CONTRALORÍA
GENERAL DE LA REPÚBLICA DEL PERÚ

CENEPRED

ÓRGANO DE CONTROL INSTITUCIONAL
CENTRO NACIONAL DE ESTIMACIÓN, PREVENCIÓN Y REDUCCIÓN DEL RIESGO DE DESASTRES – CENEPRED

INFORME DE CONTROL ESPECÍFICO N° 007-2025-2-5775-SCE

SERVICIO DE CONTROL ESPECÍFICO A HECHOS CON PRESUNTA IRREGULARIDAD

CENTRO NACIONAL DE ESTIMACIÓN, PREVENCIÓN Y REDUCCIÓN DEL RIESGO DE DESASTRES - CENEPRED

SAN ISIDRO, LIMA, LIMA

"ACONDICIONAMIENTO DEL DATACENTER DE CONTINGENCIA DEL CENEPRED"

PERÍODO: 10 DE OCTUBRE DE 2024 AL 6 DE MARZO DE 2025

TOMO I-I

LIMA – PERÚ

3 DE SETIEMBRE DE 2025

"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año de la recuperación y consolidación de la economía peruana"

0729

0072025257750 0

INFORME DE CONTROL ESPECÍFICO N° 007-2025-2-5775-SCE

"ACONDICIONAMIENTO DEL DATACENTER DE CONTINGENCIA DEL CENEPRED"

ÍNDICE

DENOMINACIÓN	N.° Pág.
I. ANTECEDENTES	3
1. ORIGEN	3
2. OBJETIVO	3
3. MATERIA DE CONTROL Y ALCANCE	3
4. DE LA ENTIDAD O DEPENDENCIA	5
5. NOTIFICACIÓN DEL PLIEGO DE HECHOS	6
II. ARGUMENTOS DEL HECHO ESPECÍFICO PRESUNTAMENTE IRREGULAR	7
FUNCIONARIOS DEL CENEPRED NO GESTIONARON LA INSTALACIÓN DEL DATACENTER DE CONTINGENCIA EN UNA UBICACIÓN GEOGRÁFICA DISTINTA A LA SEDE INSTITUCIONAL, LO QUE OCASIONÓ LA INOPERATIVIDAD DE PROCESOS CRÍTICOS Y MISIONALES, ASÍ COMO DE SISTEMAS DE GESTIÓN ADMINISTRATIVA DURANTE LOS CORTES DE ENERGÍA ELÉCTRICA OCURRIDOS EN MARZO DE 2025.	
III. ARGUMENTOS JURÍDICOS	45
IV. IDENTIFICACIÓN DE PERSONAS INVOLUCRADAS EN EL HECHO ESPECÍFICO PRESUNTAMENTE IRREGULAR	45
V. CONCLUSIÓN	45
VI. RECOMENDACIÓN	46
VII. APÉNDICES	47

CENEPRED V.B.° Jefe OCI (e)

CENEPRED SUPERVISOR ÓRGANO DE CONTROL INSTITUCIONAL

CENEPRED JEFE DE COMISIÓN OCI

CENEPRED ABOGADO OCI

000002

INFORME DE CONTROL ESPECÍFICO N° 007-2025-2-5775-SCE

"ACONDICIONAMIENTO DEL DATACENTER DE CONTINGENCIA DEL CENEPRED"

PERÍODO: 10 DE OCTUBRE DE 2024 AL 6 DE MARZO DE 2025

I. ANTECEDENTES

1. Origen

El Servicio de Control Específico a Hechos con Presunta Irregularidad al Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres (en adelante, Cenepred), corresponde a un servicio de control posterior programado en el Plan Anual de Control del 2025 del Órgano de Control Institucional - OCI del Cenepred, registrado en el Sistema de Control Gubernamental – SCG con la orden de servicio n.° 2-5775-2025-001, iniciado mediante oficio n.° 00140-2025-CENEPRED/OCI de 7 de julio de 2025, en el marco de lo previsto en la Directiva n.° 007-2021-CG/NORM "*Servicio de Control Específico a Hechos con Presunta Irregularidad*", aprobados mediante Resolución de Contraloría n.° 134-2021-CG de 11 de junio de 2021 y modificatorias.

CENEPRED Jefe OCI (e)

2. Objetivo

Determinar si el acondicionamiento del Datacenter de Contingencia del Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres - Cenepred, se efectuó de acuerdo a la normativa aplicable.

CENEPRED SUPERVISOR ÓRGANO DE CONTROL INSTITUCIONAL

3. Materia de Control y Alcance

Materia de Control

La materia de control está relacionada al acondicionamiento del Datacenter de Contingencia del Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres - Cenepred, que fue puesto en marcha el 10 de octubre de 2024[1] en su nueva sede institucional, ubicada en Av. Del Parque Norte 829 – 833, San Isidro, esto es, en el mismo predio donde se encuentra instalado el Datacenter Principal, ello, a pesar que, de acuerdo al Plan de Continuidad Operativa[2], **el Datacenter de Contingencia debe funcionar como un servidor espejo externo a sus instalaciones, es decir, en una ubicación geográfica distinta a su sede institucional**, para asegurar que, ante la materialización de peligros identificados, como el corte de servicios básicos, no se vea comprometida la información crucial para el funcionamiento continuo de las actividades y procesos institucionales.

CENEPRED JEFE DE COMISIÓN OCI

Luego de acondicionados ambos Datacenter, -que albergan servidores para el funcionamiento de las plataformas informáticas misionales y de gestión administrativa-, se presentaron problemas de

CENEPRED ABOGADO OCI

[1] Según carta n.° 01.23-008 de 24 de marzo de 2025 emitida por el Consorcio conformado por Valtom Ingenieros S.A.C. y OLC Ingenieros E.I.R.L., quienes estuvieron a cargo de su instalación, configuración y puesta en marcha.

[2] Numerales 4.1.1 y 5.5.3 del Plan de Continuidad Operativa del CENEPRED v2.0", aprobado con Resolución Jefatural n.° 00005-2024-CENEPRED/J de 12 de enero del 2024.

suministro de energía eléctrica en la nueva sede institucional, ante lo cual, el 14 de febrero de 2025, el Especialista de la Unidad Funcional de Informática[3], informó al Coordinador (e) de dicha Unidad Funcional, que el sistema de monitoreo enviaba mensajes de alerta indicando que el voltaje no estaba siendo suficiente para mantener las operaciones en ambos Datacenter, generando el riesgo que el sistema se apague automáticamente, lo que inhibiría la realización de cualquier operación dentro de los Datacenter; asimismo, señaló que este problema podía resultar en la interrupción total de los servicios y sistemas; acto seguido, el 17 de febrero de 2025, el citado Coordinador (e) de la Unidad Funcional de Informática elevó[4] dicha alerta al jefe de la Oficina de Administración, solicitando dar solución con carácter de urgencia; asimismo, en la misma fecha, le informó[5] que tal como era de su conocimiento, **el Datacenter de Contingencia debía ser instalado en un lugar diferente a la instalación donde funciona el Datacenter Principal**.

Sin embargo, pese a los problemas críticos de voltaje reportados que afectaban a ambos Datacenter, estos continuaron funcionando en la misma sede institucional, sin que se evidencien gestiones para reubicar el Datacenter de Contingencia, hasta que el lunes 3 de marzo de 2025, a las 9:18 horas, se produjo un corte general del suministro de energía eléctrica en toda la sede institucional del Cenepred, prolongándose hasta el 4 de marzo de 2025; seguidamente, el 6 de marzo de 2025, aproximadamente a las 15:20 horas, se presentó nuevamente otra interrupción en el suministro de electricidad, ocasionando la inoperatividad de las plataformas informáticas que soportan los procesos críticos y misionales, como: Sistema de Información para la Gestión del Riesgo de Desastres (Sigrid), Sistema de Información de Monitoreo, Seguimiento y Evaluación (Simse) y Aula Virtual; y sistemas de gestión administrativa como el Sistradoc[6], afectando además el acceso al SIAF[7] y SIGA[8] de la Entidad.

La inoperatividad de las plataformas informáticas antes señaladas, conllevaron a que durante los cortes de energía eléctrica, el Cenepred incumpla la función institucional de *"Establecer mecanismos que faciliten el acceso público a la información geoespacial y los registros administrativos, generados por los organismos públicos técnico-científicos, relacionados con la Gestión del Riesgo de Desastres, coordinando, para tal fin, con los órganos y entidades públicas que corresponda"*, que exige el literal g del artículo 12 de la Ley 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres - Sinagerd; evidenciándose que las acciones encaminadas a la reubicación del Datacenter de Contingencia, se iniciaron luego de los hechos antes expuestos.

Alcance

El servicio de control específico comprende el período del 10 de octubre de 2024 al 6 de marzo de 2025[9], correspondiente a la revisión y análisis de la documentación relativa al hecho con evidencias de presunta irregularidad.

3 Conforme a lo señalado con su informe n.° 00011-2025-CENEPRED-OA-UFI-JCA, de 14 de febrero de 2025.
4 Con informe n.° 00022-2025-CENEPRED-OA/UFI de 17 de febrero de 2025.
5 Con informe n.° 00019-2025-CENEPRED-OA/UFI de 17 de febrero de 2025.
6 Sistema de Trámite Documentario del Cenepred, que facilita la gestión de documentos y trámites internos dentro del CENEPRED, permitiendo a los usuarios acceder, consultar y procesar información relevante para la gestión del riesgo de desastres.
7 SIAF; herramienta informática del Ministerio de Economía y Finanzas (MEF) que brinda soporte a la administración financiera de todas las entidades públicas de los tres niveles de gobierno: Nacional, Regional y Local, en particular, y a la gestión de las finanzas públicas en general. Para registrar todas las operaciones de ingresos y gastos presupuestales, financieras y patrimoniales en el marco de las normas legales que regulan la administración de los recursos públicos.
8 Es el aplicativo informático en el cual se registran la información relacionada con el Sistema Nacional de Abastecimiento (SNA), su uso es obligatorio por parte de las entidades del Sector Público; asimismo, el monitoreo y seguimiento de su implementación se encuentra a cargo de la Dirección General de Abastecimiento (DGA).
9 Fecha de instalación, configuración y puesta en marcha del Datacenter Principal y el de Contingencias en la nueva sede institucional, según lo informado por el Proveedor con Carta n.° 01.23-008 de 24 de marzo de 2025.

4. De la entidad o dependencia

El Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres – Cenepred, es un organismo público ejecutor adscrito al Ministerio de Defensa[10], constituye el pliego presupuestal 025, conforma el Sistema Nacional de Gestión del Riesgo de Desastres-Sinagerd, con autonomía económica, presupuestal y administrativa de acuerdo a la Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres, Ley n.° 29664 y de conformidad al Reglamento de Organización y Funciones.

Es responsable técnico de coordinar, facilitar y supervisar la formulación e implementación de la Política Nacional y el Plan Nacional de Gestión del Riesgo de Desastres en los procesos de estimación, prevención y reducción del riesgo, así como de reconstrucción. Tiene dentro de sus principales funciones[11] establecer mecanismos que faciliten el acceso público a la información geoespacial y los registros administrativos, generados por los organismos públicos técnico-científicos vinculados con la Gestión del Riesgo de Desastres coordinando con los órganos y entidades públicas que correspondan.

