CONTRALORÍA
GENERAL DE LA REPÚBLICA DEL PERÚ

ÓRGANO DE CONTROL INSTITUCIONAL DE LA SUPERINTENDENCIA NACIONAL DE ADUANAS Y DE ADMINISTRACIÓN TRIBUTARIA

INFORME DE AUDITORÍA N° 049-2025-2-3793-AC

AUDITORÍA DE CUMPLIMIENTO
SUPERINTENDENCIA NACIONAL DE ADUANAS Y DE ADMINISTRACIÓN TRIBUTARIA
LIMA/LIMA/LIMA

"GESTIÓN DE INCIDENCIAS ANTE FALLAS TÉCNICAS EN LOS SISTEMAS INFORMÁTICOS DE LA SUNAT PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES TRIBUTARIAS Y ADUANERAS"

PERÍODO: 1 DE ENERO DE 2021 AL 31 DE JULIO DE 2025

TOMO (I) DE (I)

LIMA, 28 DE NOVIEMBRE DE 2025

LIMA – PERÚ

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la recuperación y consolidación de la Economía Peruana"

0716

0492025237930 0

001

CONTRALORÍA
GENERAL DE LA REPÚBLICA DEL PERÚ

INFORME DE AUDITORÍA N.° 049-2025-2-3793-AC

"GESTIÓN DE INCIDENCIAS ANTE FALLAS TÉCNICAS EN LOS SISTEMAS INFORMÁTICOS DE LA SUNAT PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES TRIBUTARIAS Y ADUANERAS"

ÍNDICE

DENOMINACIÓN	N.° Pág.
I. ANTECEDENTES	1
1.1 Origen	1
1.2 Objetivos	1
1.3 Materia de Control, Materia Comprometida y Alcance	2
1.4 De la entidad o dependencia	4
1.5 Notificación de las desviaciones de cumplimento	7
1.6 Aspectos relevantes	7
II. DEFICIENCIAS DE CONTROL INTERNO	8
III. OBSERVACIÓN EL SUPERVISOR DE LA DIVISIÓN DE GESTIÓN DE INFRAESTRUCTURA TECNOLÓGICA BRINDÓ FACILIDADES AL ESPECIALISTA RESIDENTE, PARA REALIZAR TRABAJOS EN HORARIOS DISTINTOS AL CONTEMPLADO EN LAS BASES INTEGRADAS, REGISTRANDO SU INGRESO EL 31 DE MAYO DE 2024 A LAS 12:18 HORAS, POSTERIOR A LA OCURRENCIA DEL INCIDENTE REGISTRADO A LAS 12:05 HORAS, LIMITANDO CON ELLO LA DETECCIÓN OPORTUNA DE ALERTAS, CON EL PROPÓSITO DE CONTENER LA INTERRUPCIÓN MASIVA DE LOS SISTEMAS INFORMÁTICOS; AFECTANDO LA DISPONIBILIDAD CONTINUA DE LOS SERVICIOS TRIBUTARIOS Y ADUANEROS. .	36
IV. ARGUMENTOS JURÍDICOS	46
V. IDENTIFICACIÓN DE PERSONAS COMPRENDIDAS EN LOS HECHOS OBSERVADOS	46
VI. CONCLUSIONES	46
VII. RECOMENDACIONES	48
VIII. APÉNDICES	49

SUNAT Órgano de Control Institucional JEFE RICARDO ANDRÉS LIEVA EYZAGUIRRE

INFORME DE AUDITORÍA N.°049-2025-2-3793-AC

"GESTIÓN DE INCIDENCIAS ANTE FALLAS TÉCNICAS EN LOS SISTEMAS INFORMÁTICOS DE LA SUNAT PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES TRIBUTARIAS Y ADUANERAS"

PERÍODO: 1 DE ENERO DE 2021 AL 31 DE JULIO DE 2025

1. ANTEDECENTES

1.1 Origen

La Auditoría de Cumplimiento a la Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT), en adelante "entidad", corresponde a un servicio de control posterior programado en el Plan Anual de Control 2025 del Órgano de Control Institucional, en adelante "OCI", a cargo del servicio de control, registrado en el Sistema de Control Gubernamental – SCG, con la orden de servicio N.°2-3793-2025-006, cuyo inicio fue comunicado mediante Memorándum N.° 00186-2025-SUNAT/1C0000 de 11 de agosto de 2025 en el marco de lo previsto en la Directiva N.°001-2022-CG/NORM "Auditoría de Cumplimiento" y el Manual de Auditoría de Cumplimiento aprobados mediante Resolución de Contraloría N.°001-2022-CG de 7 de enero de 2022 y modificatorias.

1.2 Objetivos

Objetivo General

Determinar si la Intendencia Nacional de Sistemas de la Información gestionó la provisión de la infraestructura tecnológica para soportar a los procesos de la SUNAT, así como de la gestión de accesos a los sistemas informáticos, de acuerdo con lo establecido en la normativa y disposiciones internas vigentes y aplicables.

Objetivos Específicos

1. Determinar si el Servicio de Soporte brindado a la infraestructura tecnológica de la SUNAT en el marco del de los Contratos N.°267-2020/SUNAT - Prestación Principal, 268-2020/SUNAT Prestación Accesoria y 143-2024/SUNAT - Prestación Principal sobre el incremento de capacidad de la solución de Nube Privada, fueron efectuados conforme a lo establecido en la normativa, estipulaciones contractuales y disposiciones internas vigentes y aplicables.

2. Determinar si las actividades de monitoreo y la gestión de eventos informáticos, que comprenden la identificación, registro, comunicación, y solución de incidentes fueron ejecutados conforme a lo establecido en la normativa y disposiciones internas vigentes aplicables.

3. Determinar si la Intendencia Nacional de Sistemas de la Información cumplió con las medidas de seguridad de la información, conforme a lo establecido en la normativa y disposiciones internas vigentes aplicables.

1.3 Materia de Control, Materia Comprometida y Alcance

Materia de Control

La SUNAT en su Plan Estratégico Institucional (PEI) para el año 2024-2028, ha establecido entre sus objetivos estratégicos institucionales, el Objetivo Estratégico Institucional - OEI 01: **Mejorar el Cumplimiento Tributario y Aduanero de los Administrados**, el cual está orientado a mejorar los niveles del cumplimiento de los administrados respecto de las obligaciones que tiene a cargo administrar, promoviendo el cumplimiento voluntario e implementando soluciones que limiten las posibilidades de incumplimiento, aprovechando la disponibilidad de información y las más avanzadas soluciones tecnológicas; asimismo, dicho objetivo está vinculado con la Acción Estratégica Institucional AEI 01.04 **Modernización y transformación digital de los procesos de la entidad** y AEI 01.07: **Servicios Virtuales con disponibilidad garantizada para los administrados.**

En razón de ello, plantea contar con la infraestructura informática que permita garantizar la continuidad operativa y contribuya al mejoramiento del nivel de disponibilidad de los servicios informáticos que brinda la Intendencia Nacional de Sistemas de Información (INSI), a través de la **Provisión de una solución de nube privada**.

En ese sentido, la materia de control está vinculada al Proceso A-03.1 Soporte de servicios informáticos, el cual forma parte del Macroproceso de A-03 *GESTIÓN DE SISTEMAS DE INFORMACIÓN*, dicho proceso tiene por objetivo proveer un adecuado soporte de servicios informáticos a los usuarios, incluyendo el manejo de incidentes y problemas que se puedan presentar como parte de la operatividad del servicio. Asimismo, se encarga de monitorear permanentemente el nivel de servicio informático a fin de garantizar una toma de decisiones oportuna para mantener la calidad del servicio ofrecido por Intendencia Nacional de Sistemas de Información (INSI).

Materia Comprometida

La materia comprometida esta vinculada a la capacidad de gestión de la Intendencia Nacional de Sistemas de Información (INSI), ante las incidencias alertadas de los sistemas informáticos de la SUNAT, los cuales son utilizados por los Contribuyentes a nivel nacional con el objeto de facilitar el cumplimiento de las obligaciones tributarias y aduanera; precisando que, dichos sistemas están soportados por una infraestructura informática cuya finalidad es garantizar la continuidad operativa y la disponibilidad de los servicios informáticos.

Asimismo, comprendió la revisión y análisis de la información alcanzada por la Gerencia de Operaciones y Soporte de Usuarios y sus Divisiones, así como de la información remitida por la Gerencia de Orientación y Servicios de la Intendencia Nacional de Gestión de Procesos.

Alcance

La Auditoría de Cumplimiento comprendió el período del 1 de enero de 2021 al 31 de julio 2025, se realizó a las subunidades orgánicas de la Intendencia Nacional de Sistemas de la Información (INSI), entre ellas, la Gerencia de Operaciones y Soporte a

Usuarios, la División de Soporte y Operaciones de la Infraestructura Tecnológica, la División de Gestión de Infraestructura Tecnológica y la División de Atención a Usuarios, las cuales forman parte de los órganos dependientes de la Superintendencia Nacional ubicadas en la Av. Coronel Andrés Reyes 320, San Isidro, Lima.

La Comisión Auditora desarrolló sus actividades en las oficinas del Órgano de Control Institucional de la SUNAT, ubicado en Av. Garcilaso de la Vega 1456, Lima (Piso 16, Edificio Sulamerica)

Siglas:

1. DAU : División de Atención a Usuarios
2. DGIT : División de Gestión de Infraestructura Tecnológica
3. DSOIT : División de Soporte y Operación de la Infraestructura Tecnológica
4. GOSU : Gerencia de Operaciones y Soporte a Usuarios
5. OSI : Oficina de Seguridad Informática
6. GOS : Gerencia de Orientación y Servicios
7. INGP : Intendencia Nacional de Gestión de Procesos
8. DEC : División de Ejecución Contractual
9. GDCUA : Gerencia de Defensoría del Contribuyente y Usuario Aduanero

Definiciones

1. Cuenta administrativa	:	Las cuentas administrativas, o cuentas de administrador, son cuentas del colaborador con privilegios administrativos completos para realizar cambios en un sistema.
2. Herramienta de gestión de servicios de tecnología de información (HGSTI)	:	Herramienta Integrada de Gestión de Servicios de Tecnología de Información vigente, basada en estándares internacionales de buenas prácticas, donde se registra, se gestiona todas las incidencias y peticiones de servicio informático.
3. Alerta	:	Es un aviso que indica que se requiere la intervención humana. El propósito de la alerta es asegurar que se notificará a la persona con habilidades apropiadas para tratar de evento.
4. Monitoreo:	:	Es la observación sistemática de los elementos de configuración y servicios para detectar condiciones de potencial importancia. Es altamente automatizada.
5. Evento:	:	Cualquier cambio de estado que sea significativo para la gestión de un elemento de configuración o servicio de tecnología de información que estando monitoreado han sido definidos como eventos.
6. Impacto:	:	Una medida del efecto de un incidente, problema o cambio en los procesos de negocio. El impacto está

a menudo basado en cómo serán afectados los niveles de servicio, ya sea en base a cantidad de usuarios o áreas organizacionales, valor monetario o de imagen, procesos de negocio, etc.

7. Solicitud de Cambio: : Una descripción de un cambio propuesto usado para iniciar un control de cambio. Incluye detalles del cambio que se necesita realizar, y debe registrarse en la HGSTI utilizada para la gestión de cambios.

8. Incidente : Una interrupción no planificada de un Servicio de TI o una reducción de la Calidad de un Servicio de TI. Incluye también cambios de estado que reflejen fallas en elementos de configuración pero que no aún no han afectado a un Servicio de TI.

9. Cuenta de acceso : Código alfanumérico que sirve para identificar a un colaborador y registrar las operaciones y transacciones que realiza interactuando con los sistemas operativos y/o sistemas de información.

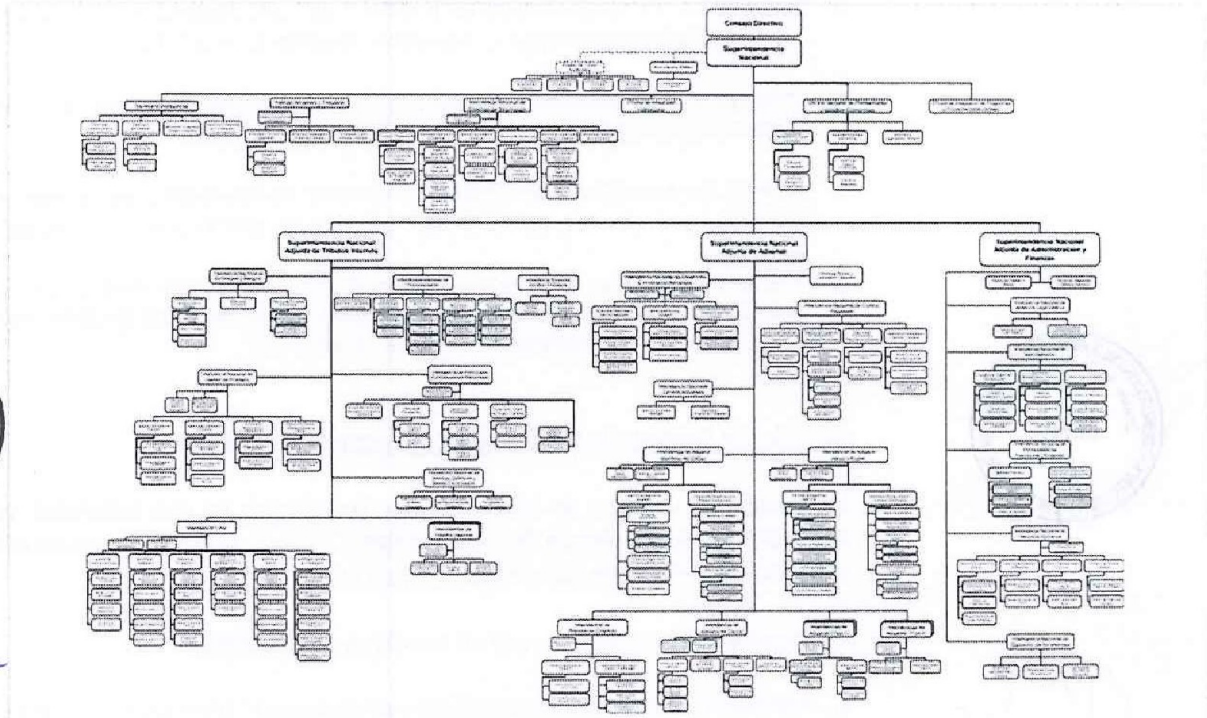
1.4 De la entidad o dependencia

La Superintendencia Nacional de Aduanas y de Administración Tributaria - SUNAT, es una entidad que pertenece al nivel de gobierno nacional y conforme a su ley orgánica, es un organismo técnico especializado, adscrito al Ministerio de Economía y Finanzas, cuenta con personería jurídica de derecho público, con patrimonio propio y goza de autonomía funcional, técnica, económica, financiera, presupuestal y administrativa que, en virtud a lo dispuesto por el Decreto Supremo N.° 061-2002-PCM, expedido al amparo de lo establecido en el numeral 13.1 del artículo 13 de la Ley N.° 27658, ha absorbido a la Superintendencia Nacional de Aduanas, asumiendo las funciones, facultades y atribuciones que por ley, correspondían a esta entidad.

Tiene entre sus funciones y atribuciones, administrar los tributos internos del Gobierno Nacional, así como los conceptos tributarios y no tributarios cuya administración o recaudación se le encargue por Ley o Convenio Interinstitucional. Asimismo, dictar normas en materia de organización y gestión interna en el ámbito de su competencia; mantener en custodia las mercancías y bienes incautados, embargados o comisados, efectuando el remate de los mismos cuando ello proceda en el ejercicio de sus funciones; controlar y fiscalizar el ingreso, permanencia, transporte o traslado y salida de los bienes controlados que puedan ser utilizados tanto en la minería ilegal como en la elaboración de drogas ilícitas.

A continuación, se muestra la estructura orgánica gráfica de la entidad:

Organigrama de la Superintendencia Nacional de Aduanas y de Administración Tributaria



Fuente: Texto Integrado del Reglamento de Organización y Funciones de la Superintendencia Nacional de Aduanas y de Administración Tributaria – SUNAT, aprobado con Resolución de Superintendencia n.°000159-2024/SUNAT, de 2 de agosto de 2024



Fuente: Texto Integrado del Reglamento de Organización y Funciones de la Superintendencia Nacional de Aduanas y de Administración Tributaria – SUNAT, aprobado con Resolución de Superintendencia n.°000159-2024/SUNAT, de 2 de agosto de 2024

Las subunidades orgánicas auditadas se detallan a continuación:

División de Soporte y Operaciones de la Infraestructura Tecnológica (DSOIT)

La División de Soporte y Operación de la Infraestructura Tecnológica es una subunidad orgánica dependiente de la Gerencia de Operaciones y Soporte a Usuarios, encargada de la operación, monitoreo y soporte de primer nivel de la infraestructura tecnológica.

Tiene entre sus funciones, las siguientes:

a) Gestionar los centros de cómputo de la SUNAT, así como administrar, operar y dar soporte a la infraestructura tecnológica de los centros de cómputo de la SUNAT.
[...]
c) Monitorear permanentemente la operatividad y la disponibilidad de los servicios informáticos puestos en producción.
[...]
f) Elaborar las especificaciones técnicas o términos de referencia para la adquisición de accesorios y/o servicios que permitan asegurar la operatividad de la infraestructura tecnológica.
g) Realizar o participar en la elaboración del modelo de la solución informática que atienda las necesidades de las unidades de organización de la SUNAT; así como, gestionar y/o ejecutar las actividades que lo implementan, cuando corresponda.
[...]

<u>División de Gestión de Infraestructura Tecnológica (DGIT)</u>

La División de Gestión de Infraestructura Tecnológica es una subunidad orgánica dependiente de la Gerencia de Operaciones y Soporte a Usuarios, encargada de la administración y soporte de la infraestructura tecnológica.

Tiene entre sus funciones las que se detallan a continuación:

a) Administrar la infraestructura tecnológica y de la seguridad informática, de la SUNAT.
[...]
d) Brindar el soporte para el correcto funcionamiento de la infraestructura tecnológica implementada por la Intendencia Nacional de Sistemas de Información.
e) Coordinar y supervisar las actividades de mantenimiento preventivo y correctivo de la infraestructura tecnológica bajo administración de la Intendencia Nacional de Sistemas de Información.
f) Elaborar las especificaciones técnicas o términos de referencia para la adquisición de los componentes y accesorios relacionados a la infraestructura tecnológica y servicios en el ámbito de su competencia, así como realizar la gestión técnica de los contratos adjudicados en el ámbito de su competencia.
g) Realizar centralizadamente la gestión técnica de los contratos adjudicados relacionados a la infraestructura tecnológica de la SUNAT
[...]

<u>División de Atención a Usuarios (DAU)</u>

La División de Atención a Usuarios es una subunidad orgánica dependiente de la Gerencia de Operaciones y Soporte a Usuarios, encargada de brindar el soporte informático requerido por los usuarios de la SUNAT.
Tiene entre sus funciones las que se detallan a continuación:

a) Atender y gestionar los reportes de incidentes en los servicios informáticos, dando solución en el ámbito de su competencia, incluyendo la atención de incidentes relacionados a telefonía móvil.
[...]
c) Brindar soporte informático a los usuarios de los servicios implementados por la Intendencia Nacional de Sistemas de Información.
[...]

1.5 Notificación de las desviaciones de cumplimiento

En aplicación de las Normas Generales de Control Gubernamental, aprobadas con Resolución de Contraloría N.° 295-2021-CG publicada el 24 de diciembre de 2021 y modificatorias, la Directiva N.° 001-2022-CG/NORM "Auditoría de Cumplimiento" y el Manual de Auditoría de Cumplimiento aprobados mediante Resolución de Contraloría N.° 001-2022-CG de 7 de enero de 2022 y modificatorias, se cumplió con el procedimiento de notificación de las desviaciones de cumplimiento a la persona comprendida en los hechos observados a fin que formule sus comentarios o aclaraciones.

1.6 Aspectos relevantes

LIMITACIONES POR PARTE DE LA INTENDENCIA NACIONAL DE SISTEMAS DE INFORMACIÓN PARA ACCEDER A LAS HERRAMIENTAS INFORMÁTICAS EN LÍNEA, LAS CUALES ESTÁN VINCULADAS AL MONITOREO DE LA PLATAFORMA TECNOLÓGICA DE LA SUNAT Y A LA GESTIÓN DE LOS INCIDENTES INFORMÁTICOS OCURRIDOS EN ELLA.

Mediante Memorándum N.° 0002-2025-OCI-SUNAT/1C0000-AC006, de 1 de setiembre de 2025, y con el propósito de cumplir los objetivos programados para la auditoría de cumplimiento "Gestión de Incidencias ante Fallas Técnicas en los Sistemas Informáticos de la SUNAT para el Cumplimiento de las Obligaciones Tributarias y Aduaneras", la Comisión Auditora solicitó a la Intendencia Nacional de Sistemas de Información el acceso, en modo de consulta y con autorización para la emisión de reportes, de las herramientas informáticas que se detallan a continuación:

- Herramienta de monitoreo, PRTG.
- Herramienta de Gestión y análisis de registros (logs), VRLI/VROP.
- Herramienta de Gestión de Servicios de Tecnología de Información, ITOP.
- Registro de Bitácora, donde se registra los incidentes relacionados a los servicios e infraestructura implementados en los Centros de Procesamiento de Datos de la SUNAT.
- Reportes de los registros de Quejas, Reclamos o Sugerencias.

En la reunión sostenida entre la Comisión Auditora y representantes de la INSI, el Sr. Johnny Valdez, Gerente de Operaciones y Servicios a Usuarios; el Sr. David Salinas, jefe de la División de Soporte y Operación de la Infraestructura Tecnológica; y el Sr. Omar Gonzales, Gerente de Seguridad de la Información, comunicaron diversas restricciones para atender la solicitud de acceso en línea.

Se informó que los Sistemas de la SUNAT solo permiten el ingreso de Usuarios que figuren en el padrón institucional y estén registrados en el Directorio Activo, condición que imposibilita otorgar accesos a personal externo, como el caso del personal de la Contraloría General de República que se encuentra asignado al OCI de la SUNAT. Asimismo, señalaron que las herramientas solicitadas contienen información reservada sobre la infraestructura y los servicios informáticos, cuya exposición podría representar un riesgo de seguridad ante posibles ciberataques.

