo de la institución.

** La única Autoridad que puede exigir el uso de EPP adicional es el propio Ministerio de Salud en base a evidencia. La relación de EPP precisada en este Anexo es lo mínimo obligatorio para el puesto de trabajo; además, el servicio de seguridad y salud en el trabajo debe realizar una evaluación de riesgos para determinar si se requieren otros equipos de protección personal adicionales.

Asimismo, las mascarillas, los respiradores N95 o sus equivalentes, los guantes y trajes para protección biológica, deben cumplir normativas asociadas a protección biológica, y la certificación correspondiente.

ANEXO 07

FLUJOGRAMA DE COMUNICACIÓN



Responsable de Seguridad y Salud = Profesional de la Salud.
Supervisor en campo = Personal en campo.

ANEXO N° 08

Guía para el uso de medidores de C02 en ambientes de trabajo y escuelas

Los medidores portátiles de dióxido de carbono (C02) permiten verificar que el aire de los ambientes se renueva permanentemente a través de una ventilación adecuada.

El nivel de $C0_2$ indica el grado de no circulación del aire interior. Al respirar, junto con los aerosoles, las personas exhalan C02, por lo que la acumulación de este gas es un buen indicador de la acumulación de aerosoles que podrían transmitir la COVID-19 . En este sentido, el monitoreo del C02 permite regular el nivel de apertura de ventanas y puertas necesario para una mantener una adecuada ventilación en un ambiente interior,

El nivel del C02 al aire libre se encuentra en una concentración de **400 partes por millón (ppm).** Este nivel puede variar, en zonas urbanas con alto tránsito vehicular o presencia de industrias.

Nivel base de $C0_2$

El nivel de concentración de C02 de un ambiente sin personas, se denomina **nivel de base de $C0_2$**. Cuando en un ambiente interior el C02 aumenta en 400 partes por millón por sobre el nivel de base del ambiente, producto de la respiración de las personas que ocupan ese espacio, se estima que el 1% del aire que se respira ya fue respirado por otra persona.

El umbral de concentración de C02 que actualmente se recomienda como indicador de una ventilación adecuada es de 400 ppm por sobre el nivel de base.

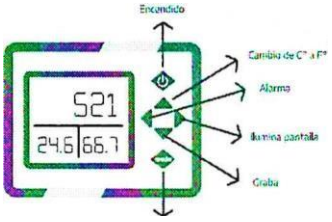
Cuando la concentración de $C0_2$ se incrementa en 400 ppm por sobre la medición con la oficina o el aula vacía (medición de base o medición basal), se debe actuar para mejorar la ventilación.

Existe consenso en que es deseable que el nivel de $C0_2$ en escuelas, hogares, oficinas, etc. se ubique por debajo de las 1.000 ppm.

Como muestra la tabla 1, el valor de C02 a partir del cual se debe procurar mejorar la ventilación difiere según las condiciones iniciales (sin personas presentes) . Así, por ejemplo, para un aula donde la medición de base arroje 350 ppm, el valor de alerta mientras transcurra la clase será de 750 ppm, mientras que para un aula donde la medición de base indique 650 ppm, el valor de alerta será de 1050 ppm.

No es necesario esperar a que la medición se incremente 400 ppm para actuar. La situación ideal es que durante el trabajo o la clase la medición del C02 se mantenga en niveles similares a los del ambiente de trabajo o el aula vacía (lo cual es posible cuando hay buena ventilación), cuando la medición muestre un aumento de 250 o 300 ppm se debe abrir más las puertas y ventanas para procurar que el valor descienda o se estabilice.

En el caso de los pasillos de circulación y otros espacios no ocupados en forma permanente, la concentración de C02 no se debe incrementar en más de 150/200 ppm con relación al valor que arroja el espacio exterior, para garantizar la renovación del aire que ingrese desde los pasillos a los interiores.



Pantalla de equipo portátil simple de medición de C02

Tabla N° 01 Niveles de alerta para un conjunto de oficinas u aulas ante el aumento de la concentración de dióxido de carbono por la respiración humana.

	Baja temperatura	Incremento de C02 con ambiente ocupado por personas (efecto de la respiración humana					
		Medición de base (aula vacía)	100	300	375	400 (umbral de ventilación adecuada)	800
Trabajo o escuela	Oficina o aula 1	400	500	700	775	800	1200
	Oficina o aula 2	450	550	750	825	850	1250
	Oficina o aula 3	500	600	800	875	900	1300
	Oficina o aula 4	550	650	850	925	950	1350
	Oficina o aula 5	600	650	900	975	1000	1400
	Riesgo de contagio	Muy bajo		Bajo	Medio bajo	Medio alto a muy alto	

Fuente: modificado de la Guía de recomendaciones para la prevención de la transmisión de COVID-19 en la provincia de Buenos Aires

Al encender el equipo luego de un breve lapso de precalentamiento, comenzará a mostrar en pantalla los valores relativos al nivel de C02 y de otras variables (temperatura, porcentaje de humedad relativa), dependiente del modelo del aparato.

