

**PERÚ**Presidencia
del Consejo de MinistrosOrganismo Supervisor de la
Inversión en Infraestructura de
Transporte de Uso Público

Presidencia del Consejo Directivo

RESOLUCION DE PRESIDENCIA**N° 0083-2025-PD-OSITRAN**

Lima, 02 de octubre de 2025

VISTO:

El Informe N° 0438-2025-JTI-GA-OSITRAN, de la Jefatura de Tecnologías de la Información de la Gerencia de Administración; el Memorando N° 0401-2025-GAJ-OSITRAN de la Gerencia de Asesoría Jurídica; el Memorando N° 511-2025-GG-OSITRAN de la Gerencia General; y

CONSIDERANDO:

Que, el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, establece el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales, por parte de las entidades de la Administración Pública en los tres niveles de gobierno;

Que, el artículo 8 del Decreto Legislativo antes citado prevé que la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de gobierno digital que comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos, seguridad digital y arquitectura digital. Dicta las normas y establece los procedimientos en materia de gobierno digital y, es responsable de su operación y correcto funcionamiento;

Que, mediante Decreto de Urgencia N° 007-2020, se aprobó el Marco de Confianza Digital y dispone medidas para su fortalecimiento, cuyo numeral 9.3 de su artículo 9 dispone que las entidades de la administración pública deben implementar un Sistema de Gestión de Seguridad de la Información (SGSI), un Equipo de Respuesta ante Incidentes de Seguridad Digital (CSIRT por sus siglas en inglés) cuando corresponda, y cumplir con la regulación emitida por la Secretaría de Gobierno y Transformación Digital (SGTD), ente rector en materia de Confianza Digital;

Que, el Reglamento de la Ley de Gobierno Digital, aprobado mediante el Decreto Supremo N° 029-2021-PCM, contiene disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo; estableciendo en su artículo 104 disposiciones asociadas a la conformación de un Equipo de Respuesta ante Incidentes de Seguridad Digital (CSIRT) en las entidades de la Administración Pública;

Que, el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros ha emitido la "Guía para la conformación e implementación de Equipos de Respuesta ante Incidentes de Seguridad Digital", documento que se constituye en una guía orientadora para que las entidades públicas conformen e implementen el Equipo de Respuesta ante Incidentes de Seguridad Digital;

Que, a través del Informe N° 0438-2025-JTI-GA-OSITRAN, la Jefatura de Tecnologías de la Información de la Gerencia de Administración, ha sustentado la necesidad de conformar el Equipo de Respuesta ante Incidentes de Seguridad Digital del Ositrán, en atención a lo dispuesto en el marco normativo previamente señalado;

Que, mediante el Memorando N° 0401-2025-GAJ-OSITRAN, la Gerencia de Asesoría Jurídica señala que considera jurídicamente viable la conformación del Equipo de Respuesta ante Incidentes de Seguridad Digital del Ositrán;

**PERÚ**Presidencia
del Consejo de MinistrosOrganismo Supervisor de la
Inversión en Infraestructura de
Transporte de Uso Público

Presidencia del Consejo Directivo

Que, por medio del Memorando N° 0511-2025-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;

De conformidad con lo dispuesto en el Reglamento de Organización y Funciones del Ositrán, aprobado por Decreto Supremo N° 012-2015-PCM y modificatorias; el Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital; el Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412; y el Decreto de Urgencia N° 007-2020, que establece el Marco de Confianza Digital y medidas para su fortalecimiento en las entidades de la administración pública;

SE RESUELVE:

Artículo 1.- Conformar el Equipo de Respuesta ante Incidentes de Seguridad Digital (Computer Security Incident Response Team, CSIRT) del Organismo Supervisor de la Inversión en Infraestructura de Transporte de Uso Público – Ositrán, el mismo que estará integrado por:

- a) El Oficial de Seguridad y Confianza Digital, en calidad de Coordinador del CSIRT.
- b) El Jefe de Tecnologías de la Información, en calidad Miembro del CSIRT.
- c) El Coordinador de Sistemas de Información, en calidad Miembro del CSIRT.
- d) El Coordinador de Infraestructura Tecnológica, en calidad Miembro del CSIRT.
- e) El Especialista en Redes y Telecomunicaciones, en calidad Miembro del CSIRT.
- f) El Especialista en Seguridad de la Información y Ciberseguridad, en calidad Miembro del CSIRT.
- g) El Especialista en Administración de Base de Datos y Aplicaciones, en calidad Miembro del CSIRT.
- h) El Responsable de Servicios de TI, en calidad Miembro del CSIRT.