Para el cumplimiento de sus funciones, cuenta con el **Sistema de Información para la Gestión del Riesgo de Desastres (en adelante, Sigrid) que es una plataforma tecnológica geoespacial en línea para consultar, compartir, analizar y monitorear información relacionada con peligros, vulnerabilidades y riesgos asociados a fenómenos naturales, así como información territorial a nivel nacional.** El Sigrid permite a los usuarios acceder a mapas y datos sobre peligros geológicos, vulnerabilidad de la población, proyectos de inversión pública y más, está dirigido al personal vinculado a la gestión del riesgo de desastres en las entidades de gobierno nacional, regional y local, a los evaluadores de riesgo, a los analistas y planificadores del territorio nacional, entre otros.

También, cuenta con el Sistema de Información de Monitoreo, Seguimiento y Evaluación (en adelante, Simse), que es una herramienta informática que permite gestionar y monitorear la implementación de la Política y el Plan Nacional de Gestión del Riesgo de Desastres - Planagerd, en los tres niveles de gobierno. El Simse, recaba información de las encuestas en línea, permite conocer el directorio nacional en GRD[12], descargar documentación relacionada a la GRD y visualizar los escenarios de riesgo a través de mapas Interactivos.

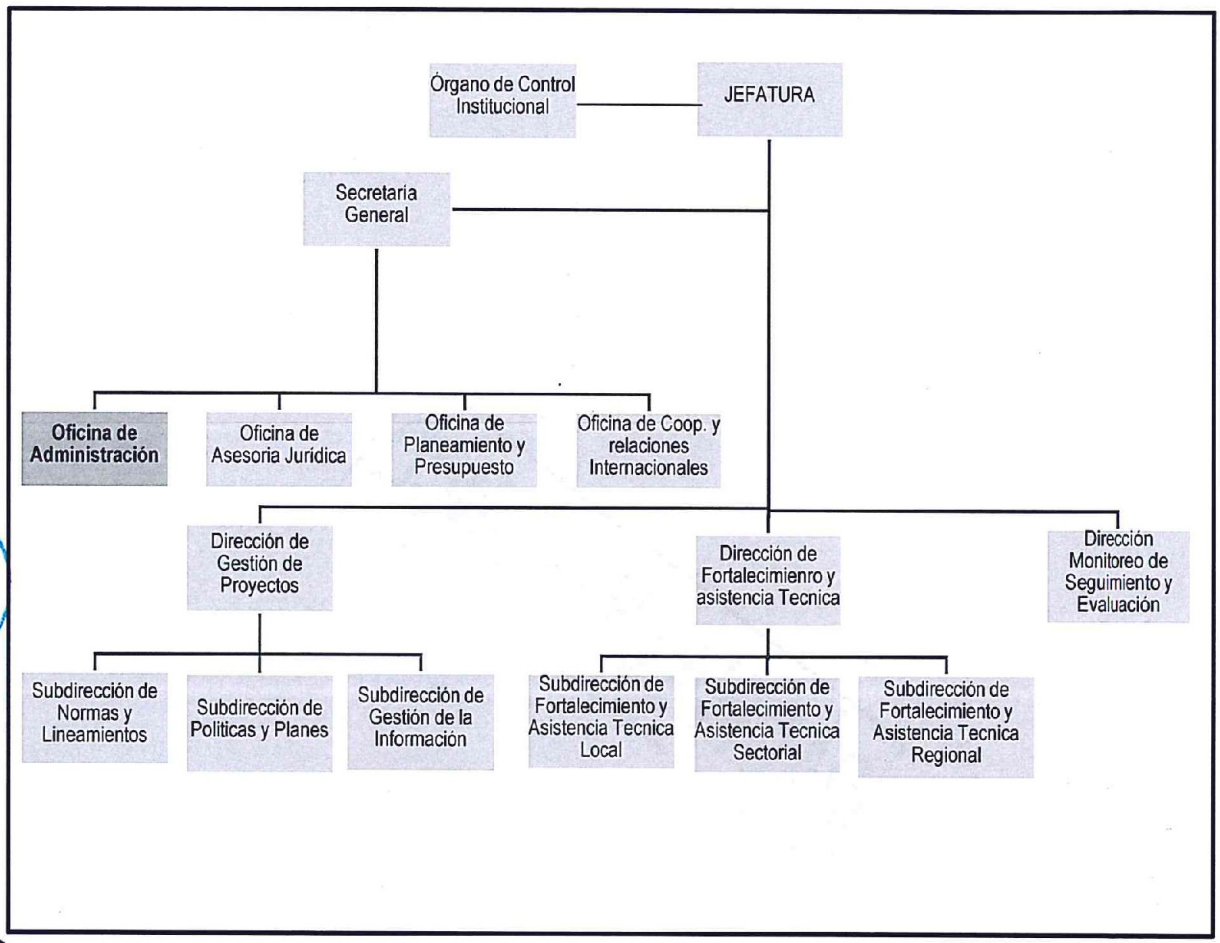
El Cenepred está conformado por órganos de alta dirección, órganos de control institucional, órganos de asesoramiento, órganos de apoyo y órganos de línea, según la estructura orgánica establecida por el Decreto Supremo n.° 104-2012-PCM de 18 de octubre de 2012.

La Oficina General de Administración del Cenepred es el órgano de apoyo encargado de realizar la gestión de recursos humanos, económicos-financieros, logísticos, los servicios generales, así como, la ejecución presupuestal y la gestión patrimonial de la institución. Tiene también a su cargo la provisión de servicios de soporte de tecnologías de información y comunicaciones, administración documentaria y archivo central de la institución depende directamente de la Secretaría General y mantiene coordinación con los demás órganos de la Entidad.

10 Mediante el Decreto Supremo n.° 018-2017-PCM de 16 de febrero de 2017, se aprobó su cambio de adscripción, trasladando formalmente al Cenepred desde la Presidencia del Consejo de Ministros hacia el Ministerio de Defensa
11 Literal g del artículo 12 de la Ley n.° 29664
12 Gestión de Riesgo de Desastres

A continuación, se muestra la estructura orgánica grafica del Cenepred:

Imagen n.° 1
Organigrama del Cenepred



Fuente: Organigrama del Cenepred aprobado mediante Decreto Supremo n.° 104-2012-PCM de 18 de octubre de 2012.
Elaborado por: Comisión de Control

5. Notificación del Pliego de Hechos

En aplicación del numeral 7.30 de las Normas Generales de Control Gubernamental, aprobadas con Resolución de Contraloría n.° 295-2021-CG y modificatorias, la Directiva n.° 007-2021-CG/NORM "Servicio de Control Específico a Hechos con Presunta Irregularidad" aprobada con Resolución de Contraloría n.° 134-2021-CG de 11 de junio de 2021 y modificatorias, así como al marco normativo que regula la notificación electrónica emitida por la Contraloría, se cumplió con el procedimiento de notificación del Pliego de Hechos a las personas comprendidas en los hechos con evidencias de presunta irregularidad a fin que formulen sus comentarios o aclaraciones.

II. ARGUMENTOS DEL HECHO ESPECÍFICO PRESUNTAMENTE IRREGULAR

FUNCIONARIOS DEL CENEPRED NO GESTIONARON LA INSTALACIÓN DEL DATACENTER DE CONTINGENCIA EN UNA UBICACIÓN GEOGRÁFICA DISTINTA A LA SEDE INSTITUCIONAL, LO QUE OCASIONÓ LA INOPERATIVIDAD DE PROCESOS CRÍTICOS Y MISIONALES, ASÍ COMO DE SISTEMAS DE GESTIÓN ADMINISTRATIVA DURANTE LOS CORTES DE ENERGÍA ELÉCTRICA OCURRIDOS EN MARZO DE 2025.

De la revisión de la documentación proporcionada por la Entidad, se evidenció que el Datacenter de Contingencia fue acondicionado e instalado en la nueva sede institucional[13] ubicada en la avenida Del Parque Norte n.º 829 – 833, distrito de San Isidro, inobservando lo dispuesto por la normativa aplicable, toda vez que, no se gestionó su implementación en una ubicación geográfica distinta a la del Datacenter Principal. Es así que, el lunes 3 de marzo de 2025, a las 9:18 horas, se produjo un corte de suministro de energía eléctrica que afectó a toda la sede del Cenepred, prolongándose hasta el día 4 de marzo del mismo año; seguidamente, el 6 de marzo de 2025, aproximadamente a las 15:20 horas, se registró un segundo corte de electricidad; originando el apagado de ambos Datacenter, y en consecuencia la inoperatividad de las plataformas informáticas que soportan los procesos críticos y misionales, como el Sigrid[14], Simse[15] y Aula Virtual, y de sistemas informáticos de gestión administrativa del Cenepred, como el **Sistradoc**[16], además de afectar el acceso a los sistemas **SIAF** y **SIGA**.

Lo expuesto inobservó lo establecido en el literal g) del artículo 12 de la Ley n.° 29664, Ley del Sistema Nacional de Gestión del Riesgo de Desastres (Sinagerd); los numerales 5.5, 5.6, 5.7 y el numeral 6.1. del "Plan de Continuidad Operativa del Cenepred v2.0"; así como los numeral 5.1, 5.2, 6.1, 7.1, 8.3 y 9.2 de la Directiva n.° 01-2016-CENEPRED/SG/OA "Plan de Contingencia Informático del Cenepred"; concordante con los numerales 6 y 7 de la Directiva n.° 008-2016-CENEPRED/J "Administración y Uso del Sistema de Información para la Gestión del Riesgo de Desastre - Sigrid"; y el numeral 5 de los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de la Entidades Públicas de los tres niveles de gobierno. Aunado a ello se ha inobservado, los numerales 4, 5, 6 de la Normativa Técnica Peruana para la Construcción de Centro de Datos ISO/IEC TS 22237 ETP-ISO/IEC TS 22237-2 2019; concordante con el anexo A y la tabla A de la Norma Técnica Peruana NTP-ISO/IEC 27001: 2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información; así como, el numeral 9 de la Norma Técnica Peruana NTP ISO/IEC 17799 2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información y el artículo 1 de la Resolución de Secretaría de Gobierno y Transformación Digital n.° 003-2023-PCM/SGTD.

Los hechos expuestos ocasionaron la inoperatividad de las plataformas informáticas que soportan los procesos críticos y misionales, como: Sistema de Información para la Gestión del Riesgo de Desastres

[13] Arrendamiento del local a través de la Contratación Directa n.° 003-2024-CENEPRED/OEC "*Servicio de alquiler de local institucional para el CENEPRED*", suscribiéndose el contrato n.° 003-2024-CENEPRED/OA de 5 de agosto de 2024.
[14] Sistema de Información para la Gestión del Riesgo de Desastres (Sigrid).
[15] Sistema de Información de Monitoreo, Seguimiento y Evaluación (Simse).
[16] Sistema de Trámite Documentario del Cenepred, que facilita la gestión de documentos y trámites internos dentro del CENEPRED, permitiendo a los usuarios acceder, consultar y procesar información relevante para la gestión del riesgo de desastres.

– **Sigrid**, Sistema de Información de Monitoreo, Seguimiento y Evaluación – **Simse** y Aula Virtual; así como sistemas de gestión administrativa: Sistradoc[17], SIAF[18], SIGA[19].

Los hechos antes expuestos, se detallan a continuación:

Instalación y acondicionamiento del Datacenter Principal y de Contingencia en la misma ubicación geográfica

Como resultado de la contratación directa n.° 002-2024-CENEPRED-1, correspondiente al "*Mejoramiento de la Plataforma Tecnológica del Sistema de Información para la Gestión del Riesgo de Desastres (Sigrid) ante la ocurrencia de inundaciones y movimientos en masa como consecuencia del probable Fenómeno El Niño 2023-2024*"[20] se contrató al Consorcio Valtom Ingenieros S.A.C. y OLC Ingenieros E.I.R.L, quien se encargó de la instalación y acondicionamiento del Datacenter Principal y de Contingencias.