Ubicación del medidor de dióxido de carbono en el ambiente de trabajo o aula:

- A un metro y medio o más de distancia de las personas: si se ubica cerca de las personas se podría alterar la medición, pues los dispositivos son muy sensibles a toda fuente de C02, incluida la exhalación directa
- A una altura de un metro o un metro y medio del piso o Lo más alejado posible de puertas y ventanas.
- De ser posible, ubicarlo aproximadamente en el centro del aula o ambiente de trabajo .

Ante situaciones donde la medición indique incrementos cercanos al umbral de 400 ppm, resulta conveniente que se realicen otras mediciones en distintos lugares del aula, especialmente en aquellos espacios donde se sospeche que hay menor ventilación

¿Cómo se realiza la medición?

- ✓ Ventilar bien la oficina o el aula antes de iniciar la medición (lo más posible). La medición de base deberealizarse sin presencia de personas y con el ambiente preparado del mismo modo en que habitualmente se desarrollan las clases o el trabajo. Con la puerta y las ventanas en una posición fija (si se utilizan habitualmente, con el aire acondicionado o calefacción encendida).
- ✓ Si es posible, evitar realizar la medición cuando las condiciones del viento sean atípicas (si es que la puerta o alguna de las ventanas da al aire libre).
- ✓ Encender y, si corresponde, aguardar el tiempo de precalentamiento. El medidor demora en estabilizarse, por lo que es aconsejable no prenderlo y apagarlo entre mediciones.
- ✓ Al comenzar la medición, el valor de C02 puede oscilar entre +/- 50 ppm durante dos minutos. Si se observa un cambio de la concentración de C02 mayor a las 50 ppm, que es la resolución del medidor,significa que el valor está cambiando y que se debe esperar a su estabilización
- ✓ Registrar el valor de C02 de la medición inicial (previa al ingreso de personas al aula) . Este es el valorde base contra el cual se deberán comparar los valores que se registren durante el transcurso de la clase.
- ✓ Monitorear y registrar el valor del C02 durante distintos momentos de la clase o jornada de trabajo (porejemplo, en las escuelas, a la mitad de la jornada antes del recreo y al finalizar la jornada)

Se debe realizar la medición una vez por semana durante dos semanas consecutivas, en cada turno de trabajo o clase en caso de una escuela

Se pueden realizar todas las mediciones adicionales que se consideren necesarias (mayor cantidad de personas en el grupo, realización de actividades de intensidad diferente, etc.).

¿Qué hacer si la medición arroja valores mayores a 400 ppm por encima del valor base?
Se deben poner en marcha acciones correctivas considerando las posibilidades de ventilación del ambiente.

1. Abrir las puertas y ventanas tanto como sea posible. Si hay varias ventanas es mejor abrir un poco todas que abrir bien solo una.
2. Si luego de aplicar medidas correctivas a través de la ventilación natural, se realiza una nueva medición sin resultados satisfactorios, se pueden instrumentar alternativas simples de ventilación mecánica, como colocar un ventilador en puertas o ventanas con el flujo de aire en dirección al exterior.
3. En el caso de que las puertas y ventanas del aula u oficina den a un pasillo interior con poca circulación de aire o a un patio interno cerrado en los que las mediciones estén por encima del límite, se deben cerrar estas aberturas lo máximo posible, dejando solo una pequeña apertura . A la vez, hay que abrir lo más posible las puertas o ventanas que den al aire libre exterior o a otros espacios interiores bien ventilados, pudiendo utilizar ventiladores que apunten hacia allí, de modo que ayuden a la renovación del aire

4. Un resultado satisfactorio en la medición de C02 en un aula u oficina implica que se puedan relajar otras medidas de prevención de riesgo, como el distanciamiento social o el uso correcto y constante de mascarillas. Cómo se mencionó, las medidas de cuidado implican estrategias de reducción de riesgo que atacan diferentes formas de posible contagio y por tanto, son complementarias.
5. Si no se puede mantener el nivel de C02 lo suficientemente bajo mientras las personas se encuentren térmicamente cómodas, se deberán evaluar otras alternativas como reducir el tiempo de duración del bloque de clases.
6. En el caso de que las mediciones determinen que ninguna de las acciones correctivas ha resultado efectiva, se requerirá un espacio alternativo para la continuidad de las clases presenciales o limitar el número de personas que utilizan el aula (ampliando el distanciamiento físico).
7. Existen técnicas de limpieza del aire, como la filtración, que si bien eliminan los aerosoles no cambian la concentración de C02 en el ambiente. Por esta razón, en los espacios donde se filtra el aire se puede tolerar un nivel más alto de variación del C02 (alrededor de 200 ppm adicionales). Dado que el filtrado complementa a la ventilación, pero no la reemplaza, siempre es más recomendable ventilar que filtrar.

La ventilación es una medida complementaria de prevenc1on y es efectiva si además se mantienen las otras medidas de cuidado como mascarillas y distanciamiento y tiempo de permanencia en el ambiente.