Artículo 2.- Son responsabilidades del Equipo de Respuestas ante Incidentes de Seguridad Digital (CSIRT) del Organismo Supervisor de la Inversión en Infraestructura de Transporte de Uso Público – Ositrán, las siguientes:

- a) El Equipo de Respuestas ante Incidentes de Seguridad Digital (CSIRT) es responsable de adoptar medidas para la gestión de riesgos e incidentes de seguridad digital que afecten a los activos del Ositrán.
- b) El Equipo de Respuestas ante Incidentes de Seguridad Digital (CSIRT) es responsable de coordinar la difusión de alertas tempranas, avisos e información sobre riesgos e incidentes de seguridad digital en el Ositrán.
- c) El Equipo de Respuestas ante Incidentes de Seguridad Digital (CSIRT) es responsable de monitorear el cumplimiento de estándares, normas técnicas y mejores prácticas de seguridad ampliamente reconocidos, por parte de los proveedores de servicios tecnológicos del Ositrán.
- d) El Equipo de Respuestas ante Incidentes de Seguridad Digital (CSIRT) es responsable de gestionar las lecciones aprendidas, a través del análisis de causa – raíz, identificación de fallos en los procedimientos y proponer ajustes en políticas, controles y tecnologías.
- e) El Equipo de Respuestas ante Incidentes de Seguridad Digital (CSIRT) asume la responsabilidad de otras acciones relacionadas con la gestión de incidentes de seguridad digital, que determine el Comité de Gobierno y Transformación Digital del Ositrán o que sean requeridas para el cumplimiento del marco normativo en la materia.
- f) El Oficial de Seguridad y Confianza Digital en su calidad de Coordinador del CSIRT, es responsable de realizar todas las actividades de gestión del CSIRT.

- g) El Oficial de Seguridad y Confianza Digital en su calidad de Coordinador del CSIRT, es responsable de comunicar, al Centro Nacional de Seguridad Digital, todo incidente de seguridad digital.
- h) El Oficial de Seguridad y Confianza Digital es responsable de coordinar y/o colaborar con el Centro Nacional de Seguridad Digital o los CSIRT de otras Entidades Públicas u organizaciones privadas, las acciones correspondientes para recibir apoyo para la atención de incidentes de seguridad digital, en el caso de requerirlo.
- i) El Jefe de Tecnologías de la Información es responsable de gestionar los recursos necesarios para asegurar la efectiva gestión de incidentes de seguridad digital en el Ositrán.
- j) El Coordinador de Sistemas de Información es responsable de gestionar todo incidente de seguridad que implique o se relacione con la modificación, actualización u optimización del código de los sistemas de información y aplicaciones.
- k) El Coordinador de Infraestructura Tecnológica es responsable de gestionar todo incidente de seguridad que implique la afectación a las operaciones, sistemas, aplicaciones y servicios en la infraestructura tecnológica tanto de redes, conectividad, hardware o software.
- l) El Especialista en Redes y Telecomunicaciones es el responsable de la seguridad de las redes y comunicaciones, servidores e infraestructuras de TI, servicios en nube de la entidad para la protección de la integridad, confidencialidad y disponibilidad de los activos de TI que puedan verse afectados en un incidente de seguridad digital.
- m) El Especialista de Seguridad de la Información y Ciberseguridad es el responsable de la gestión, monitoreo y seguimiento de los incidentes de seguridad digital hasta su superación definitiva.
- n) El Especialista de Seguridad de la Información y Ciberseguridad es responsable de elaborar los protocolos y/o procedimientos o guías necesarias para la atención de los incidentes de seguridad digital, así como asegurar su implementación y actualización permanente.
- o) El Especialista en Administración de Base de Datos y Aplicaciones es responsable de recuperar y monitorear las bases de datos y la operación de las aplicaciones críticas comprometidas en el incidente de seguridad de la información.
- p) El Responsable de Servicios de TI es responsable de gestionar el registro de incidentes y brindar soporte a los usuarios afectados hasta la solución definitiva.

Artículo 3.- Disponer que la Jefatura de Tecnologías de la Información brinde el soporte y facilidades necesarias para el cumplimiento de las responsabilidades del Equipo de Respuestas ante Incidentes de Seguridad Digital (CSIRT) del Ositrán.

Artículo 4.- Notificar la presente Resolución a la Secretaría de Gobierno y Transformación Digital (SGTD) de la Presidencia de Consejo de Ministros, así como a los miembros designados en el artículo primero de la presente Resolución, para su conocimiento y fines pertinentes.

Artículo 5.- Disponer la difusión de la presente Resolución en el portal institucional del Ositrán ubicado en la Plataforma Digital Única del Estado Peruano para Orientación al Ciudadano (www.gob.pe/ositrán).

Regístrese y comuníquese,

Firmado por
VERÓNICA ZAMBRANO COPELLO
Presidente del Consejo Directivo
Presidencia Ejecutiva



PERÚ

Presidencia
del Consejo de Ministros

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

Presidencia del Consejo Directivo

Visado por

JUAN CARLOS MEJÍA CORNEJO

Gerente General

Gerencia General

Visado por

CÉSAR TALLEDO LEÓN

Jefe de Tecnologías de la Información

Jefatura de Tecnologías de la Información

Visado por

JAVIER CHOCANO PORTILLO

Jefe de la Gerencia de Asesoría Jurídica

Gerencia de Asesoría Jurídica

NT: 2025137200

Documento electrónico firmado digitalmente en el marco de la Ley N°27269, Ley de Firmas y Certificados Digitales, su Reglamento y modificatorias.
La integridad del documento y la autoría de la(s) firma(s) pueden ser verificadas en: <https://apps.firmaperu.gob.pe/web/validador.xhtml>