Al respecto, en el numeral 5.1.3. Consideraciones para el Requerimiento de accesos,

del Procedimiento de Accesos a los Sistemas Informáticos (Versión 4[1]), aprobada con Resolución de Intendencia N.° 006-2023/SUNAT/1U0000 de 9 de marzo de 2023, señala que podrán solicitar acceso a los sistemas de información en producción *"El personal de entidades externas que por contrato y/o convenio con SUNAT requieran acceso a algún sistema de información en producción, la UUOO a la que estén designados, debe gestionar la respectiva petición de acceso, bajo lo considerado en el Lineamiento Temporal de Acceso Remoto a la Red Informática de SUNAT – Usuario Externo, que se encuentre vigente."*

Sin embargo, en el Procedimiento de Acceso a los Sistemas Informáticos (Versión 5[2]), aprobada con Resolución de Intendencia N.° 000009-2024-SUNAT/1U0000 de 14 de octubre de 2023 se excluye la referencia vinculada al acceso para entidades externas indicada en el literal a) del numeral 5.1.3 mencionado en el párrafo anterior. Esta situación limita el acceso a la información establecido en el literal m) del artículo 9 de la Ley N.°27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, que faculta a los órganos de control a requerir, conocer y examinar toda la información y documentación relacionada con las operaciones de las entidades bajo el ámbito del control gubernamental.

Considerando que dichas herramientas informáticas resultan esenciales para el monitoreo y la gestión de información relacionada con la plataforma tecnológica de la SUNAT, su no habilitación al personal de la Contraloría General de la República, asignado al OCI de la SUNAT constituye una limitación para el adecuado desarrollo de las labores de control.

Por lo tanto, la restricción señalada por la Intendencia Nacional de Sistemas de Información para otorgar acceso en línea a las herramientas informáticas solicitadas constituyó una limitación significativa para el desarrollo del presente servicio de control.

Por otra parte, la exclusión, en la Versión 5 del Procedimiento de Acceso a los Sistemas Informáticos, de la disposición que permitía el acceso a entidades externas, restringió la labor de la Comisión Auditora, respecto a contar con información en línea y corroborable del monitoreo de la plataforma tecnológica y la gestión de incidentes informáticos; afectando las labores de control gubernamental.

2. DEFICIENCIAS DE CONTROL INTERNO

Cabe señalar, que las deficiencias reveladas no constituyen necesariamente todos los aspectos de control interno que podrían ser situaciones reportables, debido a que estas fueron identificadas como resultado de la evaluación de las operaciones, procesos, actividades y sistemas relacionados con los objetivos de la auditoría de cumplimiento, y no con el propósito de evaluar en su conjunto la estructura de control interno de la entidad; por lo que, durante la ejecución de la auditoría de cumplimiento, la Comisión Auditora ha identificado las deficiencias de control interno que se detallan a continuación:

1 Vigente desde el 9 de setiembre de 2023 al 14 de octubre de 2024
2 El cual se encuentra vigente a la fecha (noviembre 2025) a partir del mes de octubre de 2024.

2.1 NORMATIVA DESACTUALIZADA Y CONTRADICTORIA QUE REGULA LA GESTIÓN DE PRÓRROGAS DE VENCIMIENTOS TRIBUTARIOS ANTE INCIDENTES INFORMÁTICOS MASIVOS, GENERAN QUEJAS DE LOS CONTRIBUYENTES, AFECTANDO EL CUMPLIMIENTO DE LAS OBLIGACIONES TRIBUTARIAS Y ADUANERAS, EXPONIENDO A LA SUNAT A UN ALTO RIESGO OPERATIVO

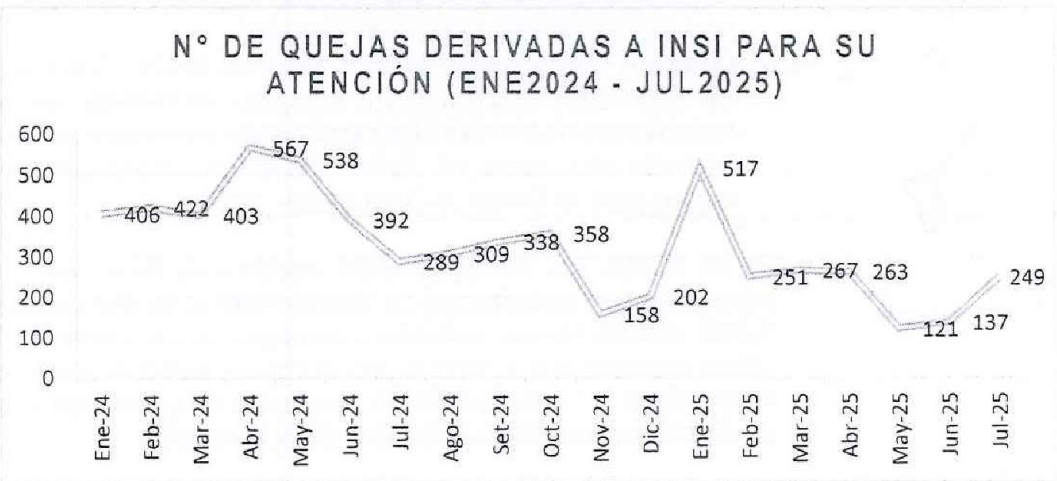
Mediante Memorándum N.° 0003-2025-OCI-SUNAT/1C0000-AC006 de 3 de setiembre de 2025, la Comisión Auditora solicitó a la Gerencia de la Defensoría del Contribuyente y Usuario Aduanero (GDCUA) remitir los documentos generados en el ámbito de su competencia, relacionados con las caídas de los sistemas informáticos que hayan afectado de manera masiva a los contribuyentes o usuarios aduaneros, así como las quejas mensuales en las que las dependencias de la INSI figuren como área responsable de su atención, correspondientes al periodo del 01/01/2024 al 31/07/2025.

En respuesta, alcanzaron entre otros documentos, el Memorándum Circular N.° 000040-2025-SUNAT/1M9000 de 25 de agosto de 2025, en el cual se precisan cuatro (4) incidentes informáticos de carácter masivo relacionados con el rubro de declaraciones y pagos, ocurridos en las siguientes fechas:

- 27/03/2024 – Declaración anual Renta 2023 (dígitos 0 y 1).
- 31/05/2024 – Declaración anual Renta 2023 (dígito 4).
- 23/01/2025 – Declaración mensual período 12-2024 (dígitos 8 y 9).
- 25 al 27/03/2025 – Declaración anual Renta 2024 (dígitos 0 y 1).

Igualmente, remitió el reporte de quejas ingresadas y derivadas a la INSI, el cual muestra la evolución mensual de las quejas registradas durante el periodo enero 2024 – julio 2025, evidenciándose incrementos significativos en aquellos meses en que se produjeron incidentes informáticos masivos relacionados con declaraciones y pagos. Estos picos coinciden con los eventos del 27/03/2024, 31/05/2024 y 23/01/2025, lo que confirma el impacto operativo y la correspondencia entre las quejas de los contribuyentes hacia las afectaciones de los sistemas relacionadas a las obligaciones tributarias. Dicho reporte se resume en la imagen siguiente:

Imagen N.°1
Número de quejas derivadas a INSI



Fuente: Reporte[3] de quejas derivadas a INSI.

[3] información alcanzada en respuesta de la Gerencia de Defensoría del Contribuyente y Usuario Aduanero a la pregunta 3 del Memorándum N.° 003-2025-OCI-SUNAT/1C0000-AC006 de 3 de setiembre de 2025.

De ahí que, en el citado Memorándum Circular se advierte que, respecto de los incidentes informáticos masivos reportados, se identificaron como principales observaciones: i) la falta de publicación oportuna de comunicados en el portal institucional, ii) la demora en la identificación del universo de contribuyentes afectados y iii) la ausencia de modificaciones de oficio en las fechas de vencimiento; situaciones que prolongaron la afectación, incrementando el riesgo de reclamos y quejas por parte de los contribuyentes.

Por otra parte, la División de Atención a Usuarios (DAU) indicó[4] que participa en la gestión de los comunicados relacionados con incidentes por la caída de los sistemas tributarios y/o aduaneros, toda vez que coordina la elaboración y publicación de dichos avisos en el portal institucional. Esto incluye los comunicados vinculados a modificaciones o prórrogas del cronograma de vencimientos.

En relación a los documentos normativos institucionales que regulan la participación de la División de Atención a Usuarios (DAU) en la gestión de comunicados en el portal institucional de la SUNAT, ante incidentes que afecten la plataforma tecnológica, dicha División señaló[5] lo siguiente: *"Los documentos institucionales que se cuenta sobre la participación de la DAU en la gestión de comunicados son antiguos y no están actualizados con el ROF actual de SUNAT"*.

De los documentos normativos alcanzados por la División de Atención al Usuario (DAU)[6] y la División de Soporte y Operaciones de la Infraestructura Tecnológica (DSOIT)[7], se identificó que están vigentes, los que se detallan a continuación:

- **Directiva N.° 007-2000/SUNAT** de 18 de julio de 2000, en la cual se "E*stablecen como instrucción que no son sancionables las infracciones tributarias cuya comisión se hubiera debido a hechos imputables a la administración tributaria"*
- **Circular N.° 032-2001** de 15 de octubre de 2001, El cual tiene como materia la *"Prórroga de la fecha de vencimiento de las obligaciones tributarias, cuando se presenten situaciones de caso fortuito o fuerza mayor."*
- **Circular N.° 17-2011** de 14 de julio de 2011. El cual tiene como materia la *"Modificación de la fecha de vencimiento de obligaciones tributarias mensuales y anuales."*
- **Circular N.° 004-2014-200000** de 19 de marzo de 2014. El cual tiene como materia la *"Modificación de fecha de vencimiento de obligaciones administradas por la SUNAT por problemas no atribuibles al contribuyente"*
- **Circular N.° 005 -2016-600000** de 26 de febrero de 2016. El cual tiene como materia los *"Mecanismos de alerta para la publicación de mensajes cuando se presenten incidentes que no permitan a los contribuyentes o usuarios el uso de los aplicativos y productos informáticos en SUNAT Virtual por causas internas o externas, y conformación del Comité de Contingencia – SOL."*

En tal sentido, las normativas antes mencionadas tienen en común establecer lineamientos para garantizar que los contribuyentes no se vean perjudicados cuando la SUNAT enfrenta hechos, incidentes o contingencias que afectan el cumplimiento de obligaciones tributarias; en razón de ello, se procedió a efectuar el análisis de lo dispuesto en el Circular N.° 005-2016-600000, puesto que este, constituye el documento más actualizado correspondiente respecto al año de su emisión.

4 En respuesta al cuestionario Suscrito por el jefe de la DAU, Víctor Mendieta Manco.
5 En respuesta a la pregunta 4 a la DAU, del Memorándum N..° 0005-2025-OCI-SUNAT/1C0000-AC006 de 24 de setiembre de 2025.
6 En respuesta a la pregunta 4 a la DAU, del Memorándum N.° 0005-2025-OCI-SUNAT/1C0000-AC006 de 24 de setiembre de 2025.
7 En respuesta a la pregunta 11 a la DSOIT, del Memorándum N.° 0005-2025-OCI-SUNAT/1C0000-AC006 de 24 de setiembre de 2025.

De modo que, el citado Circular establece que, ante incidentes que imposibiliten el uso de los aplicativos y productos informáticos en la página web de la SUNAT, debe activarse un protocolo de comunicación que contemple la difusión de mensajes emergentes en cada etapa del proceso. Esto incluye informar oportunamente la ocurrencia del incidente, así como comunicar el avance de las acciones correctivas cuando la solución exceda las dos (2) horas.

Asimismo, una vez restablecido el servicio, debe confirmarse la superación del problema y en los casos en que los incidentes coincidan con fechas de vencimiento de obligaciones tributarias, corresponde además publicar comunicados que dispongan la prórroga respectiva y expresen las disculpas institucionales por las molestias ocasionadas. Dichos mensajes emergentes deben difundirse en la página principal del portal SUNAT, en las secciones del servicio afectado, garantizando transparencia y mitigando el impacto en los contribuyentes.

Al respecto, la Comisión Auditora solicitó a la Gerencia de Orientación y Servicios[8] (GOS) de la Intendencia Nacional de Gestión de Procesos (INGP) información en el marco de la Circular N.°005-2016-600000, relacionada con la gestión de comunicados en fechas en que se hayan producido incidentes informáticos de alto impacto. En atención[9] a dicho requerimiento, la GOS remitió un cuadro en la que se identifica que hay incidentes ocurridos en el cual no se ha publicado un comunicado en el portal de la SUNAT como se observa a continuación:

Cuadro N.° 1
Incidentes que tiene comunicados en el portal

FECHA DE INCIDENTE	TIPO DE INCIDENCIA	MENSAJE EN PORTAL
27/03/2024	• APP Personas • Mis tramites y consultas en SOL	NO
31/05/2024	• Declaraciones y Pagos • SOL • CPE • Otros	SI
03/06/2024	Declaraciones y Pagos y emisión de CPE y GRE	NO
17/09/2024	Mis declaraciones y pagos / Nueva plataforma.	SI
25/09/2024	Fraccionamiento y problemas con la tarjeta de crédito/débito	NO
20/01/2025	Pago de detracciones	NO
23/01/2025	Mis declaraciones y pagos / Nueva plataforma.	SI
25/03/2025 AL 27/03/2025	Nueva Plataforma y con la presentación de la declaración del formulario 648	NO

Fuente: Respuesta al Memorándum N.° 010-2025-OCI-SUNAT/1C0000-AC006 de 9 de octubre de 2025.
Elaborado por: Comisión Auditora.

Por consiguiente, de la información alcanzada, se advierte que, si bien en algunas fechas se publicó un Comunicado en el portal, se evidencia que en ciertos casos estos fueron difundidos con retraso de hasta nueve (9) días después de ocurrido el incidente, como el incidente registrado el 17 de septiembre de 2024, el cual fue comunicado recién el 26 de setiembre del mismo año, evidenciándose dilación en la emisión del mensaje; lo que se

[8] El cual tiene entre sus funciones la de "*Conducir el seguimiento a los programas de mantenimiento preventivo de la infraestructura informática, así como las ocurrencias que pudieran afectar la operatividad de los servicios que se presten a través de los distintos canales de atención*"

[9] Al Memorándum N.° 010-2025-OCI-SUNAT/1C0000-AC006 de 9 de octubre de 2025.

muestra en la imagen siguiente:

Imagen N.° 2
Incidentes que tiene comunicados en el portal


COMUNICADO

Estimado(a) contribuyente:

Debido a los inconvenientes presentados en nuestros aplicativos:

- **Mis declaraciones y pagos / Nueva plataforma.**

Si el vencimiento para la presentación de su declaración jurada de obligaciones mensuales del periodo Agosto 2024, de acuerdo **con el último dígito de su RUC**, fue el **día 17 de setiembre de 2024**, pudo cumplir con dicha(s) obligación(es), hasta el **día 18 de setiembre de 2024**.

Pedimos disculpas por las molestias ocasionadas y agradecemos su comprensión.

Historial de comunicados

Lima, 26 de setiembre de 2024 SUNAT

Fuente: Portal Web https://www.sunat.gob.pe/mensajes/mensajes-SUNAT-2024.html

En consecuencia, se evidencia que la Gerencia de Orientación y Servicios (GOS) ha reiterado a la División de Atención al Usuario (DAU), la necesidad de comunicar oportunamente los incidentes masivos que se presenten durante el vencimiento de obligaciones tributarias; debido a que, en los meses de agosto y setiembre de 2024, ha venido ocurriendo incidentes que han generado postergaciones y estos no han sido informados de manera oportuna, lo que se muestra a continuación, en la imagen siguiente:

Imagen N.° 3
Correo de la GOS a la DAU de 23 de setiembre de 2024

De: Mendieta Manco Victor Eduardo <VMENDIET@sunat.gob.pe>
Enviado el: lunes, 23 de septiembre de 2024 17:34
Para: Salinas Rojas David <DSALINAS@sunat.gob.pe>; Alcca Soncco Marco Antonio <MALCCA@sunat.gob.pe>; Garayar Santibañez Richard Rolando <rgarayars@sunat.gob.pe>
CC: Perez Soncco Justo <jperezso@sunat.gob.pe>; Bautista Reyes Narda Geovanna <NBAUTIST@sunat.gob.pe>; Cayllahua Ninapaitan Ever Hugo <ecayllahua@sunat.gob.pe>
Asunto: RE: Incidente informático del 17 setiembre

@Salinas Rojas David @Marco Antonio Alcca Soncco @Garayar Santibañez Richard Rolando

El día de hoy, la GOS reiteró se le informe oportunamente de los incidentes masivos q se presenten durante vencimiento de obligaciones, en los dos últimos vencimientos (agosto y setiembre) se ha presentado incidentes q ha afectado al contribuyente q han ocasionado postergación de vencimiento y ellos no han sido informados oportunamente, nosotros tampoco, recién nos hemos enterado uno o dos días después, tenemos un lineamiento donde nos indican q tenemos q colocar un comunicado e informar a las áreas usuarias si el evento dura más de una hora, eso no ha sucedido en los últimos meses.

X favor, su apoyo para poder informarnos con prontitud cualquier incidente q afecte masivamente la presentación de declaraciones y pagos.

Saludos,

Fuente: Respuesta a la pregunta 2, del Memorándum N.°005-2025-OCI-SUNAT/1C0000-AC006 de 24 de setiembre de 2025.

Asimismo, la GOS precisó[10] que la SUNAT cuenta con un Comité de Contingencias conformado por representantes de la Gerencia de Orientación y Servicios (GOS) de la INGP, la Gerencia de Operaciones y Soporte a Usuarios (GOSU) de la INSI y la Gerencia de Defensoría del Contribuyente y Usuario Aduanero (GDCUA) de la Secretaria Institucional. Dicho Comité coordina la atención de incidentes mediante alertas enviadas por mensajería electrónica, correos y tickets.

Agregó que, conforme a lo dispuesto en el numeral 7.1.1 de la Circular N.° 017-2011, corresponde a la División de Atención a Usuarios (antes División de Gestión de Incidentes) publicar en el portal institucional el aviso relacionado con la modificación de fechas de vencimiento. Asimismo, la Intendencia Nacional de Sistemas de Información (INSI) debe remitir a la Superintendencia Nacional Adjunta de Tributos Internos (SNATI), un informe sobre los problemas presentados, sus causas y las acciones adoptadas, comunicando la nueva fecha de vencimiento. En ese sentido, enfatizó que el Comité de Contingencias no tiene facultad para autorizar la modificación de las fechas de vencimiento.

En relación con la publicación de los mensajes, la GOS[11] indicó que estos se difunden a través de la sección "Comunicaciones destacadas" del portal institucional www.sunat.gob.pe, espacio habilitado por la Secretaría de Gobierno y Transformación Digital de la PCM debido a las restricciones de dicha entidad para incorporar "mensajes emergentes". En ese sentido, precisó que no se publica un mensaje emergente para informar la superación del incidente.

Finalmente, la GOS indicó[12] que la gestión y publicación de comunicados sobre la modificación de fechas por incidentes informáticos se sustenta actualmente en las Circulares N.° 017-2011 y N.° 004-2014-200000, así también, que la Circular N.° 005-2016-600000 está en revisión por presentar contradicciones normativas, motivo por el cual, mediante Memorándum N.° 000123-2025-SUNAT/7B2000, solicitó a la Gerencia Normativa de Procesos evaluar la instrucción del numeral 7.3, por ser contradictorio con el numeral 7.1.2.3 de la Circular N.° 017-2011.

Asimismo, la DAU señala[13] que la Circular N.° 005-2016-600000 requiere su actualización para poder aplicarla correctamente, ya que su contenido presenta unidades orgánicas inexistentes en el ROF vigente de la SUNAT.

Por lo tanto, ante esta problemática resulta necesario contar con un procedimiento estandarizado que garantice la publicación oportuna de comunicados y la gestión inmediata de prórrogas en coordinación con las áreas técnicas responsables (INSI e INGP), evitando que los contribuyentes deban realizar gestiones adicionales para regularizar sus obligaciones.

Sobre el particular, las Normas Generales de Control Interno aprobadas mediante Resolución de Contraloría N.°320-2006-CG publicada el 3 de noviembre de 2006 y vigentes desde la misma fecha, en lo referido a las Normas Básicas para las Actividades de Control Gerencial, establecen lo siguiente:

10 En respuesta a la pregunta 1 del Memorándum N.° 010-2025-OCI-SUNAT/1C0000-AC006 de 9 de octubre de 2025.
11 En respuesta a la pregunta 7 del Memorándum N.° 010-2025-OCI-SUNAT/1C0000-AC006 de 9 de octubre de 2025.
12 En respuesta a la pregunta 11 del Memorándum N.° 010-2025-OCI-SUNAT/1C0000-AC006 de 9 de octubre de 2025.
13 En respuesta a la pregunta 5 a la DAU, del Memorándum N.° 008-2025-OCI-SUNAT/1C0000-AC006 de 7 de octubre de 2025.

"[...]
3.8. Documentación de procesos, actividades y tareas

Los procesos, actividades y tareas deben estar debidamente documentados para asegurar su adecuado desarrollo de acuerdo con los estándares establecidos, facilitar la correcta revisión de los mismos y garantizar la trazabilidad de los productos o servicios generados.

01 Los procesos, actividades y tareas que toda entidad desarrolla deben ser claramente entendidos y estar correctamente definidos de acuerdo con los estándares establecidos por el titular o funcionario designado, para así garantizar su adecuada documentación. Dicha documentación comprende también los registros generados por los controles establecidos, como consecuencia de hechos significativos que se produzcan en los procesos, actividades y tareas, debiendo considerarse como mínimo la descripción de los hechos sucedidos, el efecto o impacto, las medidas adoptadas para su corrección y los responsables en cada caso.

02 Cualquier modificación en los procesos, actividades y tareas producto de mejoras o cambios en las normativas y estándares deben reflejarse en una actualización de la documentación respectiva.

03 La documentación correspondiente a los procesos, actividades y tareas de la entidad deben estar disponibles para facilitar la revisión de los mismos.

04 La documentación de los procesos, actividades y tareas debe garantizar una adecuada transparencia en la ejecución de los mismos, así como asegurar el rastreo de las fuentes de defectos o errores en los productos o servicios generados (trazabilidad).
[...]"

De igual manera, la referida normativa, en sus normas básicas para las actividades de prevención y monitoreo, señala:

"[...]
5. NORMA GENERAL PARA LA SUPERVISIÓN
[...]

5.1 NORMAS BÁSICAS PARA LAS ACTIVIDADES DE PREVENCIÓN Y MONITOREO

5.1.1 Prevención y Monitoreo

El monitoreo de los procesos y operaciones de la entidad debe permitir conocer oportunamente si éstos se realizan de forma adecuada para el logro de sus objetivos y si en el desempeño de las funciones asignadas se adoptan las acciones de prevención, cumplimiento y corrección necesarias para garantizar la idoneidad y calidad de los mismos.