Posteriormente, mediante la contratación directa n.° 003-2024-CENEPRED/OEC, referida al "*Servicio de alquiler de local institucional para el CENEPRED*", se concretó el arrendamiento de un nuevo predio institucional ubicado en la avenida Del Parque Norte N.° 829-833, urbanización Córpac, distrito de San Isidro, provincia y departamento de Lima. Ello dio lugar a la suscripción del contrato n.° 003-2024-CENEPRED/OA, de 5 de agosto de 2024 **(apéndice n.° 3)**, suscrito entre la jefa de la Oficina de Administración, Zoila Elena Huamán Marky, en representación del Cenepred, y el arrendador[21].

En ese contexto, se procedió al traslado del Datacenter Principal y del Datacenter de Contingencia a la nueva sede institucional. Es decir, ambos fueron ubicados en el mismo predio, sin haberse verificado previamente si las instalaciones estaban en condiciones de soportar la demanda eléctrica requerida, ni gestionarse una ubicación geográfica alterna para el Datacenter de Contingencia. Esta decisión contravino los principios de seguridad y continuidad operativa[22] aplicables a este tipo de instalaciones.

Cabe señalar que, de acuerdo con lo establecido en el numeral "*IV. CARACTERÍSTICAS TÉCNICAS*" del "*CAPÍTULO III REQUERIMIENTO*", correspondiente a las bases de la contratación directa n.° 002-2024-CENEPRED-1 **(apéndice n.° 4)**, se dispuso lo siguiente:

> *"El acondicionamiento, montaje, instalación y puesta en funcionamiento debe estar alineado a los criterios y recomendaciones técnicas específicas para la construcción de centro de datos en el Perú, establecido en la* ***Normativa Técnica Peruana para la Construcción de Centros de Datos ISO/IEC TS 22237****, aprobada mediante Resolución Directoral N.° 030-2019-*

17 Sistema de Trámite Documentario de la Entidad.
18 Sistema Integrado de Administración Financiera; herramienta informática del Ministerio de Economía y Finanzas (MEF) que brinda soporte a la administración financiera de todas las entidades públicas de los tres niveles de gobierno: Nacional, Regional y Local, en particular, y a la gestión de las finanzas públicas en general. Para registrar todas las operaciones de ingresos y gastos presupuestales, financieras y patrimoniales en el marco de las normas legales que regulan la administración de los recursos públicos.
19 Sistema Integrado de Gestión Administrativa; es el aplicativo informático en el cual se registran la información relacionada con el Sistema Nacional de Abastecimiento (SNA), su uso es obligatorio por parte de las entidades del Sector Público; asimismo, el monitoreo y seguimiento de su implementación se encuentra a cargo de la Dirección General de Abastecimiento (DGA).
20 Convocada empleando la causal de "Situación de Emergencia", prevista en el literal b) del artículo 100 del Reglamento de la Ley de Contrataciones del Estado, Ley n.° 30225.
21 Luis Alberto Salazar Tafur
22 Conforme a lo establecido en el numeral 5.6.2 del Plan de Continuidad Operativa del CENEPRED v2.0, numeral 8.3.4 del Plan de Contingencia Informático del Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres – CENEPRED, numeral 5 del ETP-ISO/IEC TS 22237-2 2019, Normativa Técnica Peruana para la Construcción de Centro de Datos ISO/IEC TS 22237, numeral 9.1.4 de la NTP ISO/IEC 17799 2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información entre otros.

INACAL/DN; recomendaciones del fabricante; así como las normas de seguridad aplicables a la implementación de datacenter".

La Especificación Técnica Peruana ETP-ISO/IEC TS 22237-2 Tecnología de la información. Instalaciones e infraestructuras de centro de datos. establece entre otros lo siguiente:

> *"(...)*
> ***4. Conformidad***
> *Para que un centro de datos cumpla con este documento:*
> ***a) su ubicación debe haber sido seleccionada luego de una evaluación del sitio como se requiere en Numeral 5;***
> *(...)*
> ***5.4 Adyacencias***
> ***5.4.1 Requisitos***
> ***Se debe realizar un análisis de riesgos** que, como mínimo, considera la adyacencia a los siguientes ítems*
> *(...)*
> ***f) instalaciones altas e inestables que podrían dañar el centro de datos si estos colapsan;***
> *(...)*
> ***6.4 Servicios públicos***
> ***6.4.1 Requisitos***
> ***La prestación de los servicios públicos externos a las instalaciones debe ser adecuada para la clase disponibilidad prevista del centro de datos**, tal como se define en la ISO/IEC TS 22237-1.*
> *Se debe de recopilar la documentación que permita evaluar el riesgo para la operación del centro de datos derivado de las infraestructuras de servicios públicos (...)".* (Énfasis agregado).

Al respecto, conforme a lo establecido en la normativa citada, **antes de la instalación y acondicionamiento de un centro de datos (Datacenter), debe efectuarse una evaluación técnica del sitio**, con el propósito de verificar su idoneidad y el cumplimiento de los criterios establecidos. Dicha evaluación debe sustentarse en un análisis de riesgos que asegure que la ubicación seleccionada minimice vulnerabilidades y garantice la disponibilidad de servicios críticos redundantes y confiables (energía, telecomunicaciones, agua). Ello permite que el centro de datos no solo cumpla con los requisitos de disponibilidad y seguridad, sino que además resulte **sostenible y resiliente a lo largo de todo su ciclo de vida**.

Sin embargo, en el caso que nos ocupa, no se acreditó la realización de dicha evaluación respecto a la instalación y acondicionamiento del Datacenter Principal y de Contingencia en el nuevo predio alquilado. esta omisión se evidencia en el informe n.° 00011-2025-CENEPRED-OA-UFI-JCA, de 14 de febrero de 2025 **(apéndice n.° 5),** suscrito por el especialista de la Unidad Funcional de Informática, José Luis Codarlupo Alejos, y dirigido al coordinador (e) de dicha unidad[23]. En dicho informe, el especialista advierte sobre problemas de voltaje registrados en los Datacenter instalados en la nueva sede, señalando lo siguiente:

Sin embargo, en el caso que nos ocupa, **no se acreditó la realización de la referida evaluación** respecto de la instalación y acondicionamiento del Datacenter Principal y de Contingencia en el nuevo predio alquilado. Esta omisión generó problemas críticos que afectaron los Datacenter conforme quedó

[23] José Guillermo Yovera Vilchez

registrado en el informe n.° 00011-2025-CENEPRED-OA-UFI-JCA, de 14 de febrero de 2025 **(apéndice n.° 5),** suscrito por el especialista de la Unidad Funcional de Informática[24], y dirigido al coordinador (e) de dicha unidad. En dicho informe, el especialista advierte sobre **problemas de voltaje** registrados en los Datacenter instalados en la nueva sede, señalando lo siguiente:

> *"(...)* ***se informa sobre un problema crítico que está afectando tanto al Datacenter principal como al Datacenter de contingencia de CENEPRED****. En los últimos días, hemos observado que* ***el voltaje eléctrico en ambos Datacenter no está alcanzando los niveles requeridos para su funcionamiento adecuado****, lo que ha generado alertas constantes en los sistemas de monitoreo.*
>
> ***Situación:***
>
> - *El sistema de monitoreo ha estado enviando mensajes de alerta, los cuales se muestran en la foto que se adjunta como anexo a este informe.* ***Estos mensajes indican que el voltaje no está siendo suficiente para mantener las operaciones en ambos Datacenter.***
> - *Según los técnicos de la empresa OLC Ingenieros, si el voltaje sigue bajando, los Datacenter interpretarán esto como una tensión de bypass anormal. Como consecuencia, el* ***sistema tomará medidas automáticas y procederá a apagarse*** *para evitar daños mayores.*
>
> ***Riesgo:***
>
> - ***Si el sistema se apaga automáticamente, esto inhibirá la realización de cualquier operación dentro de los Datacenter, lo que podría resultar en la interrupción total de los servicios y sistemas dependientes de estas infraestructuras.***
> - *La no disponibilidad de los Datacenter podría generar* ***una gran pérdida económica y operativa para la institución, debido a la interrupción de la operación de servidores y otros servicios críticos.***
>
> ***Recomendaciones:***
>
> - ***Es urgente que se realice una revisión inmediata de la infraestructura eléctrica*** *en ambos Datacenter para asegurar que el voltaje se mantenga dentro de los rangos adecuados para el funcionamiento de los equipos.*
> - *Se debe revisar con la empresa Luz del sur, para que realicen una revisión de la carga de voltaje contratada (...)".* (Énfasis agregado).

El informe advirtió que un eventual apagado automático del sistema impediría cualquier operación en los Datacenter, lo que podría conllevar a la **interrupción total de los servicios críticos de la institución** y significar **pérdidas económicas y operativas considerables;** por lo cual, el especialista recomendó una revisión inmediata de la infraestructura eléctrica y la coordinación con la empresa Luz del Sur para verificar la carga de voltaje contratada.

El referido documento fue elevado al jefe de la Oficina de Administración, Elvis Renzo Revilla Llerena mediante el informe n.° 00022-2025-CENEPRED-OA/UFI, de 17 de febrero de 2025 **(apéndice n.° 6),**

[24] José Luis Codarlupo Alejos

suscrito por el coordinador (e) de la Unidad Funcional de Informática[25], a través del cual solicitó con carácter de urgencia la solución de desperfecto de voltaje eléctrico, señalando lo siguiente:

> *"(...) debido a las alertas constantes en los niveles de sistema de monitoreo del Data Center, se ha detectado que **el voltaje eléctrico no está alcanzando los niveles requeridos para su adecuado funcionamiento, lo que podría ocasionar un gran perjuicio a la institución**.*
>
> *En tal sentido, **solicito con carácter de urgencia se solucione dicho desperfecto a fin de garantizar el normal funcionamiento del este Data Center** (...)".* (Énfasis agregado).

De igual modo, a través del informe n.° 00019-2025-CENEPRED-OA/UFI, también de 17 de febrero de 2025 **(apéndice n.° 7),** el mismo coordinador de la Unidad Funcional de Informática, informó al jefe de la Oficina de Administración sobre la situación del Datacenter de Contingencia, indicando lo siguiente:

> *"(...), **como es de su conocimiento el Data Center de Contingencia debe ser instalado en un lugar diferente a la instalación donde funciona el Data Center principal; en tal sentido, se solicita se realicen las coordinaciones con la Fuerza Aérea del Perú – FAP o el Ejército del Perú – EP, para que puedan alojar nuestro Data Center de Contingencia**. (...)".* (Énfasis agregado).

En ese sentido, se advierte que, **antes de los cortes de energía eléctrica registrados en marzo de 2025**, la Unidad Funcional de Informática ya había reportado problemas críticos de voltaje que afectaban tanto al Datacenter Principal como al de Contingencia, siendo este último instalado en condiciones que no cumplían con la normativa técnica ni con las buenas prácticas internacionales

Asimismo, el coordinador (e) de la Unidad Funcional de Informática, adjuntó como sustento el informe n.° 00005-2025-CENEPRED-OA-UFI-JCA de 10 de febrero de 2025 **(apéndice n.° 8)**, suscrito por el especialista de la Unidad Funcional de Informática, en el que se expone detalladamente el estado situacional del Datacenter de Contingencia y el incumplimiento de las normas ISO y de las buenas prácticas. En dicho documento se precisa que el Datacenter de Contingencia se encuentra ubicado en el primer piso de las instalaciones del Cenepred, lo que representa una ubicación inadecuada desde el punto de vista técnico y normativo.

El informe resalta que la ubicación actual del Datacenter de Contingencia vulnera los criterios establecidos en las normas ISO 27001 y 22301, así como lo dispuesto en la Ley n.° 29783 – Ley de Seguridad y Salud en el Trabajo, señalando, entre otros aspectos, lo siguiente:

> *"(...)*
> ***1.Introducción***
> *El presente informe tiene como objetivo destacar la situación actual del **Datacenter de contingencia** ubicado en el primer piso de las instalaciones de CENEPRED, y la necesidad de adecuarlo a las normativas y buenas prácticas internacionales en cuanto a la ubicación y gestión de estos espacios. Dado el rol de CENEPRED como entidad responsable de la gestión de riesgos, es crucial recordar que, conforme a las **normas ISO y la normatividad peruana**, el equipamiento crítico de los Datacenter debe estar ubicado en lugares adecuados para garantizar la seguridad y disponibilidad de los sistemas ante cualquier contingencia.*
>
> ***2. Normatividad y Buenas Prácticas para la Gestión de un Datacenter de Contingencia***

[25] José Guillermo Yovera Vilchez,

2.1. Normas Internacionales (ISO)

Las **ISO 22301** (Gestión de Continuidad del Negocio) y la **ISO 27001** (Seguridad de la Información) son dos de las principales normas internacionales que abordan las mejores prácticas para la gestión de infraestructuras críticas, incluyendo los **Datacenter de contingencia.**

- **ISO 22301** establece que las **instalaciones de respaldo** deben estar en ubicaciones separadas de las instalaciones principales para **garantizar la continuidad operativa** en caso de desastres. La norma señala que las instalaciones deben contar con acceso restringido, protección contra riesgos ambientales y espacios adecuados para la seguridad física de los equipos.

- **ISO 27001** destaca que los **centros de datos deben estar protegidos contra incendios, inundaciones, y otros riesgos físicos** que puedan afectar la integridad de la infraestructura. Además, enfatiza la importancia de contar con procedimientos de recuperación ante desastres (DRP) y planificación de contingencias.

2.2. Normatividad Peruana

Según la Ley N° 29783 sobre Seguridad y Salud en el Trabajo, que establece la obligación de garantizar un entorno de trabajo seguro, se recomienda que los espacios que alojen equipos críticos estén alejados de áreas de alto riesgo, como aquellos susceptibles a inundaciones o con riesgo de daños estructurales, como es el caso del primer piso de las instalaciones actuales.

3. Problemas Detectados en la Ubicación Actual del Datacenter de Contingencia

Actualmente, el Datacenter de contingencia se encuentra ubicado en el primer piso de las instalaciones de CENEPRED. Esta ubicación presenta los siguientes riesgos:

- **Riesgo de Inundaciones**: La cercanía al nivel de suelo aumenta el riesgo de daños en caso de filtraciones de agua o inundaciones. Además, el primer piso es más vulnerable a daños por desastres naturales, lo que podría comprometer la disponibilidad de los sistemas.
- **Accesibilidad y Seguridad**: En términos de seguridad física, la proximidad a las áreas de acceso principal puede facilitar un acceso no autorizado. La norma ISO 27001 sugiere que los Datacenter deben estar aislados de las zonas de tráfico frecuente.
- **Cumplimiento de Buenas Prácticas**: La ubicación en el primer piso no cumple completamente con las mejores prácticas internacionales, ya que no proporciona el nivel de protección necesario para garantizar la seguridad de los equipos en situaciones de emergencia.

4. Recomendaciones para la Mejora de la Ubicación y Gestión del Datacenter de Contingencia

1. **Reubicación del Datacenter de Contingencia:** De acuerdo con las normas ISO y las recomendaciones de seguridad, se debe **reubicar el Datacenter de contingencia** a una zona elevada o a un segundo nivel dentro de las instalaciones, preferiblemente en una zona alejada de áreas de alto riesgo. Esta acción ayudará a mitigar el riesgo de daños por inundaciones o desastres naturales.
2. **Adecuación de Espacios según Normativa ISO:** La nueva ubicación debe cumplir con los **requisitos de seguridad física**, acceso restringido y protección ambiental especificados en las normativas ISO 27001 y 22301. Esto incluye la instalación de sistemas de protección contra incendios, control de temperatura adecuado y una infraestructura más robusta.

(...)

CENEPRED V°B° Jefe OCI (e)

CENEPRED SUPERVISOR ÓRGANO DE CONTROL INSTITUCIONAL

CENEPRED JEFE DE COMISIÓN OCI

CENEPRED ABOGADO OCI

5. Conclusión

*La ubicación actual del **Datacenter de contingencia** en el primer piso no cumple con las mejores prácticas internacionales ni con las normativas peruanas relacionadas con la **seguridad** y la **continuidad operativa**. Esta situación aumenta el riesgo de **daños por inundaciones** o **desastres naturales** que puedan afectar la disponibilidad de los servicios críticos de CENEPRED.*

*Por lo tanto, se recomienda proceder con la **reubicación del Datacenter de contingencia** a una ubicación más adecuada, que cumpla con los estándares de seguridad física y protección ambiental establecidos por las normativas ISO 27001 y 22301. Si la reubicación dentro de las instalaciones de CENEPRED no es viable, sería pertinente explorar la posibilidad de coordinar con entidades externas que puedan ofrecer espacios adecuados para el alojamiento del Datacenter, garantizando así la **seguridad** y la **continuidad operativa** de los servicios tecnológicos de la institución"*

En dicho informe se recomienda de manera expresa:

1. La reubicación del Datacenter de Contingencia a una zona elevada o a una ubicación externa al predio institucional, en cumplimiento de los estándares internacionales y nacionales.
2. La adecuación del nuevo espacio conforme a los lineamientos de las normas ISO 27001 y 22301, lo que incluye sistemas de protección contra incendios, control de temperatura, infraestructura segura, acceso restringido, entre otros.

Pese a estas advertencias técnicas, y a que ya se había alertado sobre las fallas de voltaje que comprometían el funcionamiento de ambos Datacenters, los funcionarios del Cenepred no adoptaron medidas correctivas respecto a la ubicación del Datacenter de Contingencia.

Cabe resaltar que, a pesar de haberse efectuado una inversión total de S/ 9 598 603,34 (nueve millones quinientos noventa y ocho mil seiscientos tres con 34/100 soles) para la adquisición e instalación de los Datacenter Principal y de Contingencia, no se gestionó el acondicionamiento del Datacenter de Contingencia en una ubicación geográfica alterna, incumpliéndose así los principios de continuidad operativa y gestión de riesgos previstos en la normativa aplicable.

Corte de fluido eléctrico

Posteriormente, el lunes 3 de marzo de 2025, a las 9:18 horas, se produjo un corte general de energía eléctrica en toda la sede institucional del Cenepred, situación que se prolongó hasta el 4 de marzo de 2025. Adicionalmente, el 6 de marzo de 2025, se registró un segundo corte de energía eléctrica, aproximadamente a las 15:20 horas.

Ante estos hechos, el Órgano de Control Institucional OCI requirió información[26] al Titular de la Entidad, siendo atendida mediante el oficio n.° 00290-2025-CENEPRED/SG, del 12 de marzo de 2025 **(apéndice n.° 9)**, emitido por la Secretaría General, el cual adjuntó documentación técnica relevante, cuya información se resume a continuación:

- Informe n.° 00161-2025-CENEPRED/OA/UFL de 7 de marzo de 2025 **(apéndice n.° 10)**, suscrito por el coordinador (e) de la Unidad Funcional de Logística reportó lo siguiente:

[26] Solicitud efectuada mediante oficio n.° 00061-2025-CENEPRED/OCI, de 7 de marzo de 2025

"(...)
II. Descripción de la incidencia

2.1 Corte de energía y diagnóstico preliminar

*a. **La interrupción afectó la totalidad de la sede, comprometiendo temporalmente la estabilidad de los sistemas y el acceso a información crítica.***

La interrupción afectó totalmente el funcionamiento de los equipos eléctricos y electrónicos (centros de datos, servidores y periféricos, equipos computacionales equipos de aire acondicionado) para el desarrollo de las actividades funcionales y operativas de todas las áreas y local del CENEPRED.

b. Se identificó preliminarmente que la infraestructura eléctrica asignada por Luz del Sur no estaba dimensionada para soportar la demanda real de 50 kW requerida para el funcionamiento del centro de datos y equipos de aire acondicionado, cuyo máximo uso se viene ejecutando en este primer trimestre de 2025.
(...)
d. Cabe mencionar que, dentro del equipamiento tecnológico se encuentran el centro de datos (principal y secundario), cuyo valor aproximado asciende a 20 millones de soles, equipos cuya integridad es prioritaria y que requieren un suministro eléctrico que garantice su funcionamiento estable y continuo. (...)". (Énfasis agregado).

- Informe n.° 055-2025-CENEPRED/DGP/SGI de 11 de marzo de 2025 **(apéndice n.° 11)**, suscrito por el subdirector de Gestión de la Información y remitido mediante el informe n.° 00030-2025-CENEPRED/DGP de 11 de marzo de 2025 **(apéndice n.° 12)**, del subdirector de la Gestión de Información señala lo siguiente:

*"(...) **El SIGRID es una plataforma tecnológica web, que se encuentra alojada en varias máquinas virtuales dentro del data center; al no contar los data center con energía, no es posible que el SIGRID esté en funcionamiento**. Por otra parte, para su conectividad y disponibilidad al usuario externo, es un requisito contar con el acceso a internet, el cual es una infraestructura que se basa en dispositivos de red que funcionan con fluido eléctrico.*

Por lo señalado, el servicio SIGRID no estuvo operativo en las fechas señaladas.
(...)
***Como se señala en la respuesta de la pregunta 6, al estar inoperativo el servicio SIGRID, los usuarios no pueden acceder y utilizarla** (...)".* (Énfasis agregado).

- Del mismo modo, el director de Monitoreo, Seguimiento y Evaluación, a través del informe n.° 00035-2025-CENEPRED/DIMSE de 11 de marzo de 2025 **(apéndice n.° 13),** adjuntó el informe técnico n.° 0007-2025-CENEPRED/DIMSE/MARA de 10 de marzo de 2025 **(apéndice n.° 14),** suscrito por el especialista en Informática de la DIMSE, quien reportó el siguiente análisis:

"(...)
II ANÁLISIS

- *El 03 de marzo de 2025 el fluido eléctrico se cortó aproximadamente a las 9:00 am **provocando que los equipos informáticos de DIMSE y los servicios que usa (internet, acceso al SIMSE que se encuentre instalado en el data center, acceso a información compartida, etc.) sean interrumpidos. El servicio eléctrico se restauró de manera***

inestable y limitada entre las 4pm y 5pm sin acceso a los servicios informáticos. *El personal de DIMSE se retiró a partir del mediodía.*

- *El 04 de marzo de 2025, el fluido eléctrico fue inestable, cortándose nuevamente aproximadamente a las 9:00 am,* ***provocando que los equipos informáticos de DIMSE y los servicios que usa (internet, acceso al SIMSE que se encuentre instalado en el data center, acceso a información compartida, etc.) sean interrumpidos****. A partir de las 11:40 am se restauró parcialmente el servicio eléctrico con accesos a los servicios informáticos de* ***manera inestable y aleatorio. El personal del DIMSE se retiró a partir de las 9:30 am*** *aproximadamente.*

- *El 05 de marzo de 2025, el fluido eléctrico fue inestable* ***provocando que los equipos informáticos de DIMSE y los servicios que usa (internet, acceso al SIMSE que se encuentre instalado en el data center, acceso a información compartida, etc.) sean limitados y aleatorios.***

- *El 06 de marzo de 2025, el fluido eléctrico se restauró en horas de la mañana, pero cerca* ***de las 3:20pm se cortó, provocando que los equipos informáticos de DIMSE y los servicios que usa (internet, acceso al SIMSE que se encuentre instalado en el data center, acceso a información compartida, etc.) sean limitados y aleatorios****.*

III. CONCLUSIONES

En horas laborales del 03, 04, 05, y 06 de marzo de 2025, DIMSE experimentó interrupción del servicio eléctrico; impidiendo el acceso normal al SIMSE y a otros servicios informáticos que frecuentemente usa entre los que se encuentran internet y acceso a información compartida.