Comentarios:

01 La supervisión constituye un proceso sistemático y permanente de revisión de los procesos y operaciones que lleva a cabo la entidad, sean de gestión, operativas o de control. En su desarrollo intervienen actividades de prevención y monitoreo por cuanto, dada la naturaleza integral del control interno, resulta conveniente vigilar y evaluar sobre la marcha, es decir conforme transcurre la gestión de la entidad, para la adopción de las acciones preventivas o correctivas que oportunamente correspondan.

02 La prevención implica desarrollar y mantener una actitud permanente de cautela e interés por anticipar, contrarrestar, mitigar y evitar errores, deficiencias, desviaciones y demás situaciones adversas para la entidad. Se fundamenta sobre la base de la observación y análisis de sus procesos y operaciones, efectuados de manera diligente, oportuna y comprometida con la buena marcha institucional. En tal sentido, está estrechamente relacionada y opera como resultado de las actividades de monitoreo."

[...]"

La situación expuesta, genera el riesgo que ante la ocurrencia de incidentes informáticos masivos, no se cuente con normativa actualizada que permita gestionar de manera oportuna información confiable a los contribuyentes respecto a lo sucedido, a efectos de reducir el incremento en las quejas y evitar la afectación del cumplimiento de obligaciones tributarias y aduaneras.

Los hechos descritos, se habrían originado debido a que la Intendencia Nacional de Sistemas de Información no gestionó ante las instancias pertinentes como propuesta de mejora la elaboración de un procedimiento estandarizado y actualizado que regule la gestión de comunicados y la emisión de prórrogas ante incidentes informáticos masivos, no atribuibles al contribuyente.

2.2 FALTA DE PROCEDIMIENTOS Y/O LINEAMIENTOS QUE REGULEN EL USO DE LA CUENTA ADMINISTRATIVA ROOT EN LOS SERVIDORES WEBLOGIC HA GENERADO UN USO INAPROPIADO Y AUSENCIA DE TRAZABILIDAD SOBRE LAS ACCIONES EJECUTADAS, SITUACIÓN QUE COMPROMETE Y PONE EN RIESGO LA INTEGRIDAD, DISPONIBILIDAD Y SEGURIDAD DE LOS SERVICIOS CRÍTICOS ALOJADOS EN DICHOS SERVIDORES.

El 3 de junio de 2024, se produjo un incidente en una fecha crítica para la declaración de las obligaciones tributarias de los contribuyentes, lo que agravó significativamente su impacto[14] operativo e institucional y se registró en la bitácora de incidentes de la División de Gestión de Infraestructura Tecnológica (DSOIT), con ID 13579, teniendo como causa raiz la eliminación de archivos de configuración.

En ese sentido, mediante Informe Técnico N.°000450-2024-SUNAT/1U5200[15], elaborado por la DGIT señala que se afectaron los componentes, que se detallan a continuación:

- Falla en la autenticación de Plataforma de "Declaración y Pago" y "Trámite y Consulta"
- Problemas en la emisión de Comprobantes de Pago y Recibos por Honorarios.

Según el citado Informe, la causa raíz se debió a la falta de archivos de configuración y plantillas, afectando el normal flujo de las operaciones atendidas desde el Centro de Datos de San Isidro, como se detalla a continuación:

- Falta de Archivo menu-sol.properties, en fileserver S00PLXWFST009:/data0.
- Falta de Archivos templates en fileserver S00PLXWFST009:/data0.

Es así que, de acuerdo con el Informe N.° 000036-2024-SUNAT/1U6000[16], la Gerencia de Seguridad de la Información identificó que, en el horario en que se originó el incidente, todas las conexiones existentes al servidor S00PLXWFST009 correspondían al usuario "ROOT".

Asimismo, señaló que "***El personal de la DSOIT no debe utilizar la cuenta 'ROOT'*** *para sus actividades inherentes a sus funciones, ya que no es posible mantener un rastro del responsable del uso ni de las acciones efectuadas con dicha cuenta*". (énfasis y

[14] De acuerdo con el Oficio N.° 083-2024-JDCCPP/CD de 28 de junio de 2024, remitido por la Junta de Decanos de Colegios de Contadores Públicos del Perú.
[15] De 16 de agosto de 2024 y elaborado y suscrito por el jefe de la DGIT, Carlos Manuel Posadas Vallejos.
[16] De 20 de junio de 2024.

subrayado es agregado)

Al respecto, la Comisión Auditora, mediante un Cuestionario dirigido a la DSOIT, consultó: (i) ¿Para qué fines se utiliza la cuenta de acceso "ROOT"? y (ii) ¿Quiénes son los responsables de su uso?, en respuesta[17], la DSOIT señaló que la cuenta "ROOT" es una cuenta administrativa que posee todos los privilegios para la gestión de un recurso informático. Asimismo, indicó que, dentro del equipo de la DSOIT, los Responsables de utilizar dicha cuenta pertenecen al Equipo de monitoreo y soporte de primer nivel, para la realización de labores de soporte específicas.

En ese contexto, el 17 de setiembre de 2025, mediante Acta de Reunión N.° 01-2025-OCI/AC-006[18], se consultó al Supervisor[19] de la DSOIT si, en su calidad de jefe de División encargado durante las fechas en que ocurrió el incidente, logró identificar al Personal Responsable de la eliminación de los archivos en el servidor S00PLXWFST009. **En respuesta, señaló que no fue posible realizar dicha identificación**, debido a que la operación se ejecutó utilizando la cuenta general "ROOT", lo que impidió determinar el autor de la acción. (énfasis y subrayado es agregado)

Por lo que, se consultó[20] a la DSOIT si existía algún documento de autorización emitido por la Oficina de Seguridad Informática (OSI) para el uso de la cuenta administrativa ROOT. Al respecto, señaló que no se ha identificado ningún documento que respalde dicha autorización.

De igual manera, se consultó[21] si existía algún procedimiento, lineamiento, indicación o memorándum relacionado con el uso de la cuenta "ROOT". En respuesta, la DSOIT indicó que cuentan con el documento denominado "*Instructivo para la solicitud, entrega y uso de cuentas administrativas en base de datos*", de 30 de setiembre de 2016. Sin embargo, según su Alcance está dirigido al Personal del área encargada de la operación, soporte y administración de la plataforma de Base de Datos Informix y Oracle en servidores de producción con el comando utilitario SUDO[22].

Al respecto al DSOIT manifiesta[23] que el servidor "S00PLXWFST009" es un servidor repositorio de archivos de registro (log) de las aplicaciones desplegadas en servidores WEBLOGIC, así como archivos de configuración y almacenamiento de información temporal de las aplicaciones web, por lo que precisó[24] que el instructivo mencionado en el párrafo anterior no aplica a servidores WEB.

En ese contexto, la Gerencia de Operaciones y Soporte a Usuarios (GOSU), mediante Memorándum N.°000142-2025-1U5000[25] del 26 de agosto de 2025 solicitó a la Gerencia de Gestión de Procesos y Proyectos de Sistemas de la INSI que, en relación con el uso de cuentas administrativas, se gestione la actualización del procedimiento IOI.UCAB.01: "*Instructivo para la solicitud, entrega y uso de cuentas administrativas en base de datos*".

---

17 Pregunta 22 del cuestionario realizado a la DSOIT, suscrito por el supervisor Marco Antonio Alcca Soncco el 29 de agosto de 2025.
18 Suscrito el 19 de setiembre de 2025.
19 El Sr. Marco Antonio Alcca Soncco, el cual estuvo encargado como jefe de la DSOIT en las fechas ocurrido el incidente del 3 de junio de 2024.
20 En el número 17 del acta de reunión N.° 01-2025-OCI/AC-006, de fecha 17 de setiembre de 2025.
21 En la pregunta 23 del cuestionario realizado a la DSOIT, suscrito por el supervisor Marco Antonio Alcca Soncco el 29 de agosto de 2025
22 SUDO: Permite ejecutar comandos con privilegios de administrador sin tener que iniciar sesión con la cuenta ROOT.
23 En respuesta al requerimiento complementario a la DSOIT (Pregunta 3), realizado por la comisión auditora a través de correo electrónico de 21 de octubre de 2025.
24 En respuesta a la pregunta 10 a la DSOIT del Memorándum N.° 005-2025-OCI-SUNAT/1C0000-AC006 de 24 de setiembre de 2025.
25 Remitida a la Comisión Auditora en respuesta a la pregunta 10 a la DSOIT del Memorándum N.° 005-2025-OCI-SUNAT/1C0000-AC006.

Es así que, dicha actualización debería ampliar el Alcance a todos los componentes de la infraestructura tecnológica en los que se identifique y resulte factible el uso de cuentas administrativas, así como incorporar las nuevas casuísticas vigentes a la fecha.
Al respecto, se solicitó[26] a la DSOIT remitir la relación de servidores de producción correspondientes a los servidores WEBLOGIC. En respuesta[27] remitió un reporte en el que se identificaron 594 servidores.

En consecuencia, el incidente ocurrido el 3 de junio de 2024 evidenció deficiencias críticas en la gestión de accesos administrativos dentro de los servidores WEBLOGIC, particularmente en el uso de la cuenta "ROOT", ya que la eliminación de archivos de configuración, el cual fue efectuada sin trazabilidad alguna debido al empleo de una cuenta con altos privilegios y sin controles, generó inoperatividad en los servicios esenciales para los contribuyentes en una fecha de alta demanda operativa.

Sobre el particular, las Normas Generales de Control Interno aprobadas mediante Resolución de Contraloría N.°320-2006-CG publicada el 3 de noviembre de 2006 y vigentes desde la misma fecha, en lo referido a las Normas Básicas para las Actividades de Control Gerencial, establecen lo siguiente:

"[...]
3.8. Documentación de procesos, actividades y tareas

Los procesos, actividades y tareas deben estar debidamente documentados para asegurar su adecuado desarrollo de acuerdo con los estándares establecidos, facilitar la correcta revisión de los mismos y garantizar la trazabilidad de los productos o servicios generados.

01 Los procesos, actividades y tareas que toda entidad desarrolla deben ser claramente entendidos y estar correctamente definidos de acuerdo con los estándares establecidos por el titular o funcionario designado, para así garantizar su adecuada documentación. Dicha documentación comprende también los registros generados por los controles establecidos, como consecuencia de hechos significativos que se produzcan en los procesos, actividades y tareas, debiendo considerarse como mínimo la descripción de los hechos sucedidos, el efecto o impacto, las medidas adoptadas para su corrección y los responsables en cada caso.
02 Cualquier modificación en los procesos, actividades y tareas producto de mejoras o cambios en las normativas y estándares deben reflejarse en una actualización de la documentación respectiva.
03 La documentación correspondiente a los procesos, actividades y tareas de la entidad deben estar disponibles para facilitar la revisión de los mismos.
04 La documentación de los procesos, actividades y tareas debe garantizar una adecuada transparencia en la ejecución de los mismos, así como asegurar el rastreo de las fuentes de defectos o errores en los productos o servicios generados (trazabilidad).
[...]"

De igual manera, la referida normativa, en sus normas básicas para las actividades de prevención y monitoreo, señala:

"[...]
5. NORMA GENERAL PARA LA SUPERVISIÓN
[...]
5.1 NORMAS BÁSICAS PARA LAS ACTIVIDADES DE PREVENCIÓN Y MONITOREO

[26] En la pregunta 4 (requerimiento complementario a la DSOIT), realizado por la Comisión Auditora a través de correo electrónico de 21 de octubre de 2025.
[27] A través de correo electrónico de 28 de octubre de 2025, por parte del jede de la DSOIT, David Salinas Rojas.

5.1.1 Prevención y Monitoreo

El monitoreo de los procesos y operaciones de la entidad debe permitir conocer oportunamente si éstos se realizan de forma adecuada para el logro de sus objetivos y si en el desempeño de las funciones asignadas se adoptan las acciones de prevención, cumplimiento y corrección necesarias para garantizar la idoneidad y calidad de los mismos.

Comentarios:

01 La supervisión constituye un proceso sistemático y permanente de revisión de los procesos y operaciones que lleva a cabo la entidad, sean de gestión, operativas o de control. En su desarrollo intervienen actividades de prevención y monitoreo por cuanto, dada la naturaleza integral del control interno, resulta conveniente vigilar y evaluar sobre la marcha, es decir conforme transcurre la gestión de la entidad, para la adopción de las acciones preventivas o correctivas que oportunamente correspondan.

02 La prevención implica desarrollar y mantener una actitud permanente de cautela e interés por anticipar, contrarrestar, mitigar y evitar errores, deficiencias, desviaciones y demás situaciones adversas para la entidad. Se fundamenta sobre la base de la observación y análisis de sus procesos y operaciones, efectuados de manera diligente, oportuna y comprometida con la buena marcha institucional. En tal sentido, está estrechamente relacionada y opera como resultado de las actividades de monitoreo."

[...]"

La situación expuesta, genera el riesgo de continuar comprometiendo la integridad, disponibilidad y seguridad de los servicios críticos alojados en los servidores, al no contar con un procedimiento y/o lineamiento que regule el acceso mediante la cuenta administrativa ROOT a los servidores WebLogic.

La situación expuesta se habría originado por la falta de seguimiento y supervisión de la Gerencia de Operaciones y Soporte a Usuarios orientados a identificar los vacíos normativos que permitan una mejora continua en la gestión de accesos a los servidores que alojan servicios críticos y que soportan la plataforma vinculada a las obligaciones tributarias de los contribuyentes.

2.3 FALTA DE IMPLEMENTACIÓN DE CONFIGUARCIÓN DE PRIVILEGIOS PARA EL COMANDO UTILITARIO SUDO, LIMITA LA TRAZABILIDAD DE LAS ACCIONES REALIZADAS POR CADA USUARIO, GENERANDO EL RIESGO EN LA OPERATIVIDAD DE LOS SERVICIOS CRÍTICOS VINCULADOS A LAS OBLIGACIONES TRIBUTARIAS DE LOS CONTRIBUYENTES ALOJADOS EN LOS SERVIDORES.

De la revisión a la información alcanzada por la División de Soporte y Operación de Infraestructura Tecnológica (DSOIT) precisó[28] que aún se recurre al uso de la cuenta "ROOT" para ejecutar acciones como la depuración de archivos, debido a que las cuentas individualizadas no cuentan con los privilegios necesarios. Asimismo, indicó que se encuentra en proceso de implementación el uso del comando utilitario SUDO, con el fin de asegurar la identificación y trazabilidad de las operaciones realizadas por cada usuario; informando[29] que dicho pedido fue gestionado mediante el ticket de requerimiento R-1280185.

[28] Mediante Acta de Reunión N.° 01-2025-OCI/AC-006 de 17 de setiembre de 2025.
[29] En respuesta a la pregunta 6 a la DSOIT del Memorándum N.° 008-2025-OCI-SUNAT/1C0000-AC006 de 7 de octubre de 2025.

Por otra parte, la DSOIT manifiesta[30] que el servidor "S00PLXWFST009" es un servidor de repositorio de archivos de registro (log) de las aplicaciones desplegadas en servidores WEBLOGIC, así como archivos de configuración y almacenamiento de información temporal de las aplicaciones web.

Por consiguiente, la Comisión Auditora solicitó[31] a la DSOIT remitir la relación de servidores de producción correspondientes a los servidores WEBLOGIC, precisando si cuentan o no con el comando utilitario SUDO operativo; en atención a lo solicitado[32] la citada División remitió un Reporte en el que se identificaron 594 servidores, **de los cuales únicamente 2 cuentan con el comando utilitario SUDO configurado**, como se muestra a continuación:



Imagen N.°4
Servidores de Producción con Utilitario SUDO implementado

hostname	Tipo de componente	SUDO operativo y en uso	Fecha de implementación del SUDO	Observación
w70msunat	consola de despliegue	no	no implementado	Sin observación
S01PLXWWLA002	consola de despliegue	no	no implementado	Sin observación
S01PLXWWLA003	consola de despliegue	no	no implementado	Sin observación
S01PLXWWLA007	consola de despliegue	no	no implementado	Sin observación
S01PLXWWLA008	consola de despliegue	no	no implementado	Sin observación
w70ssunat	consola de despliegue	no	no implementado	Sin observación
S00PLXWWLA001	consola de despliegue	no	no implementado	Sin observación
S00PLXWWLA002	consola de despliegue	no	no implementado	Sin observación
S00PLXWWLA003	consola de despliegue	no	no implementado	Sin observación
S00PLXWWLA008	consola de despliegue	no	no implementado	Sin observación
S00PLXWWLA007	consola de despliegue	no	no implementado	Sin observación
w80ssunat	Servidor de archivos	si	Abril 2012	Sin observación
w80msunat	Servidor de archivos	no	no implementado	Sin observación
S01PLXWFST009	Servidor de archivos	no	no implementado	Sin observación
S00PLXWFST009	Servidor de archivos	si	Agosto 2025	Sin observación
S00PLXWFST004	Servidor de archivos	no	no implementado	Sin observación
S00PLXWFST003	Servidor de archivos	no	no implementado	Sin observación
S01PLXWFST041	Servidor de archivos	no	no implementado	Sin observación
S01PLXWFST042	Servidor de archivos	no	no implementado	Sin observación
S01PLXWFST019	Servidor de archivos	no	no implementado	Sin observación
S01PLXWFST020	Servidor de archivos	no	no implementado	Sin observación
S00PLXWFST019	Servidor de archivos	no	no implementado	Sin observación
S00PLXWFST020	Servidor de archivos	no	no implementado	Sin observación
w95ssunat	Servidor de aplicaciones	no	no implementado	Sin observación
w96ssunat	Servidor de aplicaciones	no	no implementado	Sin observación

Fuente: Información alcanzada por la DSOIT en respuesta al requerimiento complementario (Pregunta 4), realizado por la comisión auditora a través de correo electrónico de 21 de octubre de 2025

Como se aprecia en la imagen anterior, existen únicamente dos (2) servidores de producción en los que se ha implementado el comando utilitario SUDO: el primero en el mes de abril de 2012 y el segundo en el mes de agosto de 2025. Este último corresponde

30 En respuesta al requerimiento complementario a la DSOIT (Pregunta 3), realizado por la comisión auditora a través de correo electrónico de 21 de octubre de 2025.
31 En la pregunta 4 (requerimiento complementario a la DSOIT), realizado por la comisión auditora a través de correo electrónico de 21 de octubre de 2025.
32 A través de correo electrónico de 28 de octubre de 2025, por parte del jede de la DSOIT, David Salinas Rojas.

al servidor S00PLXWFST009, en el cual ocurrió el incidente del 3 junio de 2024, que devino en el borrado de archivos de configuración. En consecuencia, se advierte que transcurrieron aproximadamente catorce (14) meses desde la ocurrencia del incidente hasta la implementación de dicho utilitario en dicho servidor, es decir, solo en dos (2) servidores de producción

Ahora bien, del Reporte se identificó tres (3) tipos de componentes en los servidores de producción, los cuales se muestran a continuación:

Cuadro N.°2
Cantidad Servidores de producción con implementación del Utilitario SUDO

Tipo de componente	Cantidad total de servidores	Utilitario SUDO implementado	Utilitario SUDO NO implementado
Consola de despliegue	11	0	11
Servidor de archivos	12	2	10
Servidor de aplicaciones	571	0	571
Total	**594**	**2**	**592**

Fuente: Información alcanzada por la DSOIT en respuesta al requerimiento complementario (Pregunta 4), realizado por la comisión auditora a través de correo electrónico de 21 de octubre de 2025

Como se aprecia en el cuadro anterior se puede identificar que en 592 servidores, no se encuentra implementado el comando utilitario SUDO y que solo 2 cuentan con dicho utilitario.

En consecuencia, la falta de implementación del comando utilitario SUDO, cuya funcionalidad permite acceder a archivos y operaciones restringidas; y, el uso recurrente de la cuenta ROOT en los servidores WEBLOGIC limitan la trazabilidad de las acciones realizadas por cada Usuario, —imposibilitando identificar responsables— lo que originó que el 3 de junio de 2024, se eliminen los archivos de configuración. Este hecho generó fallas en la autenticación de las plataformas "Declaración y Pago" y "Trámite y Consulta", así como problemas en la emisión de comprobantes, afectando directamente los servicios vinculados a las obligaciones tributarias de los contribuyentes.

No obstante, que la asignación de credenciales personalizadas se concretó recién en diciembre de 2024 y que el primer acceso individualizado se registró ocho (8) meses después del incidente, manteniéndose el uso de la cuenta ROOT. Además, solo dos (2) de los 594 servidores de producción cuentan con el comando utilitario SUDO implementado, lo que prolonga el riesgo operativo, compromete la integridad y disponibilidad de los servicios y expone a la institución a la repetición de fallas similares en el resto de la infraestructura.

Si bien la entidad ha iniciado acciones correctivas en el servidor afectado, persiste el riesgo de que incidentes de naturaleza similar se produzcan en los demás servidores de producción que alojan servicios críticos vinculados a las obligaciones tributarias, mientras no se implemente el comando utilitario SUDO en toda la infraestructura. Esta condición mantiene expuesta a la institución a eventos que podrían comprometer nuevamente la integridad, disponibilidad y seguridad de sus servicios institucionales.

Sobre el particular, el Manual de Políticas del Sistema de Gestión de Seguridad de la Información SGSI-MA-03I, aprobado con Resolución de Superintendencia N.°000148-2023/SUNAT de 18 de julio de 2023, establece lo siguiente:

"[...]
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ISO 27001-A.6)

6.1. ORGANIZACIÓN INTERNA [ISO 27001 A.6.1]
[...]

6.1.2. Segregación de funciones [ISO 27001 A.6.1.2]

a. *Toda área de la SUNAT debe solicitar los accesos para su personal alineado a sus labores y funciones documentadas o necesidad operativa, evitando cualquier conflicto para una correcta segregación de funciones.*
b. *La responsabilidad de los propietarios de los activos de información debe ser autorizar los accesos a la información teniendo en consideración:*
   - *Una adecuada definición y segregación de funciones, de acuerdo a las actividades y funciones operativas que deban cumplir los distintos usuarios*
   - *La sensibilidad de los datos*
   - *La oposición de intereses entre las áreas afectadas.*
c. *Resultará necesario determinar una declaración de perfiles de usuarios y los mismos estarán determinados por grupos específicos para cada sistema de información.*

[...]

12. SEGURIDAD DE LAS OPERACIONES (ISO 27001-A.12)
[...]

12.4. REGISTROS Y MONITOREO [ISO 27001 A.12.4]
[...]

12.4.3. Registros del administrador y del operador [ISO 27001 A.12.4.3]

a) *Todas las actividades del administrador y operador del sistema deberán estar debidamente registradas y revisadas periódicamente por la Oficina de Seguridad Informática.*

b) *Para la generación y formato de los registros de auditoría deben seguirse los siguientes lineamientos:*

   - *Se debe registrar la actividad de los administradores y operadores del sistema, identificando a la persona, hora de ingreso, motivo del uso de la cuenta de acceso y acciones realizadas.*
   - *Las actividades diarias no deben realizarse a través de cuentas con accesos privilegiados.*
   - *Toda cuenta con acceso de administrador debe poseer un responsable directo.*

[...]"