IV. RECOMENDACIONES

Para evitar futuros cortes, se sugiere el recableado eléctrico de las instalaciones de CENEPRED con instalación de infraestructura que soporte la carga eléctrica necesaria, considerando el equipamiento adicional que se piensa adquirir en los próximos años.
En situaciones similares sería preferible considerar el trabajo remoto (o similar) para proteger personas, equipos y evitar retrasos innecesarios. (...)". (Énfasis agregado).

Por tanto, conforme a lo informado por la Unidad Funcional de Logística se confirmó que el corte de fluido eléctrico ocurrido en la sede institucional afectó la totalidad de las instalaciones comprometiendo temporalmente la estabilidad de los sistemas y el acceso a información crítica. Asimismo, se señaló que la infraestructura eléctrica asignada por la empresa concesionaria Luz del Sur, no se encontraba dimensionada para soportar las operaciones de ambos Datacenter (principal y de contingencia).

A ello se suma lo informado por los directores de la Dirección de Gestión de Procesos (DGP) y la Dirección de Monitoreo, Seguimiento y Evaluación (DIMSE), quienes confirmaron que, como consecuencia directa del corte de energía, no estuvieron operativos los sistemas Sigrid[27], ni el Simse[28], plataformas tecnológicas fundamentales para el cumplimiento de las funciones institucionales.

[27] Sistema de Información para la Gestión del Riesgo de Desastres
[28] Sistema de Información de Monitoreo, Seguimiento y Evaluación

De otro lado, como resultado del requerimiento de información efectuado por el OCI[29], la empresa concesionaria Luz del Sur respondió con documento CHA.0760860.2025[30] de 26 de marzo de 2025 **(apéndice n.° 15)**, informó lo siguiente:

> *"(...) el corte de energía eléctrica (internos o externos) en Av. Del Parque Norte 829 - 833 San Isidro. El corte imprevisto de energía se debió a una falla en el cable de la conexión subterránea que abastece al suministro, el cual fue reparado por nuestra cuadrilla de emergencia.*
> *(...)*
> ***El suministro de la referencia tiene asignado la tarifa BT5B con una potencia contratada de 50 kW en horas fuera de punta y 20 kW en horas punta, y de acuerdo a los registros del medidor se observa que viene superando su potencia contratada, llegando inclusive a 80.40 kW en febrero 2025.***
> ***Este hecho pone en peligro la continuidad del servicio eléctrico que les brindamos, generando sobrecarga en nuestras redes o en nuestros clientes.***
> *Por lo antes mencionado, vuestra representada se encuentra incursa en el Art. 89°1 y Art. 90° Inciso b)2 de la Ley de Concesiones Eléctricas. En tal sentido, sírvanse regularizar a la brevedad su situación no superando su potencia contratada, encontrándose Luz del Sur facultada a cortar del servicio eléctrico, de acuerdo a las facultades que nos otorga la Ley de Concesiones Eléctricas (...)".* (Énfasis agregado).

Sobre el particular, se advierte que el **corte del fluido eléctrico** tuvo como causa, según lo informado por Luz del Sur, la **superación reiterada de la potencia contratada por parte del Cenepred**, la cual llegó incluso a **80.40 kW**, excediendo ampliamente el límite permitido. Dicha condición según la opinión técnica vertida en dicho documento pone en riesgo la continuidad del servicio, no solo para el predio arrendado, sino también para la red eléctrica y demás usuarios del servicio.

En consecuencia, se evidencia que los funcionarios del Cenepred no realizaron un análisis técnico previo del local antes de suscribir el contrato de arrendamiento[31], en contravención de lo dispuesto por la Normativa Técnica Peruana para la Construcción de Centros de Datos - ISO/IEC TS 22237-2019[32], que establece como requisito la evaluación de riesgos relacionados con la infraestructura eléctrica, a fin de prevenir afectaciones a la integridad del centro de datos. Pese a ello, se dispuso el traslado de ambos Datacenter al nuevo predio alquilado, sin prever la instalación y acondicionamiento del Datacenter de Contingencias en una ubicación geográfica distinta a la del Datacenter principal.

Sede Alterna para el Datacenter de Contingencia

Como resultado de la solicitud información[33] respecto de los requerimientos y/o solicitudes para la implementación de una infraestructura alterna a la sede institucional destinada al acondicionamiento del Datacenter de Contingencia, desde su instalación el 10 de octubre de 2024 hasta el 3 de marzo de 2025 (fecha del corte de energía eléctrica).

La Secretaría General, remitió el oficio n.° 00799-2025-CENEPRED/SG **(apéndice n.° 16)** en el cual, adjuntó el informe n.° 00166-2025-CENEPRED/DGP/SGI ambos de 11 de julio de 2025

29 Se requirió información mediante oficio n.° 00066-2025-CENEPRED/OCI de 10 de marzo de 2025
30 Remitido el 26 de marzo de 2025 por Héctor Herrera Ramírez a través del correo electrónico rherrera@luzdelsur.com.pe
31 Contrato n.° 003-2024-CENEPRED/OA de 5 de agosto de 2024, derivado de la Contratación Directa n.° 003-2024-CENEPRED/OEC "Servicio de alquiler de local institucional para el CENEPRED".
32 aprobado mediante Resolución Directoral n.° 030-2019-INACAL/DN
33 Mediante el memorándum n.° 001-2025-CENEPRED/OCI-SCE de 9 de julio de 2025

respectivamente, **(apéndice n.° 17)**, este último, elaborado y suscrito por el subdirector de Gestión de la Información, quien señaló lo siguiente:

> *"(...)*
> *La Subdirección de Gestión de la Información (SGI) no realizó requerimientos ni solicitudes para la implementación de una infraestructura alterna para el acondicionamiento del Datacenter de Contingencia, debido a que, conforme a la normativa y estructura organizacional vigentes, no se encuentra dentro del ámbito de sus competencias funcionales.* ***La responsabilidad de la gestión, acondicionamiento e implementación de la infraestructura tecnológica del CENEPRED fue asignada a la Unidad Funcional de Informática (UFI), dependiente de la Oficina de Administración,*** *conforme se señala en su resolución de creación* ***(R.J. N°061-2024-CENEPRED/J del 30.05.2024)****. Como antecedente de ello, podemos citar que, vuestro despacho recomendó a la Oficina de Administración asignar la administración del centro de datos al área de soporte informático de la Oficina de Administración (Memorándum N°0185-2024-CENEPRED/DGP).*
>
> *No obstante, en nuestro rol como unidad usuaria de los recursos informáticos e información geoespacial alojada en el datacenter, como la del Sistema de Información para la Gestión del Riesgo de Desastres (SIGRID),* ***esta Subdirección ha impulsado acciones preventivas orientadas a salvaguardar la información y asegurar la continuidad operativa del SIGRID. En ese sentido, se ha solicitado formalmente a la Unidad Funcional de Informática la ejecución de pruebas de recuperación del centro de datos y la actualización del Plan de Contingencia Informático, las cuales a la fecha se encuentran pendientes de atención****. Estas solicitudes, detalladas en el informe técnico* ***N°138-2025-CENEPRED/DGP/SGI, reafirman nuestra posición como área usuaria y parte interesada que vela por la resiliencia de los servicios, diferenciando claramente nuestro rol de supervisión y requerimiento frente al rol ejecutor y de implementación que compete a la UFI. (...)"*** (Énfasis agregado).

Asimismo, se adjuntó el informe técnico n.° 138-2025-CENEPRED/DGP/SGI de 4 de junio de 2025 **(apéndice n.° 18)**, suscrito por los especialistas: Programador GIS[34] y Modelamiento y Simulaciones[35], en el que se precisa que la subgerencia de Gestión de la Información-SGI, ha promovido acciones preventivas y correctivas orientadas a garantizar la continuidad operativa y la seguridad de la información, particularmente del Sistema de Información para la Gestión del Riesgo de Desastres (Sigrid). Entre dichas acciones, se detallan las siguientes solicitudes dirigidas a la UFI:

> *"(...)*
> *1.2. Con Memorándum N°008-2025-CENEPRED/DGP/SGI (ref. a), esta Subdirección solicitó al Coordinador de la Unidad Funcional de Informática la actualización del Plan de Contingencia Informático y la ejecución de pruebas de recuperación del centro de datos del CENEPRED.*
> *1.3. Posteriormente, a través del Memorándum N°020-2025-CENEPRED/DGP/SGI (ref. b), se reiteró la solicitud,* ***informando además sobre un posible ataque informático y la necesidad de coordinar la formulación del plan de contingencia del SIGRID. A la fecha, no se ha recibido respuesta formal sobre la programación y ejecución de las pruebas de recuperación ni sobre la designación de personal para la formulación del plan de contingencia del SIGRID.***
>
> *1.4. El Informe N° 013-2025-CENEPRED-DGP-SGI/CLV (ref. c), elaborado por el Ing. Carlos Lara Velásquez,* ***analiza la responsabilidad de la UFI en el aseguramiento de la***

[34] Carlos Lara Velásquez
[35] René Huamani Aguilar

infraestructura informática y protección de datos en plataformas críticas como el SIGRID, concluyendo que la UFI tiene entre sus funciones específicas el soporte, administración y seguridad de los sistemas y bases de datos del CENEPRED.

1.5. Mediante Memorándum Múltiple N° 00033-2025-CENEPRED/SG (ref. d), la Secretaría General comunicó a las unidades orgánicas del CENEPRED, la aprobación del Plan de Acción Anual 2025, que incluye medidas de control. Específicamente, se ha establecido la medida de control: "Elaboración de protocolos de contingencia para el restablecimiento del servicio Sigrid y cronograma de simulaciones de contingencias (min. 2 simulaciones)", la cual debe implementarse en el presente año (...)". (Énfasis agregado).

Además, se indicó que el personal técnico con experiencia en el funcionamiento del Sigrid fue transferido a la UFI[36], por lo que dicho personal podría colaborar con el equipo técnico a fin de facilitar una implementación más eficiente. En ese mismo sentido, mediante memorándum n.° 0185-2024-CENEPRED/DGP de 16 de abril de 2024 **(apéndice n.° 19)**, el director de Gestión de Procesos, manifestó la importancia de asignar la administración del centro de datos al área de soporte informático de la Oficina de Administración, para asegurar una operación fluida y eficiente, así como, mejor coordinación y colaboración entre las diferentes áreas de la organización.