Por su parte, las Normas Generales de Control Interno aprobadas mediante Resolución de Contraloría N.°320-2006-CG publicada el 3 de noviembre de 2006 y vigentes desde la misma fecha, en lo referido a las Normas Básicas para las Actividades de Control Gerencial, establecen lo siguiente:

"[...]
3.10. Controles para las Tecnologías de la Información y Comunicaciones

La información de la entidad es provista mediante el uso de Tecnologías de la Información y Comunicaciones (TIC). Las TIC abarcan datos, sistemas de información, tecnología asociada, instalaciones y personal. Las actividades de control de las TIC incluyen controles que garantizan el procesamiento de la información para el cumplimiento misional y de los objetivos de la entidad, debiendo estar diseñados para prevenir, detectar y corregir errores e irregularidades mientras la información fluye a través de los sistemas.

Comentarios:

01 Los controles generales los conforman la estructura, políticas y procedimientos que se aplican a las TIC de la entidad y que contribuyen a asegurar su correcta operatividad. Los principales controles deben establecerse en:

- *Sistemas de seguridad de planificación y gestión de la entidad en los cuales los controles de los sistemas de información deben aplicarse en las secciones de desarrollo, producción y soporte técnico*
- *Segregación de funciones*
- *Controles de acceso general, es decir, seguridad física y lógica de los equipos centrales*
- *Continuidad en el servicio.*

02 Para la puesta en funcionamiento de las TIC, la entidad debe diseñar controles en las siguientes etapas:

(i) Definición de los recursos
(ii) Planificación y organización
(iii) Requerimiento y salida de datos o información
(iv) Adquisición e implementación
(v) Servicios y soporte
(vi) Seguimiento y monitoreo.

03 La segregación de funciones implica que las políticas, procedimientos y estructura organizacional estén establecidos para prevenir que una persona controle los aspectos clave de las operaciones de los sistemas, pudiendo así conducir a acciones no autorizadas u obtener acceso indebido a los recursos de información.

De igual manera, la referida normativa, en sus normas básicas para las actividades de prevención y monitoreo, señala:

5. Norma General para la Supervisión:
[...]

5.1 NORMAS BÁSICAS PARA LAS ACTIVIDADES DE PREVENCIÓN Y MONITOREO
[...]

5.1.1 Prevención y Monitoreo

El monitoreo de los procesos y operaciones de la entidad debe permitir conocer oportunamente si estos se realizan de forma adecuada para el logro de sus objetivos y si en el desempeño de las funciones asignadas se adoptan las acciones de prevención, cumplimiento y corrección necesarias para garantizar la idoneidad y calidad de los mismos.

Comentarios:

01 La supervisión constituye un proceso sistemático y permanente de revisión de los procesos y operaciones que lleva a cabo la entidad, sean de gestión, operativas o de control. En su desarrollo intervienen actividades de prevención y monitoreo por cuanto, dada la naturaleza integral del control interno, resulta conveniente vigilar y evaluar sobre la marcha, es decir conforme transcurre la gestión de la entidad, para la adopción de las acciones preventivas o correctivas que oportunamente correspondan.

02 La prevención implica desarrollar y mantener una actitud permanente de cautela e interés por anticipar, contrarrestar, mitigar y evitar errores, deficiencias, desviaciones y demás situaciones adversas para la entidad. Se fundamenta sobre la base de la observación y análisis de sus procesos y operaciones, efectuados de manera diligente, oportuna y comprometida con la

buena marcha institucional. En tal sentido, está estrechamente relacionada y opera como resultado de las actividades de monitoreo.

La situación expuesta, estaría afectando la operatividad de los servicios críticos vinculados a las obligaciones tributarias de los contribuyentes en los servidores. al no haberse implementado el comando utilitario SUDO en los 592 servidores WEBLOGIC de producción.

Los hechos antes descritos, se habría producido por la ausencia de seguimiento y supervisión por parte de la División de Soporte y Operación de Infraestructura Tecnológica (DSOIT) en la gestión de accesos y asignación de permisos que aseguren el uso exclusivo de cuentas personalizadas y privilegiadas mediante SUDO.

SUPERINTENDENCIA NACIONAL DE ADUANAS Y DE ADMINISTRACIÓN TRIBUTARIA - Órgano de Control Institucional - JEFE - RICARDO ANDRÉS LOTHA FITZGERRE -

2.4 COBERTURA INSUFICIENTE DE SENSORES EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA NUBE PRIVADA DE LA SUNAT, LIMITA LA CAPACIDAD DE LOS OPERADORES DE MONITOREO PARA LA DETECCIÓN, REGISTRO Y COMUNICACIÓN OPORTUNA DE EVENTOS QUE PROVOCARÍAN INTERRUPCIONES EN LOS SISTEMAS INFORMÁTICOS; SITUACIÓN QUE AFECTARÍA LA CONTINUIDAD DE LOS SERVICIOS TRIBUTARIOS Y ADUANEROS.

De la revisión a la información[33] proporcionada por la División de Gestión de Infraestructura Tecnológica (DGIT) y de la División de Soporte y Operación de la Infraestructura Tecnológica (DSOIT), en relación a la indisponibilidad de los servicios informáticos ocurridos el 31 de mayo de 2024; se aprecia en el Documento Técnico[34] "Evidencias Caso Soporte HCX 31/Mayo/2024" que el incidente informático que afectó la continuidad de los servicios y sistemas[35] webs institucionales; se originó en una falla crítica de los componentes HCX[36] de la plataforma de Nube Privada[37] de la SUNAT, la cual era la encargada de mantener la comunicación y operación de los servicios virtualizados entre la plataforma de virtualización legacy Lenovo Flex System y la Solución de Virtualización de la Nube Privada.

De lo indicado en el citado documento técnico, esta interrupción se produjo como consecuencia de una contención[38] de recursos en los hosts físicos (particularmente de CPU y memoria), donde se encontraban ejecutándose los Appliances[39] HCX, generándose un comportamiento inestable de los túneles[40] de comunicación (tunnel flapping). Esta situación se agravó por el uso elevado de recursos por parte de otras

33 Remitida mediante seguimiento N.° 3 del documento Solicitud N.° 000065-2025-1C0000; y seguimiento N.° 8 del documento Solicitud N.° 000047-2025-1C0000; respectivamente por DGIT y DSOIT.

34 Documento Técnico: "Evidencias Caso Soporte HCX 31/Mayo/2024" elaborado por Renato Yamada (BROADCOM) en junio 2024.

35 1) Trámites y Consultas en SUNAT Operaciones en Línea (SOL), 2) Plataforma de Declaración y Pago, 3) Recepción de Factura Electrónica, Boleta de Venta Electrónica, Nota de Crédito Electrónica, Nota de Débito Electrónica, Resumen de Boletas de Venta Electrónica, a través del SEE- del Contribuyente y SEE-SFS, 4) Portal del Operador de Comercio Exterior, 5) Teledespacho, SEIDA, Pago Electrónico de Aduanas, Manifiesto de Carga, 6) Aplicaciones de consulta y registro, 7) Mesa de Partes Virtual – MPV, y 8) Emisión y recepción de Comprobante de pago electrónico y guía de remisión electrónico)

36 Los componentes HCX (Hybrid Cloud Extension) son módulos especializados dentro de la solución VMware HCX, una plataforma que permite migrar, conectar y extender redes entre diferentes entornos de nube o centros de datos de forma segura y eficiente.

37 Una nube privada (o private cloud) es un tipo de infraestructura de computación en la nube exclusiva para una sola organización. Esto significa que los recursos informáticos como servidores, almacenamiento, redes y servicios virtuales están dedicados únicamente a esa organización, sin compartirse con otras.

38 En el contexto de tecnología, virtualización o redes, una contención ocurre cuando dos o más procesos, máquinas virtuales o sistemas compiten por los mismos recursos físicos (como CPU, memoria RAM, disco o red), y no hay suficiente capacidad disponible para todos al mismo tiempo

39 Appliances HCX (VMware HCX Appliances) son componentes virtuales que se despliegan dentro del entorno de virtualización (como VMware vSphere o una nube privada) para permitir la interconexión, migración y extensión de redes entre centros de datos o nubes.

40 Un túnel de comunicación es una conexión segura y virtual entre dos puntos de red que permite enviar datos protegidos, como si viajaran por un canal privado, aunque lo hagan por una red pública. Se usa en VPNs, conexiones entre centros de datos y migraciones en nubes privadas.

máquinas virtuales, que compartían el mismo entorno.

Cabe mencionar, que la SUNAT cuenta con diversos softwares de monitoreo, tanto para aplicaciones, infraestructura y servicios, entre ellas: PRTG, Dynatrace, Kibana, Site24x7, Dashboard. Asimismo, la DSOIT tiene[41] como principal herramienta de monitoreo el software PRTG[42] (Paessler Router Traffic Grapher), el cual es usado para monitorizar los servicios y sistemas informáticos montados en la plataforma de la Nube Privada; no obstante, la División de Soporte y Operación de la Infraestructura Tecnológica aclaró[43] que esta herramienta de monitoreo no está orientada a componentes de propósito específico como los Appliance HCX y que este componente se monitoreaba a través de la solución VMWARE Cloud Foundation; esta afirmación fue ratificada[44] por la DSOIT, comentando además que el monitoreo se realizaba a través de vSphere Cliente.

En ese sentido, se solicitó el registro de eventos generados por la herramienta de monitoreo PRTG que fueron enviados a la Herramienta de Gestión de Servicios TI (iTop), correspondientes al 31 de mayo de 2024, con la finalidad de verificar la existencia de eventos relacionados a la contención del Appliance HCX. Del análisis efectuado, se identificaron ocho (8) registros clasificados como eventos, los cuales se vinculaban a alertas por "espacio en disco crítico".

Asimismo, del registro de bitácora de incidentes remitido por la DSOIT se identificó que los tickets I-928907, I-928905, I-928902 e I-928864 —los cuales estarían vinculados a los problemas generados por el incidente ocurrido en la Nube Privada— corresponden a incidencias que no fueron registradas por los operadores de monitoreo ni por el personal de la DSOIT responsable de la gestión de eventos y alertas, sino por usuarios que resultaron afectados por el evento crítico.

En ese entender, del registro[45] de incidencias correspondientes al 31 de mayo de 2024 en la Herramienta de Gestión de Servicios TI (iTop), se verificó que no existe ningún registro previo al inicio de la caída de los sistemas y servicios informáticos web de la entidad que guarde relación directa con la contención del Appliance HCX. No obstante, se identificaron incidencias registradas con posterioridad al inicio del evento; sin embargo, estas no fueron generadas por los operadores de monitoreo, sino por los propios usuarios de la Entidad que ya se encontraban afectados por la interrupción del servicio.

A continuación, se presenta una muestra de las incidencias reportadas por estos usuarios:

41 Respuesta a la pregunta 14 del cuestionario realizado a el jefe de la DGIT, Carlos Manuel Posadas Vallejos; y, remitido a la comisión auditora mediante correo electrónico de 27 de agosto de 2025.

42 Es un software de monitoreo de red, sirve para supervisar y gestionar en tiempo real toda la infraestructura de TI, incluyendo servidores, tráfico de red, ancho de banda y aplicaciones. Su principal objetivo es detectar y solucionar problemas antes de que afecten el rendimiento del negocio y asegurar que los componentes críticos estén siempre disponibles.

43 Respuesta a la pregunta 11 del cuestionario realizado a la DSOIT, suscrito por el supervisor Marco Alcca Soncco; y, remitido a la comisión auditora mediante correo electrónico de 29 de agosto de 2025.

44 Mediante respuesta a la pregunta 1 del Memorándum N.° 020-2025-OCI-SUNAT/1C0000-AC006 de 6 de noviembre de 2025, realizado a la DSOIT.

45 Remitida por la DAU, en respuesta a la pregunta 1 del Memorándum n.° 005-2025-OCI-SUNAT/1C0000-AC006 de 24 de septiembre de 2025.

Cuadro N.° 3
Incidentes registrados tras la ocurrencia del evento crítico

N.°	CATEGORÍA	ASUNTO	FECHA Y HORA DEL INCIDENTE
1	Aplicaciones de negocio	Problemas para acceso al RSIRAT	2024-05-31 12:32:10
2	Aplicaciones de negocio	Revisar intranet es lento para ingresar a trabajo en linea, sale error interno de servidor	2024-05-31 12:34:52
3	Aplicaciones de negocio	Problemas en RSIRAT, Echaski, INTRANET (modificacion de datos)	2024-05-31 12:41:33
4	Fraccionamiento	Problemas de ingreso al RSIRAT	2024-05-31 12:48:00
5	Aplicaciones de negocio	Problemas para ingresar al Rsirat	2024-05-31 12:59:43
6	Aplicaciones de negocio	!BIEN URGENTE! el RSIRAT falla. Saludos	2024-05-31 13:05:07
7	Cobranza coactiva	IMPOSIBILIDAD DE ACCEDER A LOS APLICATIVOS RSIRAT	2024-05-31 13:09:55
8	Aplicaciones de negocio	PROBLEMAS PARA ACCEDER AL RSIRAT	2024-05-31 13:10:15
9	Aplicaciones de negocio	No puedo ingresar al RSIRAT	2024-05-31 13:14:27
10	Control electrónico	NO SE CUENTA CON ACCESO A SGIP PARA REGISTRO DE INTERVENCIONES	2024-05-31 13:43:30
11	Cobranza coactiva	no puedo ingresar a RSIRAT con mi acceso ni a Prico ni a Mepeco	2024-05-31 13:49:14
12	Portal del funcionario	Error en el sistema	2024-05-31 13:49:30
13	Aplicaciones de negocio	SE SOLICITA REVISAR INTRANET /TRABAJO EN LINEA/EXPEDIENTE VIRTUAL/REGISTRO DE DOCUMENTOS	2024-05-31 13:59:33
14	Aplicaciones de negocio	incidente RSIRAT	2024-05-31 13:59:41
15	Cobranza coactiva	BCP Reporta Error 503 - No puede ingresar al NSEMT	2024-05-31 13:59:54
16	Fraccionamiento	ERROR SIRAT	2024-05-31 14:07:30
17	Aplicaciones de negocio	no se puede ingresar al rsirat	2024-05-31 14:14:55
18	Fraccionamiento	SIN ACCESO AL RSIRAT MEPECO y RSIRAT PRICO_REG. 516ª	2024-05-31 14:30:09
19	Cobranza coactiva	sin acceso al rsirat	2024-05-31 14:32:10
20	Cobranza coactiva	Sistema no permite ingreso al RSIRAT	2024-05-31 14:37:48
21	Cobranza coactiva	RSIRAT no funciona _31/05/2024_Intendencia Lima	2024-05-31 14:39:08
22	Aplicaciones de negocio	NO PUEDO ACCEDER AL R-SIRAT - PC NBB897	2024-05-31 14:41:26
23	Cobranza coactiva	RSIRAT NO PUEDE ACCEDER A MI DEPENDECIA ITI LORETO MEPECO	2024-05-31 14:45:18
24	Aplicaciones de negocio	RSIRAT - SIN ACCESO	2024-05-31 14:51:24
25	Cobranza coactiva	ERROR_NO SE PUEDE INGRESAR AL SIRAT – 31.05.2024	2024-05-31 15:04:16
26	Control aduanero	PROBLEMAS PARA ACCEDER A ROL REGISTRO SMART	2024-05-31 15:11:26
27	Cobranza coactiva	INTRANET_INCONVENIENTES CON SINE_31-5-2024	2024-05-31 15:26:42
28	Aplicaciones de negocio	No tengo acceso a las aplicaciones de sunat	2024-05-31 15:46:28
29	Aplicaciones de negocio	No tengo acceso a las aplicaciones de sunat	2024-05-31 15:54:09
30	Cobranza coactiva	No me permite ingresar al aplicativo y se congela el RSIRAT	2024-05-31 15:54:28

Fuente: Reporte de incidentes que corresponden a 31 de mayo de 2024, remitido por la DAU mediante Correo Electrónico de 30 de octubre de 2025.
Elaborado por: Comisión Auditora.

Por lo que, las acciones realizadas por la entidad a fin de solucionar este incidente, fueron dadas por los hechos que se detallan en el cuadro siguiente:

Cuadro N.° 4
Acciones realizadas posterior a la ocurrencia del incidente

N.°	HORA	SISTEMAS AFECTADOS
1	12:05 hrs	Indisponibilidad total de los sistemas web de la entidad
2	12:05 hrs	La DSOIT identificó mediante la herramienta de monitoreo de infraestructura PRTG una avería masiva en la plataforma de aplicaciones WEB.
3	12:45 hrs	La DGIT, con el apoyo del contratista, identificó que el incidente masivo tuvo su origen en una falla en un componente de comunicación interna (HCX) de la Solución de Virtualización Nube Privada.
4	13:43 hrs	Se escala el incidente al fabricante, VMWARE, con alta prioridad.
5	14:45 hrs	El fabricante se incorporó a la reunión Teams (War Room).
6	15:30 hrs	Se identifica la solución al incidente y se habilitan nuevos canales de comunicación.
7	16:10 hrs	Reinicio ordenado de servicios y retorno progresivo a la operatividad regular.
8	16:10 hrs	Restablecimiento del sistema de Presentaciones de la Declaración Jurada Anual del Impuesto a la Renta 2023.
9	19:19 hrs	Restablecimiento del sistema de Comprobante de Pago Electrónico – Factura Portal.
10	19:19 hrs	Restablecimiento del sistema de Comprobante de Pago Electrónico – Recibo por Honorario Electrónico.
11	21:21 hrs	Restablecimiento del sistema de Emisión Electrónica desde los Sistemas del Contribuyente / sistema Facturador SUNAT.

Fuente: Documentación presentada[46] por DSOIT en respuesta a la pregunta 14 del Memorándum N.° 005-2025-OCI-SUNAT/1C0000-AC006 de 24 de septiembre de 2025.
Elaborado por: Comisión Auditora.

Adicionalmente, a los hechos descritos en el cuadro precedente, la entidad emitió un Comunicado oficial a través de la plataforma web de SUNAT para informar a los Usuarios sobre los inconvenientes presentados y otorgó un plazo adicional a aquellos Contribuyentes que no pudieron realizar sus registros correspondientes. La falla se prolongó hasta por más de diez horas con veinte y un minutos (10:21 horas) ya que el restablecimiento de los sistemas fue dándose gradualmente.

En cuanto a los documentos normativos para la atención de eventos/alertas/incidentes informáticos, la entidad cuenta con un Procedimiento para el monitoreo y gestión de eventos de los servicios críticos V 1.0 [PSS.MGES.10] de 28 de noviembre de 2019, y el Procedimiento de Gestión de Eventos de la INSI v 2.0 [A03.3.1-PR-001] de 6 de diciembre de 2022, aprobados mediante Resolución de Intendencia N.° 022-2019-SUNAT/1U0000 y Resolución de Intendencia N.° 013-2021-SUNAT/1U0000, respectivamente.

Al respecto, el Procedimiento para el monitoreo y gestión de eventos de los servicios críticos, tiene por objetivo *"Establecer las actividades para el monitoreo y gestión de eventos con el objetivo de asegurar el normal funcionamiento de la infraestructura y aplicaciones informáticas de la SUNAT"*, siendo de alcance a todas las Unidades Orgánicas de la Intendencia Nacional de Sistemas de Información que participan en el proceso de monitoreo y gestión de eventos.

[46] Documento Técnico "Plataforma Nube Privada - Incidente ocurrido el 31 de mayo de 2024" de 5 de junio de 2024; Informe n.° 000001-2024-SUNAT/1U5100 de 3 de junio de 2024 e Informe N.° 000011-2024-SUNAT/1U5102 de 24 de junio de 2024.

Por otra parte, este procedimiento define el rol del Operador de Monitoreo con la siguiente definición *"es el encargado de realizar el monitoreo de la infraestructura de TI y aplicaciones informáticas"*, así mismo, define su responsabilidad en los términos siguientes *"1) realizar el monitoreo de la infraestructura de TI y aplicaciones informáticas. 2) reportar los eventos de advertencia y excepción que se produzcan durante el monitoreo al operador de infraestructura tecnológica"*.

Mientras tanto, el Procedimiento de Gestión de Eventos de la INSI tiene por objetivo *"Gestionar el ciclo de vida de los eventos que afectan los elementos de los servicios TI, asegurando controles que garanticen su disponibilidad"* [47]. Entre sus actores se encuentra el Operador de Monitoreo, perteneciente a la División de Soporte y Operación de la Infraestructura Tecnológica, quien es responsable de registrar los eventos[48]. Asimismo, este operador prioriza la atención según el nivel del evento (excepción o advertencia), verifica si existe un procedimiento temporal y aplica el workaround[49] correspondiente; Cuando el evento se resuelve, actualiza el ticket a estado "solucionado"; de lo contrario, lo deriva al equipo de Soporte de Monitoreo.

Por su parte, el apartado de Roles y Responsabilidades del citado procedimiento precisa que, el Operador de Monitoreo es el responsable directo de la supervisión y control de los eventos generados por los sistemas. Le corresponde, entre otras funciones, supervisar las acciones automáticas generadas por los eventos y tomar acción frente a aquellos que requieren interacción manual dentro de los procesos de gestión de incidentes.

Estos procedimientos están orientados a minimizar el impacto o prevenir posibles incidentes producto de los eventos relacionados; dicho de otra manera, las acciones de respuesta luego del análisis de las alertas (producto de un evento) presentadas en las herramientas de monitoreo deben estar enfocadas a recuperar el estado normal de un elemento de configuración.

Por otra parte, de la documentación solicitada al Operador de monitoreo (turno mañana) del 31 de mayo de 2024, señor Percy Amet Ríos Malarín, respecto a las alertas (excepción y advertencia) que se registraron automáticamente en la HGSTI (iTop) durante su turno, relacionada al incidente (Contencion Appliance HCX). Remitió ocho (8) alertas; sin embargo, no corresponden a la contención del Appliance HCX, sino que están vinculaban a alertas por "espacio en disco crítico", en algunos servidores virtuales tal como muestra la siguiente imagen:

[47] Tomado del apartado OBJETIVO, del Procedimiento de Gestión de Eventos de la INSI v 2.0 [A03.3.1-PR-001]; de 6 de diciembre de 2022.

[48] Un evento es un cambio de estado que tiene una significancia para la gestión de un elemento de configuración o un servicio informático.

[49] Un WORKAROUND es una solución temporal o alternativa provisional que se aplica para mitigar o resolver parcialmente un problema técnico, mientras se desarrolla o implementa una solución definitiva.

Imagen N.° 5
Eventos registrados en el iTOP que no guardan relación con el incidente crítico del 31-05-2024

Evento	Asunto	Organización	Reportado por	Fecha de Inicio
E-929007	'Sensor': 'Espacio Filesystem', 'Dispositivo': 's00plowfst003'	SUNAT	DSOIT-Monitoreo Administrador de Monitoreo	2024-05-31 21:22:41
E-928986	'Sensor': 'Espacio Filesystem', 'Dispositivo': 's00plowfst004'	SUNAT	DSOIT-Monitoreo Administrador de Monitoreo	2024-05-31 20:17:33
E-928789	'Sensor': 'Espacio Filesystem', 'Dispositivo': 'w8lssunat'	SUNAT	DSOIT-Monitoreo Administrador de Monitoreo	2024-05-31 16:51:10
E-927956	'Sensor': 'Espacio Filesystem', 'Dispositivo': 's00plowfst003'	SUNAT	DSOIT-Monitoreo Administrador de Monitoreo	2024-05-31 10:49:25
E-927715	'Sensor': 'Espacio Filesystem', 'Dispositivo': 'w8lmsunat'	SUNAT	DSOIT-Monitoreo Administrador de Monitoreo	2024-05-31 07:43:29
E-927711	'Sensor': 'Espacio Filesystem', 'Dispositivo': 's00plowfst003'	SUNAT	DSOIT-Monitoreo Administrador de Monitoreo	2024-05-31 06:59:25
E-927700	'Sensor': 'Espacio Filesystem', 'Dispositivo': 's00plowfst003'	SUNAT	DSOIT-Monitoreo Administrador de Monitoreo	2024-05-31 00:59:24
E-927699	'Sensor': 'Espacio Filesystem', 'Dispositivo': 's00plowfst003'	SUNAT	DSOIT-Monitoreo Administrador de Monitoreo	2024-05-31 00:39:25

Fuente: En respuesta a la pregunta 1 del requerimiento de información realizado al Sr. Percy Amet Ríos Malarin, el cual fue alcanzado mediante correo electrónico (monitor@sunat.gob.pe) del 7 de noviembre de 2025

De igual modo, ante la consulta al señor Percy Amet Ríos Malarín (Operador de monitoreo) respecto a los incidentes registrados en la HGSTI (iTop) durante su turno del 31 de mayo de 2024. Respondió *"Mi persona no registró el incidente en el itop, ya que son los propios usuarios, los que aperturan los incidentes y nos hacen llegar por correos y en la misma aplicación del itop, en la bitácora de operaciones se registró el incidente del 31 de mayo del 2024 con sus respectivos itops generados por los usuarios"*.

De lo expuesto, se advierte que, la cobertura insuficiente de sensores limitó la detección oportuna de los eventos/alertas por parte del Operador de monitoreo de turno, ya que únicamente recibió alertas relacionadas con "espacio en disco crítico" o se enteró por reportes de Usuarios posterior al inicio del evento crítico. Esto evidencia que los sensores orientados a monitorear la capacidad de recursos de la infraestructura de Nube Privada son inexistentes o no están configurados, lo cual representa una falla de control.

Asimismo, la ausencia de monitoreo constante de la plataforma de nube privada mediante la herramienta vSphere Client contribuye a que los incidentes no puedan prevenirse antes de ocurrir, dado que las acciones se ejecutan de manera reactiva y no preventiva

Al respecto, el Procedimiento de Gestión de Eventos de la INSI v 2.0 [A03.3.1-PR-001] de 6 de diciembre de 2022; aprobado con Resolución de Intendencia 013-2021/SUNAT/1U0000, establece lo siguiente:

"[...]
V. DESCRIPCIÓN DEL PROCESO GESTIÓN DE EVENTOS
[...]
5.1 Reglas del Proceso
5.1.1 Reglas generales de Gestión de Eventos
[...]

d) Es responsabilidad del solicitante del Pase a Producción, para la implementación de nuevos servicios o servidores que implique la creación de nuevos sensores, entregar todas las definiciones completas de las nuevas configuraciones de alertas de monitoreo de los servicios TI.

e) Es responsabilidad del solicitante de la Petición, para la actualización de umbrales y sensores entregar todas las definiciones de las configuraciones en los servidores de los servicios de TI, que será aprobado por su jefe directo.

[...]

g) *Toda acción de respuesta indicada en una configuración de alerta de monitoreo debe estar orientada a minimizar el impacto o prevenir posibles incidentes producto de los eventos relacionados.*

Anexo 3. Roles y Responsabilidades
[...]
Operador de Monitoreo
Es el responsable directo de la supervisión y control de los eventos generados por los sistemas.
Es responsable de:
a. Supervisar las acciones automáticas generadas por eventos.
b. Tomar acción ante los eventos que ameriten generar interacción manual con los procesos de Gestión de Incidentes, Cambios o Problemas.
c. Realizar un soporte de primer nivel ante incidentes generados por eventos, identificados en la Base de datos de errores conocidos.
[...]"

Del mismo modo, el Procedimiento para el Monitoreo y Gestión de Eventos de los Servicios Críticos v 1.0 [PSS.MGES.10] de 28 de noviembre de 2019; aprobado con Resolución de Intendencia N.°022-2019/SUNAT/1U0000, establece lo siguiente:

"[...]

V. ROLES Y RESPONSABILIDADES
5.1. Roles
[...]

b. Operador de Monitoreo: *Es el encargado de realizar el monitoreo de la infraestructura de TI y aplicaciones informáticas.*

c. Operador de Infraestructura Tecnológica: *Es el encargado de ejecutar acciones preestablecidas sobre la infraestructura tecnológica según corresponda. Asimismo, se encarga de generar los tickets de incidente cuando se trata de un evento de excepción y cuando el tratamiento a un evento no da resultado.*

5.2. Responsabilidades
[...]
b. Operador de Monitoreo
- *Realizar el monitoreo de la infraestructura de TI y aplicaciones informáticas.*
- *Reportar los eventos de advertencia y excepción que se produzcan durante el monitoreo al Operador de Infraestructura Tecnológica.*

c. Operador de Infraestructura Tecnológica
- *Registrar y ejecutar el tratamiento a los eventos de advertencia, a fin de mantener los valores monitoreados dentro de los umbrales establecidos.*
- *Generar los tickets de incidentes cuando se trata de un Evento de Excepción o cuando el tratamiento de un evento no da resultado.*
- *Mantener actualizado el registro de eventos de excepción.*
- *Comunicar los incidentes generados por eventos de excepción al Gestor de Incidentes.*

[...]"

Por su parte, las Normas Generales de Control Interno aprobadas mediante Resolución de Contraloría N.°320-2006-CG publicada el 3 de noviembre de 2006 y vigentes desde la misma fecha, en lo referido a las Normas Básicas para las Actividades de Control Gerencial, establecen lo siguiente:

"[...]

3.10. Controles para las Tecnologías de la Información y Comunicaciones

La información de la entidad es provista mediante el uso de Tecnologías de la Información y Comunicaciones (TIC). Las TIC abarcan datos, sistemas de información, tecnología asociada, instalaciones y personal. Las actividades de control de las TIC incluyen controles que garantizan el procesamiento de la información para el cumplimiento misional y de los objetivos de la entidad, debiendo estar diseñados para prevenir, detectar y corregir errores e irregularidades mientras la información fluye a través de los sistemas.

Comentarios:

01 Los controles generales los conforman la estructura, políticas y procedimientos que se aplican a las TIC de la entidad y que contribuyen a asegurar su correcta operatividad. Los principales controles deben establecerse en:

- *Sistemas de seguridad de planificación y gestión de la entidad en los cuales los controles de los sistemas de información deben aplicarse en las secciones de desarrollo, producción y soporte técnico.*

[...]

- *Continuidad en el servicio.*

02 Para la puesta en funcionamiento de las TIC, la entidad debe diseñar controles en las siguientes etapas:
(i) Definición de los recursos
[...]
(vi) Seguimiento y monitoreo.
(...]

07 Para el adecuado ambiente de control en los sistemas informáticos, se requiere que éstos sean preparados y programados con anticipación para mantener la continuidad del servicio. Para ello se debe elaborar, mantener y actualizar periódicamente un plan de contingencia debidamente autorizado y aprobado por el titular o funcionario designado donde se estipule procedimientos previstos para la recuperación de datos con el fin de afrontar situaciones de emergencia. (...)

08 El programa de planificación y administración de seguridad provee el marco y establece el ciclo continuo de la administración de riesgos para las TIC, desarrollando políticas de seguridad, asignando responsabilidades y realizando el seguimiento de la correcta operación de los controles.
"[...]

De igual forma, el referido cuerpo normativo, en sus normas básicas para la Actividad de Prevención y Monitoreo, señala:

5. NORMA GENERAL PARA LA SUPERVISIÓN

[...]

5.1 NORMAS BÁSICAS PARA LAS ACTIVIDADES DE PREVENCIÓN Y MONITOREO

5.1.1 Prevención y Monitoreo

El monitoreo de los procesos y operaciones de la entidad debe permitir conocer oportunamente si éstos se realizan de forma adecuada para el logro de sus objetivos y si en el desempeño de las funciones asignadas se adoptan las acciones de prevención, cumplimiento y corrección necesarias para garantizar la idoneidad y calidad de los mismos.

Comentarios:

01 La supervisión constituye un proceso sistemático y permanente de revisión de los procesos y operaciones que lleva a cabo la entidad, sean de gestión, operativas o de control. En su desarrollo intervienen actividades de prevención y monitoreo por cuanto, dada la naturaleza integral del control interno, resulta conveniente vigilar y evaluar sobre la marcha, es decir conforme transcurre la gestión de la entidad, para la adopción de las acciones preventivas o correctivas que oportunamente correspondan.

02 La prevención implica desarrollar y mantener una actitud permanente de cautela e interés por anticipar, contrarrestar, mitigar y evitar errores, deficiencias, desviaciones y demás situaciones adversas para la entidad. Se fundamenta sobre la base de la observación y análisis de sus procesos y operaciones, efectuados de manera diligente, oportuna y comprometida con la buena marcha institucional. En tal sentido, está estrechamente relacionada y opera como resultado de las actividades de monitoreo."

[...]"

De lo expuesto, la inexistencia de sensores y umbrales orientados a monitorear la capacidad de recursos de la plataforma de nube privada impide una detección preventiva, generando el riesgo de que se produzcan incidentes que prolonguen la indisponibilidad de los sistemas web institucionales y afecten la continuidad de los servicios tributarios y aduaneros.

La situación expuesta se habría originado por la ausencia de seguimiento y supervisión de los Operadores de Monitoreo de la División de Soporte y Operación de Infraestructura Tecnológica (DSOIT) en la gestión de umbrales y sensores destinados a monitorear la capacidad de CPU y memoria de los hosts de la nube privada.

2.5 INCIDENTES INFORMÁTICOS CUYOS TIEMPOS DE REPARACIÓN SUPERAN EL PLAZO MÁXIMO ESTABLECIDO CONTRACTUALMENTE, NO TIENEN REGISTROS EN LA HERRAMIENTA ITOP QUE PERMITAN VERIFICAR LA TRAZABILIDAD DE LA ATENCIÓN, GENERANDO EL RIESGO DE QUE EL CONTRATISTA NO CUMPLA EN DICHO PLAZO CON LA REPARACIÓN Y SERVICIOS DE LOS BIENES OFERTADOS, LIMITANDO LA IDENTIFICACIÓN DE PENALIDADES INCURRIDAS.

De la información remitida por la División de Ejecución Contractual (DEC[50]), se identificó que, en la evaluación de los Informes Técnicos Trimestrales del Servicio de Soporte, correspondiente al Contrato N.° 268-2020/SUNAT y realizada por el colaborador de la DGIT, Jaime Pacheco Huamán, se reportaron diversos incidentes informáticos vinculados a componentes de hardware y se detallan en el siguiente cuadro:

Cuadro N.° 5
Listado de Incidentes Informáticos de componentes de Hardware

N.°	NÚMERO DE INFORME TRIMESTRAL	NÚMERO DE TICKET DEL FABRICANTE	DESCRIPCIÓN DEL INCIDENTE	FECHA DE INICIO	FECHA DE CIERRE	TIEMPO DE REPARACIÓN
1	Informe Técnico N.°055-2023-SUNAT/1U5200	#157302313	Falla de disco en Host 15.	30/11/2022 09:40 am	01/12/2022 10:00 am	1 día y 20 minutos

50 En respuesta al Memorándum n.° 0001-2025-OCI-SUNAT/1C0000-AC006 de 28 de agosto de 2025.

N.°	NÚMERO DE INFORME TRIMESTRAL	NÚMERO DE TICKET DEL FABRICANTE	DESCRIPCIÓN DEL INCIDENTE	FECHA DE INICIO	FECHA DE CIERRE	TIEMPO DE REPARACIÓN
2	Informe Técnico N.°055-2023-SUNAT/1U5200	#159534550 / #159635419	Desconexion de las interfaces de red de los HOST 6 y Host 7 MNG (Management)	04/01/2023 11:00 am	06/01/2023 09:00 am	1 dia y 22 horas
3	Informe Técnico N.°210-2023-SUNAT/1U5200	#165919236	Se presentó un error en un módulo de memoria en el Host 5 de WLD 1 (Producción)	12/04/2023 11:30 pm	14/04/2023 10:00 pm	1 dia, 22 horas y 30 minutos
4	Informe Técnico N.°210-2023-SUNAT/1U5200	#165589931	Se presentó un error en un módulo de memoria en el Host 6 de WLD 1 (Producción	04/04/2023 09:30 am	04/04/2023 10:00 pm	12 horas y 30 minutos
5	Informe Técnico N.°210-2023-SUNAT/1U5200	#166377723	Se presentó un error en un módulo de memoria en el Host 6 de WLD 1 (Producción	16/04/2023 09:30 am	16/04/2023 10:00 pm	12 horas y 30 minutos
6	Informe Técnico N.°371-2023-SUNAT/1U5200	#171952786	Se presentó un error en el módulo de memoria Host 8 del WLD1 (Producción)	14/07/2023 09:00 am	14/07/2023 11:30 pm	14 horas y 30 minutos
7	Informe Técnico N.°371-2023-SUNAT/1U5200	#171090519	Se presentó un error en Network Uplink redundancia lost en el Host 5 del WLD1	29/06/2023 09:30 am	30/06/2023 11:00 pm	1 día, 14 horas y 30 minutos
8	Informe Técnico N.°000539-2023-SUNAT/1U5200	#174726773	Desconexión de la vmnic 2 del Host 5 del WLD 1 (Producción)	05/09/2023 09:00 am	13/09/2023 04:00 pm	8 días y 7 horas extras
9	Informe Técnico N.°000539-2023-SUNAT/1U5200	#174726834	Desconexión de la vmnic 2 del Host 7 del WLD 1 (Producción)	29/08/2023 09:00 am	30/08/2023 10:00 pm	1 día y 13 horas
10	Informe Técnico N.°000539-2023-SUNAT/1U5200	#175147466	Falla en un módulo de memoria del Host 12 del WLD1	01/09/2023 2:30 pm	01/09/2023 11:00 pm	8 horas 30 minutos
11	Informe Técnico N.°000539-2023-SUNAT/1U5200	#176302625	Falla en un disco de capacidad del Host 3 del WLD1	21/09/2023 02:00 pm	25/09/2023 10:00 pm	4 días y 8 horas
12	Informe Técnico N.°000539-2023-SUNAT/1U5200	#177992407	Falla en un módulo de memoria en el Host 6 de producción Nube privada	18//10/2023 03:00 pm	18/10/2023 10:00 pm	7 horas
13	Informe Técnico N.°000301-2024-SUNAT/1U5200	#192598211	Unknown disconnection behavior between VxRail Port 25 Health Check de su Networking S5248F-ON	19/06/2024 15:56 hrs	19/06/2024 22:00 hrs	6 horas y 4 minutos
14	Informe Técnico N.°000301-2024-SUNAT/1U5200	#193472082	Se presentó un error no recuperable de memoria en el HOST6 de Producción, lo que ocasionó su reinicio y el de las VMs alojadas.	04/07/2024 10:07 hrs	04/07/2024 23:00 hrs	12 horas 53 minutos
15	Informe Técnico N.°000301-2024-SUNAT/1U5200	#193856287	"Warning" en el módulo de memoria A12	11/07/2024 08:00 hrs	11/07/2024 23:00 hrs	14 horas
16	Informe Técnico N.°000301-2024-SUNAT/1U5200	#194968785	Problema de memoria en el HOST08, error de memoria en la ubicación DIMM_A10	29/07/2024 16:09 hrs	29/07/2024 23:00 hrs	6 horas y 51 minutos

Fuente: Informes técnicos trimestrales de la DGIT, en la que evalúan el servicio de soporte del contratista, información alcanzada en respuesta al Memorándum N.°0001-2025-OCI-SUNAT/1C0000-AC006 de 28 de agosto de 2025

Elaborado por: Comisión Auditora

Como se aprecia en el cuadro anterior, los tiempos de reparación superan las cuatro (4) horas establecidas. Según el numeral 5.10.2 de las Bases Integradas de la Licitación

Pública N.° 0015-2020-SUNAT/8B1200, que dispone que la reparación de los equipos (hardware) debe realizarse dentro de un tiempo máximo de cuatro (04) horas. Este tiempo se computa desde la comunicación del mal funcionamiento al Contratista hasta la reparación y puesta en funcionamiento del equipo a satisfacción de la Entidad, incluyendo el reemplazo de las partes o componentes defectuosos por repuestos originales o el cambio del componente por uno nuevo.

Al respecto, de los informes técnicos mencionados en el cuadro anterior, el evaluador señala que los excesos en los tiempos de reparación no serían atribuibles al Contratista, sino a coordinaciones internas de la propia Entidad. En ese sentido, con el fin de verificar la trazabilidad de los incidentes e identificar los tiempos empleados desde su ocurrencia hasta el reemplazo de las partes, se solicitó[51] a la DGIT los tickets generados en la herramienta ITOP relacionados con dichos incidentes y las solicitudes de cambio de los componentes averiados, así como los correos de coordinación para el ingreso al Data Center u otros que correspondan. Cabe precisar que los tickets mencionados en el cuadro precedente corresponden a los generados por el fabricante y no por la Entidad.

En respuesta a lo solicitado, la DGIT[52] remitió los correos de coordinación para el ingreso del personal encargado de realizar los trabajos de reemplazo de partes en el Data Center, así como las Guías de remisión de los componentes que iban a ser sustituidos. Asimismo, respecto a los tickets de incidentes, señaló lo siguiente:

"[...]
La plataforma de Nube Privada está configurada bajo un esquema de alta disponibilidad y tolerancia a fallas, ***por lo que las alertas de posibles fallas de los componentes de hardware no se traducen, necesariamente, en un ticket de incidente (ITOP).***
[...]

Respecto a los tickets de solicitud de cambio, manifestó lo siguiente:

*"****Los Incidentes que generan cambio de partes no generan tickets en nuestra herramienta de gestión de tickets ITOP*** *dado que no se no considera la categoría asociada a los cambios proactivos de partes o componentes de HW,* ***se ha considerado crear una nueva categoría a fin de que estos casos queden registrados en el sistema****, adjuntando a dichos registros las guías de remisión que correspondan"* (énfasis y subrayado es agregado)

En ese sentido, al no contar con los tickets generados en la herramienta ITOP de la Entidad, se procedió a revisar la información disponible, incluyendo los correos de coordinación para el ingreso al Data Center y las Guías de remisión que acreditan la recepción de las partes a reemplazar. De dicha revisión se obtuvo la información que detalla el cuadro siguiente:

Cuadro N.° 6
Coordinaciones para el ingreso al Data center y llegada de equipos para la atención de incidentes Informáticos

N.°	NÚMERO DE TICKET	FECHA Y HORA DE INICIO DEL INCIDENTE	COORDINACIONES PARA EL INGRESO AL DATA CENTER	COMPONENTES DE REEMPLAZO SEGÚN GUIA DE REMISIÓN
1	157302313	30/11/2022 09:40 am	01/12/2022 07:52 am	No ubicada
2	159534550	04/01/2023 11:00 am	06/01/2023 09:21 am	06/01/2023
3	165919236	12/04/2023	14/04/2023	14/04/2023

51 Mediante Memorándum N.° 008-2025-OCI-SUNAT/1C000-AC006 de 7 de octubre de 2025 y Memorándum N.° 018-2025-OCI-SUNAT/1C000-AC006 de 31 de octubre de 2025

52 Mediante correo electrónico de 22 de octubre de 2025 y 10 de noviembre de 2025.

N.°	NÚMERO DE TICKET	FECHA Y HORA DE INICIO DEL INCIDENTE	COORDINACIONES PARA EL INGRESO AL DATA CENTER	COMPONENTES DE REEMPLAZO SEGÚN GUIA DE REMISIÓN
		11:30 pm	12:26 pm	22:40
4	165589931	04/04/2023 09:30 am	04/04/2023 04:32 pm	04/04/2023 22:09
5	171952786	14/07/2023 09:00 am	14/07/2023 05:30 pm	14/07/2023 22:17
6	171090519	29/06/2023 09:30 am	30/06/2023 7:21 pm	30/06/2023 22:13
7	174726773	05/09/2023 09:00 am	13/09/2023 11:35 am	13/09/2023 13:30
8	174726834	29/08/2023 09:00 am	31/08/2023 2:41 pm	No ubicada
9	175147466	01/09/2023 2:30 pm	01/09/2023 8:23 PM	No ubicada
10	176302625	21/09/2023 02:00 pm	25/09/2023 12:21 PM	25/09/2023 22:04
11	192598211	19/06/2024 15:56 hrs	19/06/2024 8:17 PM	19/06/2024 23:30
12	1934772082	04/07/2024 10:07 hrs	04/07/2024 6:44 PM	04/07/2024 22:14
13	193856287	11/07/2024 08:00 hrs	11/07/2024 7:56 PM	11/07/2024 21:50
14	194968785	29/07/2024 16:09 hrs	29/07/2024 9:55 PM	29/07/2024 23:20

Fuente: Correos de coordinación al Data center y guías de remisión; información alcanzada en respuesta al Memorándum N.°0008-2025-OCI-SUNAT/1C0000-AC006 de 7 de octubre de 2025
Elaborado por: Comisión Auditora.

Del cuadro precedente se advierte que las coordinaciones realizadas para el ingreso al Data Center se efectuaron después de haber transcurrido las cuatro (4) horas establecidas como tiempo máximo de reparación. Asimismo, la fecha y hora consignadas en las Guías de remisión, correspondientes a la llegada de las partes a reemplazar, también se registran con posterioridad a dicho plazo. Por otra parte, los registros permiten concluir que no todo el tiempo excedido respecto del plazo de cuatro horas es atribuible a la entidad. Cabe precisar que las Bases Integradas contemplan, en el rubro "Otras penalidades", las penalidades aplicables por el incumplimiento del tiempo máximo de reparación ante incidencias relacionadas con el servicio de soporte.