Finalmente, de la revisión de la Resolución Jefatural n.° 061-2024-CENEPRED/J de 30 de mayo de 2024 **(apéndice n.° 20)** se advierte que las funciones asignadas a la UFI comprenden, entre otras:

"(...)

1. *Diseñar, desarrollar e implementar soluciones de tecnología de sistemas y aplicaciones informáticas que soporten los procesos de línea y de gestión del CENEPRED.*
2. *Brindar mantenimiento y soporte técnico al hardware y software de la red informática.*
3. *Administrar y configurar el acceso y salida del servicio de internet.*
4. *Proponer, aplicar y difundir las políticas, normas y procedimientos de su competencia.*
5. *Brindar asesoramiento en el campo de su especialidad.*
6. *Emitir informes técnicos, dar conformidad, y visar documentos relacionados al ámbito de su competencia, así como participar e integrar equipos y/o comisiones de trabajos relaciones a su especialidad o similares.*
7. *Administrar la infraestructura tecnológica y de telecomunicaciones del CENEPRED.*
8. *Administrar las redes, servicios de voz/datos y equipos de información de la institución.*
9. *Administrar la integridad, confiabilidad y seguridad en el acceso y modificación de la base de datos institucional, así como establecer mecanismos de registro histórico de modificaciones, autenticación de los usuarios, auditoría y control de accesos a la base de datos.*
10. *Gestionar la actualización y dar mantenimiento al portal web de la institución y otras plataformas digitales, en coordinación con otros órganos, apoyando las acciones de transparencia y gobierno de datos abiertos.*
11. *Gestionar en coordinación con los órganos y unidades orgánicas las actividades de desarrollo, mantenimiento e implementación de software, a fin de cuidar su integridad y compatibilidad entre ellos y su integración, según corresponda.*
12. *Brindar soporte técnico para el correcto funcionamiento del Sistema Integrado de Gestión Administrativa (SIGA), Sistema Electrónico de Contrataciones del Estado, Sistema Integrado de Administración Financiera (SIAF), Sistema de Gestión Documental, Sistema de Registro de Visitas, Aplicativo Informático para el Registro Centralizado de Planillas y de Datos de los Recursos Humanos del Sector Público, Sistema Informático de Catalogo - Perú Compras y otras de uso obligatorio en las entidades del Estado.*

CENEPRED VºBº Jefe OCI (e)

CENEPRED SUPERVISOR ÓRGANO DE CONTROL INSTITUCIONAL

CENEPRED JEFE DE COMISIÓN OCI

CENEPRED ABOGADO OCI

[36] Unidad Funcional de Informática

13. Otras funciones que le asigne el Jefe de la Oficina de Administración relacionadas con la misión de la unidad funcional o aquellas que les corresponda por norma expresa.

En tal sentido, la Unidad Funcional de Informática dependiente de la Oficina de Administración, es responsable de la administración e implementación de soluciones tecnológicas de sistemas y aplicaciones informáticas que soporten los procesos de línea y de gestión del Cenepred y la Oficina de Administración **de administrar los recursos para el soporte informático,** de comunicaciones y desarrollo de soluciones informáticas para el cumplimiento de las funciones de la entidad[37].

Por otro lado, se solicitó información[38] al jefe de la Oficina de Administración, Elvis Renzo Revilla Llerena a fin que se informe si la Oficina de Administración o la Unidad Funcional de Informática realizaron acciones conducentes a la implementación de una infraestructura alterna a la sede institucional para el Datacenter de Contingencia, desde su instalación en la sede actual el 10 de octubre de 2024, hasta el 3 de marzo de 2025.

Sobre el particular, con memorándum n.° 00621-2025-CENEPRED/OA de 16 de julio de 2025 **(apéndice n.° 21),** el jefe de la Oficina de Administración, dio respuesta adjuntando para tal fin el informe n.° 00108-2025-CENEPRED-OA/UFI de 15 de julio de 2025 **(apéndice n.° 22),** suscrito por el coordinador (e) de la Unidad Funcional de Informática, señalando lo siguiente:

> *"(...) **en el mes de marzo se realizaron coordinaciones con el Jefe de Conida**; sin embargo, no se obtuvo resultados positivos; bajo ese mismo contexto, se tuvo una reunión con el jefe de telemática del Ejercito del Perú, dichas coordinaciones fueron comunicadas mediante el documento de referencia b). Asimismo, mediante el documento de la referencia c), este Centro Nacional, formalizo la solicitud ante Ejército del Perú, quienes brindaron viabilidad para la reubicación del Datacenter de Contingencia de este Centro Nacional, brindándonos el espacio físico en el BIN COM N° 111, ubicado en la ciudad de Piura, mediante el documento de la referencia d). Finalmente, mediante el documento de la referencia e), se solicitó a la Unidad Funcional de Logística, información técnica para el traslado del Datacenter, con la finalidad de continuar con la gestión administrativa para la reubicación. (...)".* (Énfasis agregado).

Asimismo, el coordinador (e) de la Unidad Funcional de Informática adjuntó el informe n.° 00057-2025-CENEPRED-OA/UFI de 21 de abril de 2025 **(apéndice n.° 23),** que señala: *"(...) Durante el presente año, con la finalidad de contar con un data center en otra instalación, **el 10 de marzo, se tuvo una reunión con el jefe de Conida** a fin de llevar nuestro Data Center Alterno a sus instalaciones (...)".* (Énfasis agregado).

En consecuencia, se advierte que, antes del corte de energía eléctrica (3, 4 y 6 de marzo de 2025) **no se realizaron acciones conducentes a la implementación de una infraestructura alterna a la sede institucional para el traslado del Datacenter de Contingencias;** toda vez que, las reuniones con el jefe de Conida[39] se realizaron el 10 de marzo de 2025 según lo manifestado por el coordinador (e) de la Unidad Funcional de Informática.

Cabe precisar que, según lo establecido en la Directiva n.° 008-2016-CENEPRED/J *"Administración y Uso del Sistema de Información para la Gestión del Riesgo de Desastre – Sigrid[40]", la* Oficina de

---

37 Conforme a lo establecido en el literal g), del artículo 21, del Reglamento de Organización y Funciones del Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastre – CENEPRED, aprobado con Decreto Supremo n.° 104-2012-PCM de 18 de octubre de 2012.

38 Con memorándum n.° 002-2025-CENEPRED/OCI-SCE de 9 de julio de 2025.

39 Comisión Nacional de Investigación y Desarrollo Aeroespacial

40 Aprobado con Resolución Jefatural n.° 068-2016-CENEPRED/J de 3 de mayo de 2016.

Administración y el Área de Sistemas está a cargo de administrar los recursos tecnológicos para el soporte informático y de comunicaciones que garanticen la operatividad del SIGRID; además, tiene como funciones mantenerlos operativos conforme se señala a continuación:

> *"(...)*
> ***6. <u>RESPONSABILIDADES</u>***
>
> *Son responsables de su aplicación las siguientes unidades orgánicas del CENEPRED:*
>
> ***6.2. La Oficina de Administración del CENEPRED,** el área de Sistemas, quien **estará a cargo de administrar los recursos tecnológicos para el soporte informático y de comunicaciones que garanticen la operatividad del SIGRID;***
> *(...)*
> ***7.1.3. <u>Oficina de Administración a través del Área de Sistemas</u>***
> ***a)** Mantener operativos los servicios que ofrece el SIGRID.*
> ***b)** Resolver los problemas técnicos que pudieran afectar la operatividad del SIGRID.*
> ***c)** Mantener y optimizar la red dedicada al servicio SIGRID.*
> ***d)** Mantener operativos los servicios de red y comunicaciones (voz, datos e imagen).**"***

<u>Respecto del funcionamiento de los sistemas informáticos misionales y de gestión administrativa</u>

Sistema de Información para la Gestión del Riesgo de Desastres – Sigrid

En relación con el funcionamiento de los servicios informáticos durante el corte de energía eléctrica, como resultado del requerimiento de información[41] efectuado a la Dirección de Gestión de Procesos (DGP), se solicitó el **reporte de usuarios que accedieron al servidor Sigrid**[42],, discriminado por horas correspondientes a los días **3, 4, 5 y 6 de marzo de 2025**, en formato PDF y debidamente firmado.

Sobre el particular, mediante oficio n.° 00450-2025-CENEPRED/SG de 15 de abril de 2025 **(apéndice n.° 23)**, la Secretaría General adjuntó el informe n.° 0093 -2025-CENEPRED/DGP/SGI de 14 de abril de 2025 **(apéndice n.° 25)**, adjuntando el Reporte de acceso al Sigrid **(apéndice n.° 26)**.

De la revisión de dicho reporte se advierte lo siguiente:

- El **3 de marzo de 2025**, a partir de las **10:00 horas**, no se registraron accesos de usuarios hasta las **17:00 horas del 4 de marzo de 2025**.
- Asimismo, el **6 de marzo de 2025**, no se registraron accesos desde las **16:00 horas hasta las 21:00 horas**.

Lo señalado se muestra gráficamente en la imagen siguiente:

41 Con memorándum n.° 0059-2025-CENEPRED/OCI de 11 de abril de 2025
42 Sistema de Información para la Gestión del Riesgo de Desastres

Imagen n.° 1
Reporte de Accesos al Sigrid los días 3, 4, 5 y 6 de marzo de 2025

Horas	Días			
	3/03/2025	4/03/2025	5/03/2025	6/03/2025
0-1	8	0	7	22
1-2	8	0	6	4
2-3	2	0	2	3
3-4	2	0	6	2
4-5	3	0	4	3
5-6	1	0	1	1
6-7	1	0	5	5
7-8	13	0	11	20
8-9	46	0	65	54
9-10	14	0	76	83
10-11	0	0	74	59
11-12	0	0	81	46
12-13	0	0	56	54
13-14	0	0	15	16
14-15	0	0	45	40
15-16	0	0	45	20
16-17	0	p	55	0
17-18	0	79	44	0
18-19	0	47	47	0
19-20	0	18	22	0
20-21	0	24	13	0
21-22	0	20	24	14
22-23	0	24	14	40
23-24	0	15	10	15
TOTAL	98	227	728	501

Fuente: Reporte remitido por la DGP, con informe n.° 00093-2025-CENEPRED/DGP/SGI de 14 de abril de 2025

En tal sentido, conforme a lo informado por la Dirección de Gestión de Procesos (DGP), el Sistema de Información para la Gestión del Riesgo de Desastres (Sigrid), identificado como el proceso crítico misional más relevante de la Entidad, permaneció inoperativo los días 3, 4 y 6 de marzo de 2025, a raíz de los cortes de energía eléctrica; toda vez que tanto el Datacenter Principal como el Datacenter de Contingencia se encontraban fuera apagados.