De la revisión efectuada se advierte que la DGIT no registró en la herramienta ITOP los tickets correspondientes a incidentes de hardware ocurridos en la nube privada ni aquellos vinculados a solicitudes de cambio de componentes. Además, se verificó que los tiempos de reparación de estos incidentes superaron el máximo de cuatro (4) horas establecido en el numeral 5.10.2 de las Bases Integradas de la Licitación Pública N.° 0015-2020-SUNAT/8B1200. Si bien los informes técnicos atribuyen dichos excesos a coordinaciones internas de la Entidad, no ha sido posible evidenciar fehacientemente que el Contratista excedió dichos plazos contractuales y por tanto identificar la aplicación de penalidades.

Por su parte, las Normas Generales de Control Interno aprobadas mediante Resolución de Contraloría N.° 320-2006-CG publicada el 3 de noviembre de 2006 y vigentes desde la misma fecha, en lo referido a las Normas Básicas para las Actividades de Control Gerencial, establecen lo siguiente:

"[...]
3.10. Controles para las Tecnologías de la Información y Comunicaciones

La información de la entidad es provista mediante el uso de Tecnologías de la Información y Comunicaciones (TIC). Las TIC abarcan datos, sistemas de información, tecnología asociada, instalaciones y personal. Las actividades de control de las TIC incluyen

controles que garantizan el procesamiento de la información para el cumplimiento misional y de los objetivos de la entidad, debiendo estar diseñados para prevenir, detectar y corregir errores e irregularidades mientras la información fluye a través de los sistemas. Comentarios:

01 Los controles generales los conforman la estructura, políticas y procedimientos que se aplican a las TIC de la entidad y que contribuyen a asegurar su correcta operatividad. Los principales controles deben establecerse en:

- *Sistemas de seguridad de planificación y gestión de la entidad en los cuales los controles de los sistemas de información deben aplicarse en las secciones de desarrollo, producción y soporte técnico*
- *Segregación de funciones*
- *Controles de acceso general, es decir, seguridad física y lógica de los equipos centrales*
- *Continuidad en el servicio.*

02 Para la puesta en funcionamiento de las TIC, la entidad debe diseñar controles en las siguientes etapas:

(i) Definición de los recursos
(ii) Planificación y organización
(iii) Requerimiento y salida de datos o información
(iv) Adquisición e implementación
(v) Servicios y soporte
[...]

03 La segregación de funciones implica que las políticas, procedimientos y estructura organizacional estén establecidos para prevenir que una persona controle los aspectos clave de las operaciones de los sistemas, pudiendo así conducir a acciones no autorizadas u obtener acceso indebido a los recursos de información.

De igual manera, la referida normativa, en sus normas básicas para las actividades de prevención y monitoreo, señala:

"[...]
5. NORMA GENERAL PARA LA SUPERVISIÓN
[...]

5.1 NORMAS BÁSICAS PARA LAS ACTIVIDADES DE PREVENCIÓN Y MONITOREO

5.1.1 Prevención y Monitoreo

El monitoreo de los procesos y operaciones de la entidad debe permitir conocer oportunamente si éstos se realizan de forma adecuada para el logro de sus objetivos y si en el desempeño de las funciones asignadas se adoptan las acciones de prevención, cumplimiento y corrección necesarias para garantizar la idoneidad y calidad de los mismos.

Comentarios:

01 La supervisión constituye un proceso sistemático y permanente de revisión de los procesos y operaciones que lleva a cabo la entidad, sean de gestión, operativas o de control. En su desarrollo intervienen actividades de prevención y monitoreo por cuanto, dada la naturaleza integral del control interno, resulta conveniente vigilar y evaluar sobre la marcha, es decir conforme transcurre la gestión de la entidad, para la adopción de las acciones preventivas o correctivas que oportunamente correspondan.

02 La prevención implica desarrollar y mantener una actitud permanente de cautela e interés por

anticipar, contrarrestar, mitigar y evitar errores, deficiencias, desviaciones y demás situaciones adversas para la entidad. Se fundamenta sobre la base de la observación y análisis de sus procesos y operaciones, efectuados de manera diligente, oportuna y comprometida con la buena marcha institucional. En tal sentido, está estrechamente relacionada y opera como resultado de las actividades de monitoreo."

[...]"

La situación expuesta, respecto a la falta de trazabilidad de los incidentes, imposibilita computar el plazo de atención por parte del Contratista, lo que genera el riesgo de un posible incumplimiento contractual y que no sea posible identificar el cobro de las penalidades incurridas.

Los hechos descritos se originaron debido a falta de gestión de la División de Gestión de Infraestructura Tecnológica (DGIT) para generar los registros de las incidencias en la herramienta ITOP, a efectos de contar con la trazabilidad de la atención por parte del Contratista.

3. OBSERVACIÓN

2.1 EL SUPERVISOR DE LA DIVISIÓN DE GESTIÓN DE INFRAESTRUCTURA TECNOLÓGICA BRINDÓ FACILIDADES AL ESPECIALISTA RESIDENTE, PARA REALIZAR TRABAJOS EN HORARIOS DISTINTOS AL CONTEMPLADO EN LAS BASES INTEGRADAS, REGISTRANDO SU INGRESO EL 31 DE MAYO DE 2024 A LAS 12:18 HORAS, POSTERIOR A LA OCURRENCIA DEL INCIDENTE REGISTRADO A LAS 12:05 HORAS, LIMITANDO CON ELLO LA DETECCIÓN OPORTUNA DE ALERTAS, CON EL PROPÓSITO DE CONTENER LA INTERRUPCIÓN MASIVA DE LOS SISTEMAS INFORMÁTICOS; AFECTANDO LA DISPONIBILIDAD CONTINUA DE LOS SERVICIOS TRIBUTARIOS Y ADUANEROS.

La SUNAT mediante Licitación Pública N.° 0015-2020-SUNAT/8B1200 convocó la contratación para la "Provisión de una solución de nube privada", para atender las demandas de los servicios informáticos de la entidad, resultando ganador de la buena pro la empresa INTEGRIT S.A.C. suscribiendo el 7 de diciembre de 2020, el Contrato N.° 268-2020/SUNAT (**Apéndice N.° 3**) para la etapa de la Prestación Accesoria, dicho servicio contempló la participación de un Especialista Residente por parte del Contratista, con el fin de cumplir un rol específico en la gestión técnica de la plataforma, quien de acuerdo con lo establecido en las Bases Integradas[53] tenía entre sus actividades la de Gestionar la capacidad, configuración y cambios del software de la plataforma de nube privada, debiendo cumplir con un horario laboral de lunes a viernes, de 08:30 a 17:30 horas, en la sede de la Intendencia Nacional de Sistemas de Información[54]; asimismo, que dichas actividades, serían coordinadas y supervisadas por la División de Gestión de Infraestructura Tecnológica (DGIT)[55], recayendo dicha responsabilidad en el colaborador Iván Corzano Correa[56], Supervisor de Cloud.

---

53 ***CLÁUSULA SÉTIMA: PARTES INTEGRANTES DE EL CONTRATO***
El Contrato está conformado por las Bases Integradas, la Oferta ganadora y los documentos derivados del procedimiento de selección que establezcan obligaciones para las partes.
[...]

54 Ubicado en el distrito de San Isidro en la provincial de Lima.

55 Numeral 5.10.2 "Servicio de Soporte" de las Bases Integradas de la Licitación Pública N.° 0015-2020-SUNAT/8B1200. **(Apéndice N.° 4)**

56 Designado mediante Resolución de Superintendencia N.° 000100-2023/SUNAT de 3 de mayo de 2023 en el Cargo de Confianza de Supervisor 1, de la División de Gestión de Infraestructura Tecnológica de la Gerencia de Operaciones y Soporte a Usuarios de la Intendencia Nacional de Sistemas de Información. **(Apéndice N.° 5)**

Es así que, la Comisión Auditora solicitó[57] el reporte del seguimiento de visitas(**Apéndice N.° 6**), del Especialista Residente, del cual se tomó conocimiento que el **31 de mayo de 2024 no registró ingreso** en la sede San Isidro, cabe precisar que en este día a **las 12:05 horas**, se produjo un incidente en la solución de nube privada debido a una contención[58] de recursos, ocasionando la caída de múltiples servicios web soportados por la plataforma de nube privada productiva.

De otra parte, al verificar los registros de conexión vía VPN[59] (**Apéndice N.° 7**) se constató que el 31 de mayo de 2024, el **Especialista Residente registró su ingreso a las 12:18 horas**, es decir estaba realizando sus actividades en lugar distinto al señalado en las Base Integradas, limitando la capacidad de respuesta oportuna, -puesto que no se registró a las 08:30 horas como está establecido contractualmente- ante las alertas emitidas por la plataforma, a efectos de mitigar la ocurrencia del evento crítico, ya que él contaba con acceso a la herramienta vCenter, la cual emite alertas relacionadas con el funcionamiento de la plataforma de nube privada y permite la gestión de sus recursos.

En ese sentido, el Supervisor brindó facilidades al Especialista Residente para que este realice trabajo en lugar y horarios distintos al establecido en el numeral 5.10.2 "SERVICIO DE SOPORTE" de las Bases Integradas de la Licitación Pública N.° 0015-2020-SUNAT/8B1200; situación que limitó la detección oportuna de alertas generando una interrupción masiva de los sistemas informáticos; afectando la disponibilidad continua de los servicios tributarios y aduaneros.

Los hechos advertidos se exponen a continuación:

1. **Del Contrato N.° 268-2020/SUNAT-Prestación de Servicios "Prestación Accesoria"**

   La SUNAT, mediante Licitación Pública N.° 0015-2020-SUNAT/8B1200 convocó la contratación para la "Provisión de una solución de nube privada", para atender las demandas de los servicios informáticos de la entidad, en el que obtuvo la buena pro la empresa INTEGRIT S.A.C. suscribiendo el 7 de diciembre de 2020, el Contrato N.° 268-2020/SUNAT-"Prestación de Servicios para la etapa de Prestación Accesoria, teniendo como plazo de ejecución 1095 días calendario, el cual iniciaría al día siguiente de la conformidad del servicio de instalación y configuración de la nube privada, la cual fue otorgada el 6 de agosto de 2021; en consecuencia, la vigencia inició el 7 de agosto de 2021 y culminó el 5 de agosto de 2024, dicho servicio corresponde las actividades que se detallan a continuación:

Cuadro N.° 7
PRESTACIÓN ACCESORIA

Actividad	*Forma de Pago (%)*
Servicio de mantenimiento preventivo	*20% del monto total contratado de la prestación accesoria, pagado de manera proporcional en forma anual, durante el periodo de ejecución contractual.*

57 a la Oficina de Seguridad y Defensa Nacional mediante Memorándum N.° 0006-2025-OCI-SUNAT/1C0000-AC006 de 24 de setiembre de 2025.

58 En el contexto de tecnología, virtualización o redes, una contención ocurre cuando dos o más procesos, máquinas virtuales o sistemas compiten por los mismos recursos físicos (como CPU, memoria RAM, disco o red), y no hay suficiente capacidad disponible para todos al mismo tiempo.

59 Red Privada Virtual, es un servicio que crea una conexión segura y encriptada entre tu dispositivo e Internet, actuando como un túnel para proteger tus datos y enmascarar tu dirección IP.

Actividad	Forma de Pago (%)
Servicio de Soporte	80% del monto total contratado de la prestación accesoria, pagado de manera proporcional en forma trimestral durante el periodo de ejecución contractual.

Fuente: Bases Integradas de la Licitación Pública N.° 015-2020-SUNAT8B1200
Elaborado por: Comisión Auditora

En ese sentido, respecto al "Servicio de Soporte" el Contratista[60] debía asignar como mínimo un "Especialista Residente" para prestar servicios en las instalaciones de la sede San Isidro, con un horario de labores mínimo de lunes a viernes de 08:30 a 17:30 horas, quien debía realizar entre otras actividades, la de Gestionar la capacidad, la configuración y los cambios del software de la solución de la Nube Privada, teniendo un perfil de carácter operativo y orientado a las tareas de operación diaria; estableciendo que el área técnica responsable **de coordinar y supervisar la labor del Especialista Residente es la División de Gestión de Infraestructura Tecnológica (DGIT),** responsabilidad que recae en el colaborador Iván Corzano Correa[61], Supervisor de Cloud.

De igual forma, se tomó conocimiento[62] que el Especialista Residente, asignado por el Contratista fue el Sr. Moisés Aparicio Toro Martínez, identificado con carné de extranjería N.° 001293926, cuyas labores iniciaron el 7 de agosto de 2021 y culminaron el 5 de agosto de 2024, precisando la DGIT[63] que el citado Especialista cumplía con el horario establecido en las Bases Integradas; esto es, de lunes a viernes de 8:30 a 17:30 horas, de manera presencial, y que los registros de ingreso y salida son efectuados manualmente por el servicio de seguridad de la Institución.

De ahí que, la Comisión Auditora solicitó a la Oficina de Seguridad y Defensa Nacional[64] el reporte de entradas y salidas a las instalaciones del Sr. Moisés Aparicio Toro Martínez, especialista residente a la Intendencia Nacional de Sistemas de Información de la sede San Isidro, correspondiente al periodo del 1 de enero al 5 de agosto de 2024, del cual se identificó que registró ciento cuatro (104) ingresos presenciales, de un total de ciento cuarenta y siete (147)[65] días hábiles.

Ahora bien, entre los diversos periodos en los que el citado Especialista residente no registró ingreso presencial, están los días del 24 de mayo al 3 de junio de 2024; es decir, siete (7) días hábiles consecutivos sin registro en la Sede San Isidro; en ese sentido, la Comisión Auditoria solicitó a la DGIT[66] informar respecto a la ausencia del Sr. Moisés Aparicio Toro Martínez, especialista residente en las instalaciones de la INSI; señalando la DGIT en respuesta alcanzada por el Sr. Iván Corzano, que se brindaron las facilidades a los residentes para realizar labores de manera remota, adjuntando como sustento el reporte de accesos efectuados mediante conexión VPN. Asimismo, precisó que no fue necesario activar medidas de contingencia ni designar personal de reemplazo.

60 Numeral 5.10.2 SERVICIO DE SOPORTE, Capítulo III REQUERIMIENTO, de las Bases Integradas LP N.° 0015-2020-SUNAT/8B1200
61 Designado mediante Resolución de Superintendencia N.° 000100-2023/SUNAT de 3 de mayo de 2023 en el Cargo de Confianza de Supervisor 1, de la División de Gestión de Infraestructura Tecnológica de la Gerencia de Operaciones y Soporte a Usuarios de la Intendencia Nacional de Sistemas de Información.
62 Correo electrónico de 21 de julio de 2025 del Sra .Jery Morales Jibaja en respuesta al Memorándum n.° 000174-2025-SUNAT/1C0000 de 15 de julio de 2025. **(Apéndice N.° 8)**
63 En atención al Correo Electrónico del 25 de agosto de 2025, la DIGIT remitió el Cuestionario de Control Interno suscrito el 27 de agosto de 2025 por el Jefe de la DGIT, Carlos Manuel Posadas Vallejos. **(Apéndice N.° 9)**
64 Memorándum N.° 0006-2025-OCI-SUNAT/1C0000-AC006 de 24 de setiembre de 2025 atendido con el Oficio N.° 000114-2025-SUNAT/801000 de 29 de setiembre de 2025.
65 El total de ciento cuarenta y siete (147) días hábiles se calculó considerando los días de lunes a viernes, que suman cuatrocientos catorce (156), excluyendo los once (9) feriados nacionales y no laborables del sector público.
66 Memorándum N.° 012-2025-OCI-SUNAT/1C0000-AC006 de 16 de octubre de 2025. **(Apéndice N.° 10)**

De la revisión a las conexiones remotas a través de conexión VPN, se identificó que, el 31 de mayo de 2024 el Especialista Residente registró su ingreso a la red institucional a las 12:18:04 horas, utilizando el usuario *"ex_integrit_resi"*, correspondiente al Sr. Moisés Aparicio Toro Martínez, desde el equipo *"LAPTOP-89THTETE"*; fecha en la que, ocurrió la caída masiva de los servicios Web de SUNAT debido a un incidente en la plataforma de nube privada productiva, -cuyo servicio de soporte se encontraba vigente en el marco del Contrato N.° 268-2020/SUNAT- el cual según Informe Técnico N.° 000450-2024-SUNAT/1U5200[67] inició a las 12:05 horas, **comprometiendo la operatividad y continuidad de diversos sistemas informáticos vinculados a diversos procesos tributarios y aduaneros con una duración aproximada de seis (6) horas.**

En ese contexto, se evidenció que, el acceso remoto del Especialista Residente se produjo con posterioridad al inicio del incidente, situación que refleja la ausencia de atención oportuna ante una afectación crítica en el entorno productivo. Cabe agregar que, las acciones realizadas por la DGIT para brindar facilidades para el cambio de modalidad de trabajo y del horario laboral, del Residente Especialista no se encuentran contempladas el numeral 5.10.2 "Servicio de Soporte" de las Bases Integradas de la Licitación Pública N.° 0015-2020-SUNAT/8B1200.

2. Del incidente ocurrido el 31 de mayo de 2024.

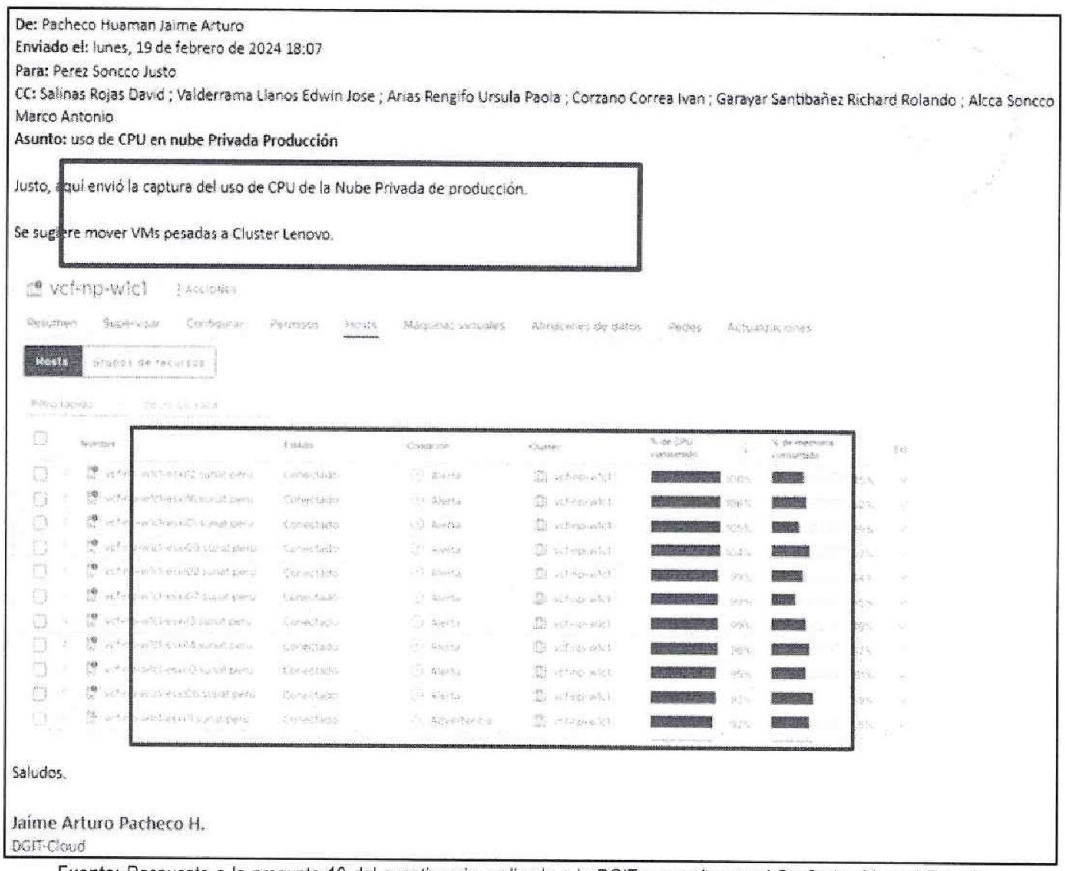
El incidente del 31 de mayo de 2024, se produjo en una fecha crítica para la declaración de las obligaciones tributarias de los contribuyentes, lo que agravó significativamente su impacto[68] operativo e institucional. El Informe Técnico N.° 000450-2024-SUNAT/1U5200 de 16 de agosto de 2024[69], elaborado por la DGIT, señala que la causa raíz del evento fue una falla en el componente de comunicación interna HXC[70] de la solución de Virtualización de Nube Privada, provocada por la saturación de los recursos de procesamiento en el entorno de producción, es decir, por el uso intensivo del CPU y/o memoria en los hosts que soportaban las máquinas virtuales.

Al respecto, la Comisión Auditora[71] solicitó a la DGIT que, en relación con la implementación del componente HCX, precise la fecha de su despliegue, la duración del proceso, el responsable de la ejecución y de la supervisión correspondiente; en ese sentido, la DGIT señaló que el componente HCX fue implementado por el personal técnico del Contratista encargado del proyecto, bajo la supervisión del Administrador de la plataforma[72] junto con los supervisores designados[73]. Asimismo, que dicha herramienta fue desplegada durante la fase de migración de servidores, en el año 2021, como parte integral del servicio contratado. Por lo tanto, al haber sido incorporado el componente HCX como parte de la solución tecnológica; la gestión, mantenimiento y soporte operativo también forman parte de las obligaciones comprendidas en el Servicio de Soporte del Contrato N.° 268-2020/SUNAT.

67 De 16 de agosto de 2024 y suscrito por el jefe de la División de Gestión de Infraestructura Tecnológica. **(Apéndice N.° 11)**
68 De acuerdo con el Oficio n.° 083-2024-JDCCPP/CD de 28 de junio de 2024, remitido por la Junta de Decanos de Colegios de Contadores Públicos del Perú. **(Apéndice N.° 12)**
69 En atención al Memorándum N.° 005-2025-OCI-OCI/1C 0000-AC006, la Gerencia de Operaciones y Soporte de Usuarios -GOSU remitió a la Comisión Auditora el Cuestionario de Control Interno de 27 de agosto de 2025. **(Apéndice N.° 13)**
70 Los componentes HCX (Hybrid Cloud Extension) son módulos especializados dentro de la solución VMware HCX, una plataforma que permite migrar, conectar y extender redes entre diferentes entornos de nube o centros de datos de forma segura y eficiente.
71 Mediante el Memorándum N.° 0005-2025-OCI-SUNAT/1C0000-AC006, de 24 de setiembre de 2025.
72 Sr. Jaime Arturo Pacheco Huamán.
73 En ese entonces el Sr. Warren Roque y, posteriormente, el Sr. Eddy Reinoso.

Por otra parte, se consultó[74] a la DGIT si, antes del incidente ocurrido el 31 de mayo de 2024, se habían identificado alertas relacionadas con la saturación de recursos de hardware en la plataforma de nube privada de producción; **indicando que sí se habían detectado dichas alertas**, por lo que, el Administrador de la plataforma sugirió trasladar las máquinas virtuales de mayor carga a otro clúster, tal como se muestra en la siguiente imagen:

Imagen N.° 6
Notificación del uso del CPU de la Nube Privada de Producción



Fuente: Respuesta a la pregunta 10 del cuestionario realizado a la DGIT y suscrito por el Sr. Carlos Manuel Posadas Vallejos, jefe de la DGIT, el 27 de agosto de 2025.

Como se aprecia en la imagen precedente, en febrero de 2024 ya se registraban alertas en los hosts relacionadas con el alto porcentaje de uso del CPU, las cuales fluctuaban alrededor del 100%.

Por su parte, el supervisor Iván Corzano Correa en el numeral 9 del Acta de Reunión N.° 02-2025-OCI/AC-006[75] (**Apéndice N.° 14**), confirmó que antes del incidente del 31 de mayo de 2024, las alertas relacionadas con recurso de procesamiento del uso de CPU[76] se gestionaban mediante el balanceo de cargas entre las máquinas virtuales y los hosts[77], a fin de mitigar la alta demanda de procesamiento.

---

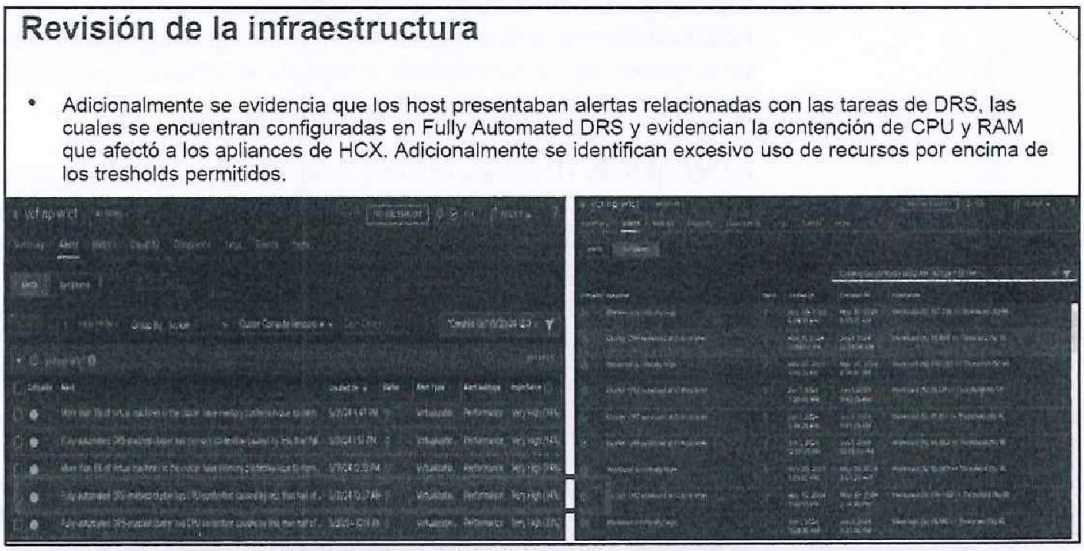
74 En la pregunta 10 del cuestionario realizado a la DGIT y suscrito por el Sr. Carlos Manuel Posadas Vallejos, jefe de la DGIT, el 27 de agosto de 2025.
75 Acta realizada entre personal de la DGIT y la comisión Auditora, suscrita entre el 23 y 26 de setiembre de 2025.
76 Unidad Central de Procesamiento, es el que ejecuta las instrucciones y procesa datos para las tareas del servidor, actuando como el componente principal que maneja las operaciones, cálculos y la carga de trabajo
77 Es un servidor físico con hardware (CPU, RAM, almacenamiento y red) que ejecuta un software de virtualización.

Asimismo, en los numerales 1 y 14 del Acta de Reunión N.° 02-2025-OCI/AC-006, señaló que la herramienta vCenter es utilizada para la gestión y administración de la plataforma de nube privada, y que el Especialista Residente cuenta con credenciales habilitadas que le permiten realizar el seguimiento y la atención de las alertas generadas en dicha herramienta.

Estos hechos demuestran que la DGIT tenía pleno conocimiento de la elevada demanda de procesamiento y la forma como mitigar la demanda de uso de CPU, antes del incidente ocurrido el 31 de mayo de 2024, por lo que, resalta la importancia del cumplimiento de las labores presenciales del Especialista Residente, a fin de atender oportunamente dichas alertas y adoptar las medidas preventivas correspondientes.

Es así que, que el 1 de julio de 2024, el Fabricante del software de la nube privada BROADCOM remitió al Intendente Nacional de Sistemas de Información una presentación denominada "Evidencias caso Soporte HCX 31/Mayo/2024" (**Apéndice N.° 15**), en la que se evidencia que antes de ocurrido el incidente a las 12:05 horas, los Host presentaban alertas relacionadas a niveles críticos de CPU, lo cual se muestra en la siguiente imagen:

Imagen N.° 7
Alertas presentadas antes del Incidente del 31 de mayo de 2024.



Fuente: Presentación "Evidencias caso Soporte HCX 31/Mayo/2024".

Como se aprecia en la imagen precedente, el 31 de mayo de 2024, previo a la caída masiva de los servicios Web de la SUNAT, ya se registraban alertas de niveles críticos de CPU.

Por lo tanto, considerando la alta demanda de procesamiento en la plataforma de nube privada y que el Especialista Residente tenía acceso, mediante vCenter a las alertas generadas; además, de la responsabilidad de gestionar la capacidad, configuración y cambios del software, y de haber cumplido con la modalidad de trabajo y el horario laboral establecido en las Bases Integradas, estaba en la capacidad de identificar oportunamente las alertas críticas por el uso intensivo de CPU y aplicar las acciones correspondientes para mitigar el impacto del incidente del

31 de mayo de 2024 ocurrido a las 12:05 horas; sin embargo, el citado **Especialista registró su ingreso recién a las 12:18 horas**, es decir fuera del horario establecido en las Bases Integradas.

3. Del personal responsable de gestionar el Contrato N.° 268-2020/SUNAT

La Comisión Auditora en el marco del Contrato N.° 268-2020/SUNAT solicitó[78] a la DGIT indicar quienes fueron los responsables directos de la Supervisión de las actividades del especialista residente, Sr. Moisés Toro Martínez; señalando que dichas funciones fueron encargadas, entre otros al Sr. Iván Corzano Correa, Supervisor de Cloud.

Se tomó conocimiento que el Sr. Iván Corzano Correa, fue designado mediante Resolución de Superintendencia N.° 000100-2023/SUNAT[79] de 3 de mayo de 2023 en el cargo de confianza de Supervisor 1 de la División de Gestión de Infraestructura Tecnológica, de la Gerencia de Operaciones y Soporte a Usuarios de la Intendencia Nacional de Sistemas de Información con efectividad a partir del 8 de mayo de 2023; siendo, en esa misma fecha asignado a la Supervisión 7 de la citada subunidad orgánica.

Cabe precisar que, la Supervisión 7 de la DGIT fue creada el 6 de julio de 2020, a solicitud de la Intendencia Nacional de Sistemas de Información, mediante Memorándum Electrónico N.° 00075-2020-1U0000[80] de 17 de junio de 2020 (**Apéndice N.° 16**). Desde su creación, dicha supervisión fue establecida con funciones orientadas al aseguramiento del soporte técnico de Especialistas a través de la gestión de los contratos de soporte de la infraestructura tecnológica y de los servicios implementados sobre la nube privada.

En ese sentido, al momento en que el Sr. Iván Corzano Correa asumió el cargo de Supervisor 1 y fue designado a la Supervisión 7, tenía bajo su responsabilidad funciones, directamente vinculadas con el seguimiento del cumplimiento contractual de las labores realizadas por el Especialista Residente, Sr. Moisés Aparicio Toro Martínez, así como de la gestión operativa de la infraestructura tecnológica de nube privada. Estas actividades resultaban fundamentales para garantizar la continuidad del servicio, la atención oportuna de incidentes y la eficiencia operativa de la plataforma de nube privada productiva.

Por tal motivo, se consultó[81] a la DGIT si el Sr. Iván Corzano Correa tenía conocimiento de que el Especialista Residente, en determinadas oportunidades, desarrollaba sus labores bajo la modalidad de trabajo remoto; al respecto la DGIT señaló que, debido a que el servicio se dio durante el período de la emergencia sanitaria por la COVID19, durante el cual la SUNAT dispuso el trabajo no presencial en las oficinas y que esta medida también tuvo su alcance al personal residente, como es el caso del especialista residente, Sr. Moisés Aparicio Toro Martínez; situación que culminó **el 5 de setiembre de 2022 donde la Institución dispuso el retorno presencial para los supervisores de la DGIT.**

---

78 Mediante Memorándum N.° 0012-2025-OCI-SUNAT/1C0000-AC006 de 16 de octubre de 2025. **(Apéndice N.° 10)**

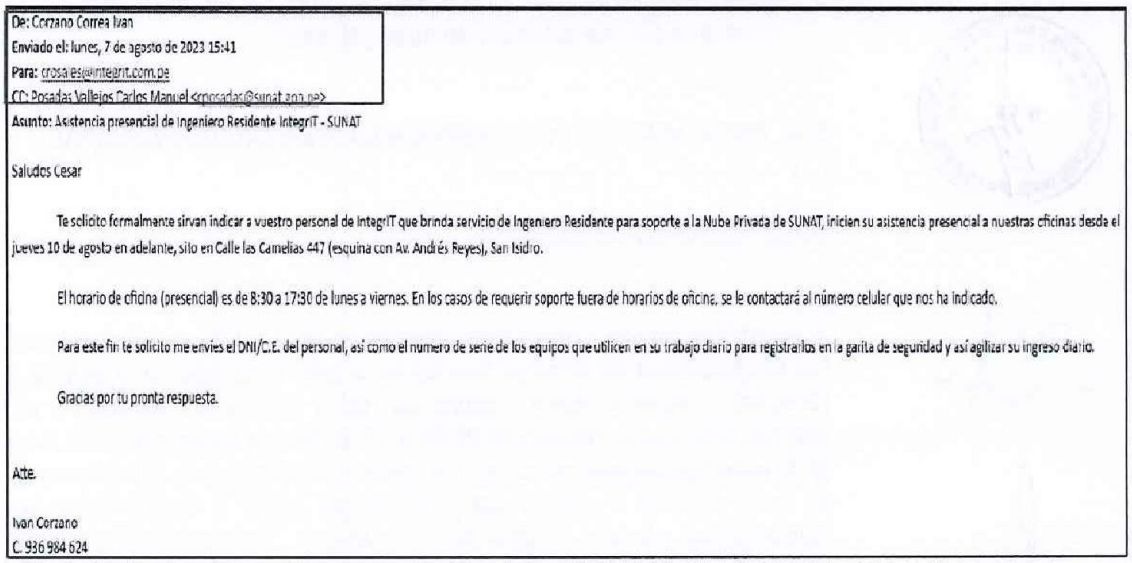
79 Proporcionado a la comisión auditora en respuesta al Memorándum N.° 014-2025-OCI-SUNAT/1C0000-AC006 de 17 de octubre de 2025. **(Apéndice N.° 5)**

80 Proporcionado a la comisión auditora en respuesta al Memorándum N.° 011-2025-OCI-SUNAT/1C0000-AC006 de 13 de octubre de 2025. **(Apéndice N.° 16)**

81 A través del Memorándum N.° 018-2025-OCI-SUNAT/1C0000-AC006 de 31 de octubre de 2025. **(Apéndice N.° 17)**

Asimismo, indicó que, el 8 de mayo de 2023 el Sr. Iván Corzano Correa ingresó a laborar en la SUNAT, y que el 7 de agosto de 2023 comunicó al Contratista que, el Especialista Residente debía cumplir con realizar trabajo presencial, de acuerdo con lo establecido en las Bases Integradas, las cuales disponían un horario laboral de lunes a viernes, de 08:30 a 17:30 horas como mínimo a ser realizado en las instalaciones de la sede San Isidro. En respaldo de dicha comunicación, la DGIT adjuntó la captura que se muestra a continuación:

Imagen N.° 8
Comunicación al Contratista para el retorno presencial del especialista residente.



De: Corzano Correa Ivan
Enviado el: lunes, 7 de agosto de 2023 15:41
Para: crosales@integrit.com.pe
CC: Posadas Vallejos Carlos Manuel <cposadac@sunat.gob.pe>
Asunto: Asistencia presencial de Ingeniero Residente IntegriT - SUNAT

Saludos Cesar

Te solicito formalmante sirvan indicar a vuestro personal de IntegriT que brinda servicio de Ingeniero Residente para soporte a la Nuba Privada de SUNAT, inicien su asistencia presencial a nuestras oficinas desde el jueves 10 de agosto en adelante, sito en Calle las Camelias 447 (esquina con Av. Andrés Reyes), San Isidro.

El horario de oficina (presencial) es de 8:30 a 17:30 de lunes a viernes. En los casos de requerir soporte fuera de horarios de oficina, se le contactará al número celular que nos ha indicado.

Para este fin te solicito me envíes el DNI/C.E. del personal, así como el numero de serie de los equipos que utilicen en su trabajo diario para registrarlos en la garita de seguridad y así agilizar su ingreso diario.

Gracias por tu pronta respuesta.

Atte.

Ivan Corzano
C. 936 984 624

Fuente: Captura de pantalla remitida en respuesta al Memorándum N.° 018-2025-OCI-SUNAT/1C0000-AC006 de 31 de octubre de 2025. **(Apéndice N.° 17)**

Como se aprecia en la imagen precedente, a partir del 10 de agosto de 2023 el Especialista Residente debía iniciar su asistencia a las instalaciones de la INSI, es decir, el Supervisor tomó acciones tres (3) meses después de haber asumido las funciones de la Supervisión 7 de la DGIT. Cabe señalar que, las disposiciones normativas del Gobierno habían prorrogado la vigencia del trabajo remoto para los sectores público y privado, en el marco de la emergencia sanitaria por la COVID-19, hasta el 31 de diciembre de 2022, mediante el Decreto de Urgencia N.° 115-2021 (**Apéndice N.° 18**).

No obstante, SERVIR, en su calidad de ente rector del Sistema Administrativo de Gestión de Recursos Humanos, interpretó que el tercer párrafo de la Única Disposición Complementaria Final del Decreto de Urgencia N.° 055-2021 (**Apéndice N.° 19**) **permitía a las entidades públicas mantener el trabajo remoto durante la vigencia del estado de emergencia sanitaria hasta el 25 de febrero de 2023.**

A pesar de que, al momento del ingreso laboral del Sr. Iván Corzano ya se encontraban vigentes las disposiciones normativas que establecían el retorno al trabajo presencial, y que las Bases Integradas del Contrato N.° 268-2020/SUNAT disponían expresamente que el Especialista Residente debía cumplir labores presenciales, se advirtió que dicho Supervisor demoró tres (3) meses en comunicar al Contratista la obligación del Especialista Residente para el retorno a la modalidad presencial y cumplir con el horario laboral.

Por otra parte, se tomó conocimiento que, durante el año 2024 el Especialista Residente continuó desempeñando sus labores en modalidad remota en 43 días hábiles; no obstante, que, el 7 de agosto de 2023 se requirió al Contratista el cumplimiento del trabajo presencial y el horario laboral, señalado en las Bases Integradas; por consiguiente, se evidenció que entre el 23 de junio y el 3 de julio de 2024, no realizó trabajo presencial, intervalo en el que ocurrió un incidente de alto impacto que afectó los servicios web de la SUNAT el 31 de mayo de 2024 a la 12:05 horas.

Los hechos expuestos transgredieron la normativa que se detalla a continuación:

- **Bases integradas de la Licitación Pública N° 0015-2020-SUNAT/8B1200 "Provisión de una solución de nube privada":**

"[...]

5.10. PRESTACIONES ACCESORIAS A LA PRESTACIÓN PRINCIPAL
[...]

5.10.2. SERVICIO DE SOPORTE

[...]
El contratista deberá asignar como mínimo un especialista residente que ***se ubique en las instalaciones de la sede San Isidro u otro local que se le asigne. La Entidad facilitará el espacio físico y punto de red*** *al especialista residente y el* ***horario de labores será como mínimo de 08:30 a 17:30 hrs de lunes a viernes (modalidad 8 x 5)****. El especialista residente deberá ser personal del fabricante del software de la solución de nube privada; o deberá ser personal del postor y deberá tener las siguientes certificaciones oficiales emitidas por el fabricante: "Certificación oficial en virtualización de datacenter" y "Certificación oficial en gestión y/o automatización de nube (cloud) del software de nube ofertado".* (énfasis es agregado)

El especialista residente realizará como mínimo las siguientes actividades:

- *Operación del software ofrecido (incluye despliegue de aplicaciones) que conforma la solución de nube privada, su perfil es operativo y orientado a las tareas de operación diaria.*
- *Personalización de plantillas/templates de acuerdo con la necesidad de la Entidad.*
- *Deberá ayudar a obtener el máximo provecho a las herramientas de software ofrecido de la solución de nube privada.*
- *Gestionar la capacidad de la solución de nube privada mediante la herramienta de monitoreo ofrecida.*
- *Gestionar la configuración y los cambios del software ofrecido que conforma la solución de nube privada.*
- *Gestionar los releases del software ofrecido que conforma la solución de nube privada.*
- *Realización de "Health Checks" y remediación del software ofrecido que conforma la solución de nube privada.*
- *Recomendación de mejoras para la operatividad de la solución de nube privada.*

El área técnica que coordinará y supervisará la labor de especialista residente es la División de Gestión de Infraestructura Tecnológica (DGIT).
[...]."

La situación expuesta limitó la detección oportuna de alertas, afectando la disponibilidad

continua de los servicios tributarios y aduaneros.

Los hechos descritos, se han producido por el accionar contrario a lo establecido en las Bases Integradas que forman parte del Contrato N.° 268-2020/SUNAT por parte del señor Iván Corzano Correa, en su calidad de Supervisor de la División de Gestión de Infraestructura Tecnológica de la Gerencia de Operaciones y Soporte a Usuarios de la Intendencia Nacional de Sistemas de Información, encargado de supervisar la labor del Especialista Residente en el marco del Contrato N.° 268-2020/SUNAT para la etapa de la Prestación Accesoria, al no cautelar el cumplimiento de la modalidad de trabajo y del horario laboral de dicho especialista.

Comentario de la persona comprendidas en los hechos observados.

La persona comprendida en los hechos observados, el señor Iván Corzano Correa presentó sus comentarios y/o aclaraciones mediante documento s/n del 25 de noviembre de 2025, conteniendo documentos de sustento en copia simples, remitidos mediante Correo Electrónico Institucional de SUNAT, conforme se detalla en el **(Apéndice n.° 20)** del Informe de Auditoría.

Evaluación de los comentarios o aclaraciones de la persona comprendida en los hechos

Efectuada la evaluación de los comentarios y aclaraciones y documentos presentados concluyendo que no se desvirtúan los hechos notificados en la Desviación de Cumplimiento. La referida evaluación, la cédula de comunicación y la notificación, forman parte del **Apéndice n.° 20** del presente Informe de Auditoría.

IVÁN CORZANO CORREA, identificado con DNI N.° [redacted] y con Registro SUNAT N.° [redacted] en calidad de Supervisor de la labor del Especialista Residente en el marco del Contrato N.° 268-2020/SUNAT para la etapa de la Prestación Accesoria, designado mediante Resolución de Superintendencia N.° 000100-2023/SUNAT de 3 de mayo de 2023 en el Cargo de Confianza de Supervisor 1, asignado a la Supervisión 7, de la División de Gestión de Infraestructura Tecnológica de la Gerencia de Operaciones y Soporte a Usuarios de la Intendencia Nacional de Sistemas de Información, correspondiente al período de gestión del 8 de mayo de 2023 al 5 de agosto de 2024 **(Apéndice n.° 21)**; notificado mediante Cédula de Notificación n.° 001-2025-OCI-SUNAT/1C0000-AC006 del 14 de noviembre de 2025, alcanzó sus comentarios y aclaraciones mediante documento s/n de 25 de noviembre de 2025, conteniendo documentos de sustento en copias simples, remitidos por Correo Electrónico Institucional de SUNAT **(Apéndice n.° 20)**.

De la evaluación realizada cuyo desarrollo consta en el **Apéndice n.° 20** del Informe de Auditoría, se ha identificado su participación en calidad de Supervisor de la labor del Especialista Residente en el marco del Contrato N.° 268-2020/SUNAT para la etapa de la Prestación Accesoria, por no cautelar el cumplimiento de la modalidad de trabajo y horario laboral del Especialista Residente.

Puesto que, el señor Iván Corzano Correa, no solo incumplió el deber funcional de supervisar y monitorear permanentemente la ejecución de las prestaciones vinculadas al "Servicio de Soporte" del Contrato N.° 268-2020/SUNAT, deber que se encontraba expresamente previsto en las Bases Integradas de la Licitación Pública N.° 0015-2020-SUNAT/8B1200, las cuales buscan asegurar la presencia y disponibilidad del Especialista Residente durante el horario laboral establecido; sino también, omitió

verificar el cumplimiento del horario laboral, permitiendo que el Especialista Residente el 31 de mayo de 2024 se conectara recién a partir de las 12:18 horas, contraviniendo el horario mínimo obligatorio de 08:30 a 17:30 horas.

Por su parte, inobservó lo establecido en el numeral 5.10.2 "SERVICIO DE SOPORTE" de las Bases Integradas de la Licitación Pública N.° 0015-2020-SUNAT/8B1200 para la Provisión de una solución de nube privada, al brindar facilidades para que el Especialista Residente realice sus labores en modalidad y horarios distintos al establecido contractualmente.

4. ARGUMENTOS JURÍDICOS

Los argumentos jurídicos por presunta responsabilidad administrativa no sujetos a la potestad sancionadora de la Contraloría, de la observación N.°1 **"EL SUPERVISOR DE LA DIVISIÓN DE GESTIÓN DE INFRAESTRUCTURA TECNOLÓGICA BRINDÓ FACILIDADES AL ESPECIALISTA RESIDENTE, PARA REALIZAR TRABAJOS EN HORARIOS DISTINTOS AL CONTEMPLADO EN LAS BASES INTEGRADAS, REGISTRANDO SU INGRESO EL 31 DE MAYO DE 2024 A LAS 12:18 HORAS, POSTERIOR A LA OCURRENCIA DEL INCIDENTE REGISTRADO A LAS 12:05 HORAS, LIMITANDO CON ELLO LA DETECCIÓN OPORTUNA DE ALERTAS, CON EL PROPÓSITO DE CONTENER LA INTERRUPCIÓN MASIVA DE LOS SISTEMAS INFORMÁTICOS; AFECTANDO LA DISPONIBILIDAD CONTINUA DE LOS SERVICIOS TRIBUTARIOS Y ADUANEROS"** están desarrollados en el **Apéndice N.° 2** del presente Informe de Auditoría.