Sistema de Información de Monitoreo, Seguimiento y Evaluación – Simse

Del mismo modo, como resultado del requerimiento de información efectuado por el Órgano de Control Institucional - OCI[43], la Dirección de Monitoreo, Seguimiento y Evaluación (Dimse) remitió el informe técnico n.° 0007-2025-CENEPRED/DIMSE/MARA de 10 de marzo de 2025 **(apéndice n.° 14)** elaborado y suscrito por el especialista de Informática de la Dimse[44]. En dicho documento informó la **afectación del servicio del SIMSE por falta de fluido eléctrico el 3, 4, 5 y 6 de marzo de 2025**, señalando lo siguiente:

> *"(...)*
> - *El 03 de marzo de 2025 el fluido eléctrico se cortó aproximadamente a las 9:00 am provocando que los equipos informáticos de DIMSE y los servicios que usa (internet, acceso*

[43] Con oficio n.° 00061-2025-CENEPRED/OCI de 7 de marzo de 2025
[44] Miguen Ángel Ruiz Adarmes

al SIMSE que se encuentra instalado en el data center, acceso a información compartida, etc.) sean interrumpidos. *El servicio eléctrico se restauró de manera inestable y limitada entre las 4pm a 5pm* ***sin acceso a los servicios informáticos. El personal de DIMSE se retiró a partir del mediodía.***

- *El 04 de marzo de 2025, el fluido eléctrico fue inestable, cortándose nuevamente aproximadamente a las 9:00 am, provocando que* ***los equipos informáticos de DIMSE y los servicios que usa (internet, acceso al SIMSE que se encuentra instalado en el data center, acceso a información compartida, etc.) sean interrumpidos***. *A partir de las 11:40 am se restauró parcialmente el servicio eléctrico con acceso a los servicios informáticos de manera inestable y aleatorio. El personal de DIMSE se retiró a partir de las 9:30 am aproximadamente.*
- *El 05 de marzo de 2025, el fluido eléctrico fue inestable, provocando que los equipos informáticos de DIMSE y los servicios que usa (internet, acceso al SIMSE que se encuentra instalado en el data center, acceso a información compartida, etc.) sean limitados y aleatorios.*
- *El 06 de marzo de 2025, el fluido eléctrico se restauró en horas de la mañana, pero cerca de 3:20pm se cortó provocando que los equipos informáticos de DIMSE y los servicios que usa (internet, acceso al SIMSE que se encuentra instalado en el data center, acceso a información compartida, etc.) sean limitados y aleatorios.*

(...)

III. CONCLUSIONES

En horas laborales del ***03, 04, 05, y 06 de marzo de 2025, DIMSE experimentó interrupción del servicio eléctrico; impidiendo el acceso normal al SIMSE y a otros*** *servicios informáticos que frecuentemente usa entre los que se encuentran internet y acceso a información compartida (...)".* (Énfasis agregado).

En consecuencia, conforme a lo informado por la Dirección de Monitoreo, Seguimiento y Evaluación – (Dimse) el Sistema de Información de Monitoreo, Seguimiento y Evaluación (Simse) permaneció inoperativo los días 3, 4 y 6 de marzo de 2025 durante el corte de energía eléctrica; toda vez que, ambos Datacenter Principal y de Contingencias se encontraban apagados.

Sistema de Información de Aula Virtual

Como resultado del requerimiento de información efectuado por el Órgano de Control Institucional (OCI)[45], la Dirección de Fortalecimiento y Asistencia Técnica - DIFAT, remitió el reporte de usuarios que accedieron de acuerdo a la base de datos del servidor del aula virtual del Cenepred, discriminado por horas de los días 3, 4, 5 y 6 de marzo de 2025, en formato PDF debidamente firmado.

Sobre el particular, con oficio n.° 00484-2025-CENEPRED/SG **(apéndice n.° 27)**, la Secretaría General trasladó el informe n.° 007-2025-CENEPRED/DIFAT-MASS, ambos de 25 de abril de 2025 **(apéndice n.° 28)**, suscrito por el director de Fortalecimiento y Asistencia Técnica, en atención al requerimiento efectuado por el OCI;

De la revisión y análisis de la información remitida se advierte que el **3 de marzo de 2025** se registraron **catorce (14) ingresos hasta las 9:17 horas**, no volviéndose a registrar accesos a partir del corte de energía eléctrica, conforme se resume en el cuadro siguiente:

[45] con oficio n.° 00061-2025-CENEPRED/OCI de 7 de marzo de 2025

Cuadro n.° 1
Registro de accesos del aula virtual el día 3 de marzo de 2025

Fecha de incidencia	ítem	hora	Nombre y apellido
3/3/2025	1	02:23:06	Jair Antonio Buiza Paitan
	2	02:41:11	Pablo Alberto
	3	02:44:13	Andrés Alexander Sánchez Trujillo
	4	02:49:18	Gustavo Enrique Montufar Solórzano
	5	05:44:18	Suzalhem Marilia Montalvo Huanca
	6	07:18:06	Alejandro Guerrero Conde
	7	07:25:56	Jhon Thomas Ticona Chambi
	8	08:15:35	Rayner Ali Enríquez Gamarra
	9	08:45:42	Gerardo Carbajal Chauca
	10	09:11:02	Arturo Elmer Callohuari Loayza
	11	09:11:48	Dora Isabel Torres Robledo
	12	09:12:40	Dayanna Giraldo Alegre
	13	09:13:38	Nino Salvador Chura Quispe
	14	09:16:24	Arturo Eduardo Meza Aquino

Fuente: Reporte remitido por la Difat, con informe n.° 007-2025-CENEPRED/DIFAT-MASS de 25 de abril de 2025
Elaborado por: Comisión de Control

Respecto del día 4 de marzo de 2025, se registraron dieciséis (16) ingresos desde las 17:45 horas hasta las 23:13 horas, lo que se resume en el cuadro siguiente:

Cuadro n.° 2
Registro de accesos del aula virtual el día 4 de marzo de 2025

Fecha de incidencia	ítem	hora	Nombre y apellido
4/3/2025	1	17:45:10	Javier Noe Lliuyacc Huaman
	2	18:20:00	Carlos Daniel Moreno Camacaro
	3	18:28:59	Jorge Luis Gallegos Meza
	4	18:40:16	Jhielsin Osorio Lanazca
	5	19:50:46	Jorge Alexander Lozada Calero
	6	20:24:52	Rolando Hilario Rada
	7	21:01:24	Yetsabel Gina Alvino Barrientos
	8	21:06:16	Mary Carpio Llica
	9	21:24:06	Herix Clinton Figueroa Diego
	10	21:54:53	Jahaira Janely García Rodriguez
	11	22:01:37	Antonio Espinoza Solorzano
	12	22:15:38	Key Maria Jaqueline Alva Sunción
	13	22:32:01	Lesly Roxana Conde Sosa
	14	22:58:02	Ana Ysabel Polanco Aguilar
	15	23:01:25	Sonia Márquez Pinto
	16	23:13:12	William Guillén Pinto

Fuente: Reporte remitido por la Difat, con informe n.° 007-2025-CENEPRED/DIFAT-MASS de 25 de abril de 2025
Elaborado por: Comisión de Control

Respecto del 6 de marzo de 2025, se registraron treinta y cinco (35) ingresos entre la 1:50 horas y las 22:55 horas; no obstante, se advierte que durante el corte de energía eléctrica no se registraron accesos, específicamente desde las 15:18 hasta las 21:39 horas, conforme se resume en el cuadro siguiente:

Cuadro n.° 3
Registro de accesos del aula virtual el día 6 de marzo de 2025

Fecha de incidencia	ítem	hora	Nombre y apellido
6/3/2025	1	01:50:44	Marlon López Reyes
	2	01:50:50	Arian Marcelo Huaman Coaquira
	3	04:06:41	Josep Luis Antonio Ramos Tixi
	4	08:06:30	Giovana Elizabeth Infante Guerrero
	5	08:32:26	Edgar Jeanpiere Carrion Rodriguez
	6	08:32:30	Evo Alejandro Eloy Larico Flores
	7	09:20:29	Flor Asunciana Reyes Huayac
	8	09:46:27	Gisela Anali Blas Mercado
	9	10:02:08	Yunior Nilton Carrión Alejo
	10	10:05:14	Hamilton Mena Chávez
	11	10:08:58	Miguel Angel Sanchez Suarez
	12	10:15:21	Gary Fernando Ramírez Toledo
	13	10:21:16	Nilo Eloy Quispe Chillihuani
	14	10:32:40	Fabricio Stefano Sihuas Baltodano
	15	10:55:12	Carlos Mauricio Abad Assante
	16	11:19:59	Maikol Justino Pinedo
	17	11:28:12	Wilder Javier De La Cruz Bernilla
	18	11:47:00	Alex Berto Zamora
	19	12:03:56	Johnny Rosales
	20	12:04:05	Esthefany Mollo Torres
	21	12:16:38	Klinton Gibson Asto Azurza
	22	12:25:09	Cristopher Arturo Ramos Velazco
	23	12:30:35	Kelly Aracely Torres Martínez
	24	12:44:58	Oscar Jiménez Pastor
	25	13:01:41	Tommy Deza
	26	13:05:31	Luis Edward Quintana Faya
	27	13:35:23	Marko Condori Carrasco
	28	14:04:34	Jefferson Flores Castro
	29	14:12:03	Pamela Ingrid Guzmán Quispe
	30	14:32:34	Frank Llordy Escalante Cárdenas
	31	14:48:26	Jesus Davis HUaman Macalopu
	32	**15:18:20** ▲	Jean Carlos Chumbe Yapu
	33	**21:39:56** ▼	Julián Claudio Huamaní Díaz
	34	21:42:47	Omar Alexander Davila Diaz
	35	22:59:04	Rosa Salinas

Fuente: Reporte remitido por la Difat, con informe n.° 007-2025-CENEPRED/DIFAT-MASS
Elaborado por: Comisión de Control

En consecuencia, como resultado del análisis de la información proporcionada se corroboró que, los días 3, 4 y 6 de marzo de 2025, no se pudo acceder al aula virtual durante el corte de energía eléctrica; toda vez que tanto el Datacenter Principal como el de Contingencias se encontraban apagados.

Sistemas informáticos de gestión administrativa -Sistradoc

Por otro lado, la comisión de control requirió información[46] a la Coordinación de la Unidad Funcional de Informática lo siguiente:

[46] Mediante memorándum n.° 003-2025-CENEPRED/OCI-SCE de 9 de julio de 2025

"(...) remita el reporte de usuarios que accedieron de acuerdo a la base de datos del servidor SIAF, SIGA y Sistradoc, ***discriminado por horas de los días 3, 4, 5 y 6 de marzo de 2025****, en formato Excel y en PDF debidamente firmado (...)".*

En atención a ello, mediante oficio n.° 00800-2025-CENEPRED/SG de 14 de julio de 2025 **(apéndice n.° 29)**, la Secretaría General otorgó respuesta sustentándolo en los informes n.°s 00162-2025-CENEPRED/OA, 00105-2025-CENEPRED-OA/UFI y 0044-2025-CENEPRED/OA/UFI/JCA de 14, 11 y 10 de julio de 2025 **(apéndices n.°s 30, 31 y 32)**, respectivamente.