5. IDENTIFICACIÓN DE PERSONAS COMPRENDIDAS EN LOS HECHOS OBSERVADOS

En virtud de la documentación sustentante, la cual se encuentra detallada en los anexos del presente Informe de Auditoría, la persona comprendida en los hechos observados está identificado en el **Apéndice N.° 1.**

6. CONCLUSIONES

Como resultado de la Auditoría de Cumplimiento practicado a la Superintendencia Nacional de Aduanas y de Administración Tributaria, se formulan las conclusiones siguientes:

1. El Supervisor de la División de Gestión de Infraestructura Tecnológica encargado de supervisar la labor del Especialista Residente en el marco del Contrato N.° 268-2020/SUNAT para la etapa de la Prestación Accesoria brindó facilidades para que este, realice trabajos en lugar y horarios distintos al contemplado en las Bases Integradas, advirtiendo de los registros de conexión vía VPN[82] que, el 31 de mayo de 2024, el **Especialista Residente registró su ingreso a las 12:18 horas**, es decir, no se encontraba en la Sede San Isidro y tampoco realizó su registró a las 08:30 horas como está establecido contractualmente-, sino posterior a la ocurrencia del incidente registrado a las **12:05 horas**.

   La situación expuesta trasgredió lo establecido en el numeral 5.10.2 "SERVICIO DE SOPORTE" de las Bases Integradas de la Licitación Pública N.° 0015-2020-SUNAT/8B1200; limitando con ello la detección oportuna de alertas con el propósito de contener la interrupción masiva de los sistemas informáticos; afectando la disponibilidad continua de los servicios tributarios y aduaneros; debido al accionar contrario a lo

[82] Red Privada Virtual, es un servicio que crea una conexión segura y encriptada entre tu dispositivo e Internet, actuando como un túnel para proteger tus datos y enmascarar tu dirección IP.

establecido en las Bases Integradas por parte del señor Iván Corzano Correa, en su calidad de supervisor de la labor del Especialista Residente en el marco del Contrato N.° 268-2020/SUNAT para la etapa de la Prestación Accesoria
(Observación N.° 1)

2. Durante la ejecución de la presente Auditoria de Cumplimiento se presentaron limitaciones por parte de la Intendencia Nacional de Sistemas de Información para acceder a las herramientas informáticas en línea, las cuales están vinculadas al monitoreo de la plataforma tecnológica de la SUNAT y a la gestión de los incidentes informáticos ocurridos en ella; advirtiéndose que en anterior normativa si estaba contemplado el acceso de personal externo a los sistemas de información en producción, no obstante, en la norma actual fue excluida, lo señalado se contrapone a lo establecido el literal m) del artículo 9 de la Ley N.° 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, que faculta a los órganos de control a requerir, conocer y examinar toda la información y documentación relacionada con las operaciones de las entidades bajo el ámbito del control gubernamental.
(Aspecto relevante N.° 1.6.1)

3. Existencia de normativa desactualizada y contradictoria que regula la gestión de prórrogas de vencimientos tributarios ante incidentes informáticos masivos, situación genera el riesgo que ante la ocurrencia de incidentes informáticos masivos, no se cuente con normativa actualizada que permita gestionar de manera oportuna información confiable a los 5contribuyentes respecto a lo sucedido, a efectos de reducir el incremento en las quejas y evitar la afectación del cumplimiento de obligaciones tributarias y aduaneras. Los hechos descritos, se habrían originado debido a que la Intendencia Nacional de Sistemas de Información no gestionó ante las instancias pertinentes como propuesta de mejora la elaboración de un procedimiento estandarizado y actualizado que regule la gestión de comunicados y la emisión de prórrogas ante incidentes informáticos masivos, no atribuibles al contribuyente.
(Deficiencia de Control Interno N.° 2.1)

4. Ausencia de un procedimiento y/o lineamientos que regulen el uso de la cuenta administrativa ROOT en los servidores WEBLOGIC ha generado un uso inapropiado y ausencia de trazabilidad sobre las acciones ejecutadas, situación que compromete y pone en riesgo la integridad, disponibilidad y seguridad de los servicios críticos alojados en dichos servidores. La situación expuesta se habría originado por la falta de seguimiento y supervisión de la Gerencia de Operaciones y Soporte a Usuarios orientados a identificar los vacíos normativos que permitan una mejora continua en la gestión de accesos a los servidores que alojan servicios críticos y que soportan la plataforma vinculada a las obligaciones tributarias de los contribuyentes.
(Deficiencia de Control Interno N.° 2.2)

5. No se ha implementado la configuración de privilegios para el comando utilitario SUDO limitando la trazabilidad de las acciones realizadas por cada Usuario, generando el riesgo en la operatividad de los servicios críticos vinculados a las obligaciones tributarias de los contribuyentes alojados en los servidores, existe el riesgo que nuevamente se produzca el borrado de archivos de configuración; situación que se habría producido por la ausencia de seguimiento y supervisión por parte de la División de Soporte y Operación de Infraestructura Tecnológica (DSOIT) en la gestión de accesos y asignación de permisos que aseguren el uso exclusivo de cuentas personalizadas y privilegiadas mediante SUDO.
(Deficiencia de Control Interno N.° 2.3)

6. Cobertura insuficiente de sensores en la infraestructura tecnológica de la nube privada de la SUNAT, limita la capacidad de los Operadores de Monitoreo para la detección, registro y comunicación oportuna de eventos que provocarían interrupciones en los sistemas informáticos; situación que afectaría la continuidad de los servicios tributarios y aduaneros. Dicha situación se habría originado por la ausencia de seguimiento y supervisión de los Operadores de Monitoreo de la División de Soporte y Operación de Infraestructura Tecnológica (DSOIT) en la gestión de umbrales y sensores destinados a monitorear la capacidad de CPU y memoria de los hosts de la nube privada.
(Deficiencia de Control Interno N.° 2.4)

7. Existencia de Incidentes informáticos cuyos tiempos de reparación superan el plazo máximo establecido contractualmente, sin que la Entidad cuente con registros en la herramienta ITOP que permitan verificar la trazabilidad de la atención; genera el riesgo de que el Contratista no cumpla en dicho plazo con la reparación y servicios de los bienes ofertados, limitando la identificación de penalidades incurridas. Los hechos descritos se originaron debido a falta de gestión de la División de Gestión de Infraestructura Tecnológica (DGIT) para generar los registros de las incidencias en la herramienta ITOP, a efectos de contar con la trazabilidad de la atención por parte del Contratista.
(Deficiencia de Control Interno N.° 2.5)

7. RECOMENDACIONES

Al Superintendente Nacional

1. Realizar las acciones tendentes a fin que el órgano competente efectúe el deslinde de las responsabilidades que corresponda, del funcionario públicos de la división de gestión de infraestructura tecnológica de la gerencia de operaciones y soporte a usuarios de la intendencia nacional de sistemas de información comprendido en los hechos observados del presente informe de auditoría, de acuerdo a las normas que regulan la materia.
(Conclusión N.° 1)

Al Intendente de Intendencia Nacional de Sistemas Información

En uso de las atribuciones conferidas en el literal b) del artículo 15° de la Ley N.°27785, con el propósito de coadyuvar a la mejora de la capacidad y eficiencia de la entidad en la toma de decisiones y en el manejo de sus recursos, se formulan las recomendaciones siguientes:

2. Realizar las coordinaciones con las áreas que correspondan a efectos de establecer mecanismos formales que permitan habilitar el acceso en línea, en modo de consulta y con permisos de emisión de reportes, a las herramientas informáticas necesarias para garantizar la ejecución de los servicios de control, mediante la actualización del Procedimiento de Acceso a los Sistemas Informáticos y la incorporación de disposiciones que regulen el acceso para personal de entidades externas como es el caso de la Contraloría General de la República, en concordancia con las facultades establecidas en la Ley N.° 27785.
(Conclusión N.° 2)

3. Realizar las coordinaciones con las áreas que correspondan para la elaboración de un procedimiento estandarizado y actualizado que regule la gestión de comunicados y la emisión de prórrogas de vencimientos tributarios ante incidentes informáticos no atribuibles al Contribuyente, definiendo criterios de activación, responsables, canales de difusión, plazos, los mecanismos de validación y aprobación correspondientes; y, otros que resulten

necesarios.
(Conclusión N.° 3)

4. Disponer la elaboración de un procedimiento y/o lineamiento que regule el uso de la cuenta administrativa ROOT en los servidores de producción WebLogic que alojan servicios críticos, definiendo responsabilidades, niveles de acceso, restricciones de uso y mecanismos de autenticación y otros que resulten necesarios.
(Conclusión N.° 4)

5. Disponer, que la Gerencia de Operación y Soporte a Usuarios (GOSU) realice las acciones que correspondan para la implementación de la gestión de accesos y la asignación de permisos en los servidores de producción WebLogic mediante la configuración del comando utilitario SUDO y la creación de cuentas individualizadas y privilegiadas, estableciendo reglas de uso y niveles de autorización que permitan identificar las acciones ejecutadas por cada usuario.
(Conclusión N.° 5)

6. Disponer que la División de Soporte y Operación de Infraestructura Tecnológica (DSOIT realice las gestiones pertinentes a fin de Implementar los umbrales y sensores destinados al monitoreo de la capacidad de los recursos de los hosts de la nube privada productiva, asegurando su integración con las herramientas de monitoreo existentes, con el propósito que las alertas sean detectadas y gestionadas de manera oportuna por los Operadores de Monitoreo.
(Conclusión N.° 6)

7. Disponer que la División de Gestión de Infraestructura Tecnológica (DGIT) realice las coordinaciones respectivas para fortalecer la gestión de incidentes informáticos atendidos por los Contratistas mediante el registro obligatorio y oportuno de los tickets de incidentes y de las solicitudes de cambio de partes en la herramienta ITOP, asegurando la trazabilidad de cada atención, a fin de garantizar el cumplimiento de los plazos contractualmente establecidos.
(Conclusión N.° 7)

8. APÉNDICES

Apéndice N.° 1 : Relación de personas comprendidas en la observación.

Apéndice N.° 2 : Argumentos jurídicos por presunta responsabilidad administrativa no sujeta a la potestad sancionadora de la Contraloría.

Apéndice N.° 3 : Copia simple del Contrato N.° 268-2020/SUNAT-Prestación de Servicios "Prestación Accesoria" descargado del siguiente link: https://prod4.seace.gob.pe/contratos/publico/#/detalle/idContrato/tipo/2026196/1

Apéndice N.° 4 : Copia fedateada del Acta de integración de las Bases Integradas de la Licitación Pública N.° 0015-2020-SUNAT/8B1200, se adjunta copia simple del apartado 5.10.2 Servicio de Soporte de las bases integradas.

Apéndice N.° 5 : Copia simple de la Resolución de Superintendencia N.° 000100-2023/SUNAT de 3 de mayo de 2023 de designación en el Cargo de Confianza de Supervisor 1, de la División de Gestión de Infraestructura

Tecnológica de la Gerencia de Operaciones y Soporte a Usuarios de la Intendencia Nacional de Sistemas de Información.

Apéndice N.° 6 : Copia simple del Reporte del seguimiento de visitas del Especialista Residente, Sr. Moisés Aparicio Toro Martínez, en atención a lo solicitado con el Memorándum N.° 006-2025-OLCI-SUNAT/1C0000-AC006.

Apéndice N.° 7 : Copia simple de los Registros de conexión vía VPN del Especialista Residente, Sr. Moisés Aparicio Toro Martínez.

Apéndice N.° 8 : Copia simple de los Correos electrónicos de la Sra. Jery Morales Jibaja en respuesta al Memorándum N.° 000174-2025-SUNAT/1C0000 de 15 de julio de 2025.

Apéndice N.° 9 : Copia simple del Cuestionario de Control Interno suscrito el 27 de agosto de 2025 remitido por el Jefe de la DGIT, Carlos Manuel Posadas Vallejos, en atención al Correo Electrónico del 25 de agosto de 2025.

Apéndice N.° 10: Copia simple del Memorándum N° 012-2025-OCI-SUNAT/1C0000-AC006 de 16 de octubre de 2025 de la comisión auditora a la DGIT, elevado mediante solicitud electrónica N.° 000054-2025-SUNAT/1C0000 de 16 de octubre de 2025; y respuesta mediante seguimiento n.° 2 de la misma solicitud electrónica.

Apéndice N.° 11: Copia simple del Informe Técnico N.° 000450-2024-SUNAT/1U5200 de 16 de agosto de 2024 y suscrito por el jefe de la División de Gestión de Infraestructura Tecnológica. Solicitada mediante correo electrónico de 21 de agosto de 2025, y respuesta mediante correo electrónico de 27 de agosto de 2025, se adjunta cuestionario.

Apéndice N.° 12: Copia simple del Oficio n.° 083-2024-JDCCPP/CD de 28 de junio de 2024, remitido por la Junta de Decanos de Colegios de Contadores Públicos del Perú.

Apéndice N.° 13: Copia simple del Memorándum N.° 0005-2025-OCI-SUNAT/1C0000-AC006, de 24 de setiembre de 2025 de la DGIT, elevada mediante solicitud electrónica N.° 000047-2025-SUNAT/1C0000 de 24 de septiembre de 2025; y respuesta mediante seguimiento n.° 8 de la misma solicitud electrónica.

Apéndice N.° 14: Copia simple del Acta de Reunión N.° 02-2025-OCI/AC-006.

Apéndice N.° 15: Copia simple de la Presentación "Evidencias caso Soporte HCX 31/Mayo/2024.

Apéndice N.° 16: Copia simple del Memorándum Electrónico N.° 00075-2020-1U0000 de 17 de junio de 2020 Proporcionado a la comisión auditora en respuesta al Memorándum N.° 011-2025-OCI-SUNAT/1C0000-AC006 de 13 de octubre de 2025.

Apéndice N.° 17: Copia simple del correo electrónico de 10 de noviembre de 2025, adjunta cuestionario de respuesta; solicita mediante Memorándum N.° 018-2025-OCI-SUNAT/1C0000-AC006 de 31 de octubre de 2025 de la Comisión

Auditora, elevada mediante Solicitud Electrónica N.° 000062-2025-SUNAT/1C0000 DE 31 de octubre de 2025.

Apéndice N.° 18: Copia simple del Decreto de Urgencia N.° 115-202

Apéndice N.° 19: Copia simple de la Opinión de SERVIR del Decreto de Urgencia N.° 055-2021.

Apéndice N.° 20: Copia simple de la Cedula de notificación, los comentarios o aclaraciones presentados por la persona comprendida en la irregularidad y la evaluación de comentarios o aclaraciones elaborada por la Comisión de Control, por cada uno de los involucrados.

Iván Corzano Correa

i) Copia simple de la Cedula de Notificación n.° 001-2025-OCI-SUNAT/1C0000-AC006 de 14 de noviembre de 2025 que adjunta la Desviación de Cumplimiento.
ii) Copia simple de los comentarios y aclaraciones por parte del Sr. Iván Corzano Correa, recibido mediante correo electrónico de 25 de noviembre de 2025.
iii) Evaluación de Comentarios o aclaraciones de la comisión auditora.

Apéndice N.° 21: Documentos que sustentan el presunto incumplimiento funcional:

i) Copia simple de la ficha de trabajador del Sr. Iván Corzano Correa,
ii) Copia simple de la Resolución de Superintendencia N.° 000100-2023/SUNAT de 3 de mayo de 2023 .
iii) Copia simple Reglamento Interno de Trabajo de la SUNAT, aprobado mediante Resolución de Superintendencia n.° 235-2003/SUNAT de 23 de diciembre de 2003 y sus modificatorias.
iv) Copia simple del Memorándum Electrónico N.° 00075-2020-1U0000 de 17 de junio de 2020.

Lima, 1 de diciembre de 2025.

Maria Guadalupe Alva Salazar
Supervisora

Edwin Eder León Díaz
Jefe de Comisión

Sammy Karen Chipana Sánchez
Abogada e Integrante de la Comisión Auditora

Delfín Gutiérrez Llavilla
Integrante de la Comisión Auditora

El jefe del Órgano de Control Institucional de la Superintendencia Nacional de Aduanas y de Administración Tributaria – SUNAT que suscribe el presente informe, ha revisado su contenido y lo hace suyo, procediendo a su aprobación.

Lima, 1 de diciembre de 2025

SUPERINTENDENCIA NACIONAL DE ADUANAS Y DE ADMINISTRACIÓN TRIBUTARIA – SUNAT
Órgano de Control Institucional
JEFE
RICARDO ANDRÉS LEIVA EYZAGUIRRE

Ricardo Andrés Leiva Eyzaguirre
Jefe del Órgano de Control Institucional
de la Superintendencia Nacional de Aduanas y de
Administración Tributaria

Apéndice n.° 1

APÉNDICE N° 1 DEL INFORME DE AUDITORÍA DE CUMPLIMIENTO N.°
RELACIÓN DE PERSONAS COMPRENDIDAS EN LAS OBSERVACIÓN

SUPERINTENDENCIA NACIONAL DE ADUANAS Y DE ADMINISTRACIÓN TRIBUTARIA - Órgano de Control Institucional - JEFE - RICARDO ANDRÉS LENA EYZAGUIRRE

N°	Sumilla del Hecho Observado	Nombres y Apellidos	Documento Nacional de Identidad N°	Cargo Desempeñado	Período de Gestión		Condición de vínculo laboral o contractual	Casilla Electrónica	Dirección domiciliaria	Presunta responsabilidad identificada			
					Desde	Hasta				Civil	Penal	Administrativa funcional	
												Sujeta a la potestad sancionadora de la Contraloría	Entidad
1	El Supervisor de la División de Gestión de Infraestructura Tecnológica brindó facilidades al Especialista Residente, para realizar trabajos en horarios distintos al contemplado en las Bases Integradas, registrando su ingreso el 31 de mayo de 2024 a las 12:18 horas, posterior a la ocurrencia del incidente registrado a las 12:05 horas, limitando con ello la detección oportuna de alertas, con el propósito de contener la interrupción masiva de los sistemas informáticos; afectando la disponibilidad continua de los servicios tributarios y aduaneros	Iván Corzano Correa	[redacted]	Supervisor 1 de la División de Gestión de Infraestructura Tecnológica de la Gerencia de Operaciones y Soporte a Usuarios de la Intendencia Nacional de Sistemas de Información	08/05/2023	05/08/2024	D.L N.° 728	-	[redacted]				X

Firmado electrónicamente por:
RICARDO ANDRES LEIVA EYZAGUIRRE
JEFE OFICINA ESPECIAL
ÓRGANO DE CONTROL INSTITUCIONAL
Fecha y hora: 01/12/2025 20:15

MEMORÁNDUM N.º 000289-2025-SUNAT/1C0000

A : JAVIER EDUARDO FRANCO CASTILLO

SUPERINTENDENCIA NACIONAL

De : RICARDO ANDRES LEIVA EYZAGUIRRE
JEFE OFICINA ESPECIAL
ÓRGANO DE CONTROL INSTITUCIONAL

Asunto : **Remisión de Informe de Auditoría N.° 049-2025-2-3793-AC**

Referencia : a) Memorándum N° 000054-2025-SUNAT/1C0000 de 17 de marzo de 2025

b) Directiva n.° 001-2022-CG/NORM "Auditoría de Cumplimiento" y "Manual de Auditoría de Cumplimiento" aprobada mediante Resolución de Contraloría n.° 001-2022-CG de 7 de enero de 2022 y modificatorias.

Lugar y fecha : Lima, 1 de diciembre de 2025

Me dirijo a usted con relación al documento de la referencia a), mediante el cual se comunicó el inicio de la Auditoría de Cumplimiento a la "Gestión de Incidencias ante fallas técnicas en los Sistemas Informáticos de la SUNAT para el cumplimiento de las obligaciones Tributarias y Aduaneras" correspondiente al período 1 de enero de 2021 al 31 de julio de 2025, en la Superintendencia Nacional de Aduanas y de Administración Tributaria a su cargo.

Sobre el particular, como resultado de la Auditoría de Cumplimiento, se ha emitido el Informe de Auditoría N.° 049-2025-2-3793-AC, que recomienda a su Despacho disponer el inicio del procedimiento administrativo al servidor público involucrado en el hecho observado; asimismo, contiene recomendaciones para la mejora de la gestión, debiendo informar al Órgano Control Institucional, las acciones adoptadas al respecto.

Atentamente,

Atentamente,

RICARDO ANDRES LEIVA EYZAGUIRRE

RLE/eld

Documento: MEMORÁNDUM

Autorizar Lectura

N° Documento:	000289-2025-1C0000
Estado:	FIRMADO
Tipo de Firma:	FIRMA ELECTRÓNICA
Area Emisora:	1C0000 - ÓRGANO DE CONTROL INSTITUCIONAL
Usuario Emisor:	6024 - LEIVA EYZAGUIRRE RICARDO ANDRES
Fecha y Hora Emisión:	01/12/2025 20:15
Area Destino:	100000 - SUPERINTENDENCIA NACIONAL
Usuario Destino:	0530 - FRANCO CASTILLO JAVIER EDUARDO
Asunto:	Remisión de Informe de Auditoría N.° 049-2025-2-3793-AC
Usuario Proyecta:	4408 - GUZMAN RODRIGUEZ CARLOS ELMER
Fecha Proyección:	01/12/2025 16:39

Documento Usuarios en Copia

Seguimientos Conclusión

Expandir Seg. Contraer Seg. Buscar

	Seg.	Fecha y hora	Derivado por	UO deriva	Colaborador destino	UO destino	Instrucciones	Adj.	Copia
+	1	01/12/2025 20:15	6024-LEIVA EYZAGUIRRE RICARDO ANDRES	1C0000	0530-FRANCO CASTILLO JAVIER EDUARDO	100000	DERIVACIÓN AUTOMÁTICA		
+	2	02/12/2025 19:23	0530-FRANCO CASTILLO JAVIER EDUARDO	100000	2250-SALGUERO COLETTI IRIS GIULIANA	1M0000	Estimada Iris, se deriva para las acciones correspondientes. Saludos, Javier.		
+	3	03/12/2025 10:04	2250-SALGUERO COLETTI IRIS GIULIANA	1M0000	3672-QUISPE CORREA ANGULO ALFREDO ALONSO	1M0000	Estimado Arfredo, por favor revisar y proyectar respuesta pertinente.		