Con relación al informe n.° 00162-2025-CENEPRED/OA de 14 de julio de 2025 **(apéndice n.° 30)**, suscrito por el jefe de la oficina de Administración, Elvis Renzo Revilla Llerena, anexó el informe n.° 00105-2025-CENEPRED-OA/UFI de 11 de julio de 2025 **(apéndice n.° 31)**, suscrito por la Unidad Funcional de Informática; a través del cual, el coordinador (e) de la Unidad Funcional de Informática, remite la información solicitada correspondiente a los usuarios del Sistradoc; aunado a ello, adjuntan el informe n.° 00044-2025-CENEPRED/OA/UFI/JCA de 10 de julio de 2025 **(apéndice n.° 32)**, elaborado y suscrito por el especialista de la Unidad Funcional de Informática, en el que se incluyó el reporte de accesos al Sistradoc de los días 3, 4 y 6 de marzo de 2025 **(apéndice n.° 33)** de la revisión a la información proporcionada respecto al Sistradoc, se pudo corroborar que, durante el corte de fluido eléctrico **no se tuvo acceso a dicho sistema de trámite documentario,** conforme se resume en los cuadros a continuación:

Cuadro n.° 4
Registro de accesos del Sistradoc 3 de marzo de 2025

Registro de Usuarios			
n.°	**Hora y fecha**	**Apellido**	**Nombre**
1	3/03/2025 07:50	Becerra Noblecilla	Walter Martin
2	3/03/2025 07:58	Alfaro	Renato
3	3/03/2025 07:59	Tafur Cavides	Javier
4	3/03/2025 08:00	Acosta Farfán	Manuel
5	3/03/2025 08:03	Del Águila Reátegui	Miguel Ángel
6	3/03/2025 08:04	Gómez Mendoza	Eliana Del Rosario
7	3/03/2025 08:06	Gutiérrez Trujillo	Magna Rosa
8	3/03/2025 08:09	Tafur Cavides	Javier
9	3/03/2025 08:13	Aguirre Gonzalo	Oscar Manuel
10	3/03/2025 08:20	Pérez Tijero	Ivone Carolina
11	3/03/2025 08:22	Lescano Diaz	Rosario Odeli
12	3/03/2025 08:23	Caballero Vargas	Jorge Luis
13	3/03/2025 08:23	González Ibáñez	Alicia
14	3/03/2025 08:23	Pautrat Vega	Brenda Giuliana
15	3/03/2025 08:31	Balbín Mendoza	Julio César
16	3/03/2025 08:37	Olortegui Azato	Jarumi
17	3/03/2025 08:38	Lugo Valdiviano	Oswaldo Miguel
18	3/03/2025 08:39	Huarancca Boza	Carlos Miguel
19	3/03/2025 08:40	Jaimes Espinoza	Ena Maria
20	3/03/2025 08:44	Condezo Celis	Mayra Natali
21	3/03/2025 08:45	Becerra Noblecilla	Walter Martin
22	3/03/2025 08:46	Cueva Rovelo	Sheyla Haydee
23	3/03/2025 08:46	Palacios Moreno	Gastón Jean Pierre
24	3/03/2025 08:47	Obregón Acevedo	Chrisna Karina
25	3/03/2025 08:58	Plasencia Amaya	Franklin
26	3/03/2025 08:58	Revilla Llerena	Elvis Renzo
27	3/03/2025 09:00	Obregón Acevedo	Chrisna Karina
28	3/03/2025 09:00	Pillco Valenzuela	Wilber
29	3/03/2025 09:01	Manchego Cáceres	Harold Edward Federico

CENEPRED V°B° Jefe OCI (e)

CENEPRED SUPERVISOR ÓRGANO DE CONTROL INSTITUCIONAL

CENEPRED JEFE DE COMISIÓN OCI

CENEPRED ABOGADO OCI

Registro de Usuarios			
n.°	Hora y fecha	Apellido	Nombre
30	3/03/2025 09:02	Palacios Moreno	Gastón Jean Pierre
31	3/03/2025 09:03	Cenepred	Logistica1
32	3/03/2025 09:05	Cueva Rovelo	Sheyla Haydee
33	3/03/2025 **09:06**	Revilla Llerena	Elvis Renzo

Fuente: Listado de accesos remitido con informe n.° 00044-2025-CENEPRED/OA/UFI/JCA de 10 de julio de 2025
Elaborado por: Comisión de Control

Respecto del día 3 de marzo de 2025, se advierten treinta y tres (33) registros de usuarios conforme se muestra en el cuadro precedente los funcionarios y servidores del Cenepred solo accedieron hasta las 9:06 am.

Cuadro n.° 5
Registro de accesos del Sistradoc 4 de marzo de 2025

Registro de Usuarios			
n.°	Hora y fecha	Apellido	Nombre
1	4/03/2025 **17:30**	Marangunich Rachumi	Martina Gisella
2	4/03/2025 17:33	Administrativa	Gestión
3	4/03/2025 17:38	Paz Llanos	Jorge Luis
4	4/03/2025 17:41	Cenepred	Inversiones
5	4/03/2025 17:41	Mercado Flores	Rolando Raúl
6	4/03/2025 17:42	Otero More	Juan Francisco
7	4/03/2025 17:47	Capucho Cárdenas	Rolando Gustavo
8	4/03/2025 18:01	Capucho Cárdenas	Rolando Gustavo
9	4/03/2025 18:01	Pereyra Franco	Jorge Luis
10	4/03/2025 18:04	Otero More	Juan Francisco
11	4/03/2025 18:10	Apoyo	OPP
12	4/03/2025 18:35	Obregón Acevedo	Chrisna Karina
13	4/03/2025 18:38	Jaimes Espinoza	Ena María
14	4/03/2025 18:47	Administrativa	Gestión
15	4/03/2025 18:52	Pautrat Vega	Brenda Giuliana
16	4/03/2025 18:57	Ochoa Enríquez	Karen Liliana
17	4/03/2025 19:00	Jaimes Espinoza	Ena Maria
18	4/03/2025 19:01	Pautrat Vega	Brenda Giuliana
19	4/03/2025 19:10	Apoyo	OPP
20	4/03/2025 19:15	Obregón Acevedo	Chrisna Karina
21	4/03/2025 19:18	Pérez Tijero	Ivone Carolina
22	4/03/2025 19:25	Pereyra Franco	Jorge Luis
23	4/03/2025 20:00	Obregón Acevedo	Chrisna Karina
24	4/03/2025 20:00	Pérez Tijero	Ivone Carolina
25	4/03/2025 20:06	Pereyra Franco	Jorge Luis
26	4/03/2025 20:12	Chafloque Sotomayor	Yindy Franchesca
27	4/03/2025 20:22	Celis Gómez	Marysussan Disa
28	4/03/2025 21:05	Pérez Tijero	Ivone Carolina
29	4/03/2025 21:08	Chafloque Sotomayor	Yindy Franchesca
30	4/03/2025 21:15	Obregón Acevedo	Chrisna Karina
31	4/03/2025 21:46	Gutiérrez Trujillo	Magna Rosa
32	4/03/2025 22:01	Obregón Acevedo	Chrisna Karina
33	4/03/2025 22:01	Gutiérrez Trujillo	Magna Rosa
34	4/03/2025 22:14	Pérez Tijero	Ivone Carolina
35	4/03/2025 23:10	Pérez Tijero	Ivone Carolina

Fuente: Listado de accesos remitido con informe n.° 00044-2025-CENEPRED/OA/UFI/JCA de 10 de julio de 2025
Elaborado por: Comisión de Control

CENEPRED V°B° Jefe OCI (e)
CENEPRED SUPERVISOR ÓRGANO DE CONTROL INSTITUCIONAL
CENEPRED JEFE DE COMISIÓN OCI
CENEPRED ABOGADO OCI

Respecto del día 4 de marzo de 2025, se advierte treinta y cinco (35) registros de usuarios, conforme se muestra en el cuadro precedente. Ello indica que los funcionarios y servidores del Cenepred recién pudieron acceder al Sistradoc a partir de las 17:30 horas, con relación, al día 6 de marzo de 2025, se advierten doscientos veintitrés (223) registros desde las 07:36 horas, hasta las 15:20 horas; toda vez que, a partir de esa hora se presentó otro corte de energía eléctrica desde las 15:20 horas.

En tal sentido, conforme a lo informado por el especialista de la Unidad Funcional de Informática[47], el Sistradoc estuvo inoperativo los días 3, 4 y 6 de marzo de 2025, durante el corte de energía eléctrica; toda vez que, ambos Datacenter Principal y de Contingencias se encontraban apagados.

Respecto de los Sistemas Sistema Integrado de Información Financiera (SIAF), y el Sistema Integrado de Gestión Administrativa (SIGA)

Con oficio n.° 00478-2025-CENEPRED/SG de 22 de abril de 2025[48] **(apéndice n.° 34)**, la Secretaría General remitió el informe n.° 00058-2025-CENEPRED-OA/UFI de 21 de abril de 2025 **(apéndice n.° 35)** suscrito por el coordinador (e) de la Unidad Funcional de Informática, en el cual, señala lo siguiente:

> *"(...)*
> ***1. Respecto al Data Center Principal y de Contingencia (Pregunta1 y Pregunta2):***
> *Efectivamente, ambos centros de datos contienen los dispositivos empleados como servidores de las plataformas institucionales (**SIGRID, Aula Virtual, SIMSE, RENAERD, RENAT y REFOCAP), los sistemas de información (SIGA, SIAF, SISTRADOC), además de servicios de internet y almacenamiento de datos**, en conformidad con lo estipulado en el subnumeral 5.6.1 del Plan de Continuidad Operativa del CENEPRED.*
> ***(...)"***

En consecuencia, se confirma que durante el corte de energía eléctrica no se tuvo acceso a los sistemas misionales como el Sigrid, Simse y Aula Virtual; tampoco se pudo acceder al sistema administrativo como el Sistradoc. Del mismo modo, conforme a lo señalado por el coordinador (e) de la Unidad Funcional de Informática, el SIAF, SIGA y el servicio de internet operan a través de los servidores de los Datacenter Principal y de Contingencias; por lo que, al encontrarse ambos apagados, tampoco se tuvo acceso a dichos sistemas.

En conclusión, el análisis de la información remitida por las distintas áreas del Cenepred permitió corroborar que, durante los cortes de energía eléctrica ocurridos los días 3, 4 y 6 de marzo de 2025, se produjo la inoperatividad de los sistemas informáticos misionales (Sigrid, Simse y Aula Virtual) y de gestión administrativa (Sistradoc y correo electrónico), toda vez que tanto el Datacenter Principal como el de Contingencias permanecieron apagados, contraviniendo con ello los principios básicos de continuidad operativa y disponibilidad de servicios tecnológicos establecidos en el Plan de Continuidad Operativa del Cenepred.

[47] Informe n.° 00044-2025-CENEPRED/OA/UFI/JCA de 10 de julio de 2025, se adjuntó el reporte de accesos al Sistradoc de los días 3, 4, y 6 de marzo de 2025.
[48] Información remitida a solicitud del OCI, con oficio n.° 0090-2025-CENEPRED/OCI de 11dde abril de 2025

Respecto del Plan de Continuidad Operativa del Cenepred[49] establece lo siguiente:

> *"(...)*
> ***1. Actividades críticas.*** *Están constituidas por las* ***actividades que la entidad haya identificado como indispensables y que no pueden dejar de realizarse****, conforme a sus competencias y atribuciones señaladas en las normas sobre la materia*
> *(...)*
>
> ***5.6. Determinación de la sede alterna de trabajo***
> ***5.6.1. Situación actual***
> *(...)*
> *Así mismo, mediante Resolución Ministerial N° 004-016-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana "**NTP ISO /IEC 27001:2014** Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad", en todas las entidades integrantes del Sistema Nacional de informática.* ***Esta norma técnica, así como otros modelos y buenas prácticas están orientadas a la Gestión de la Continuidad, a través de políticas para la seguridad de las operaciones y el respaldo de la información****, específicamente en la generación de copias de seguridad* ***y su custodia en una localización geográficamente diferente e independiente del almacenamiento principal****.*
>
> *En este contexto, y en base a lo escrito en los párrafos anteriores, se informa que el CENEPRED actualmente cuenta con un centro de datos ubicado en una única sede de la institución. Dicho centro de datos alberga a los equipos que son utilizados como SERVIDORES los cuales almacenan datos, plataformas (SIGRID, Aula Virtual, SIMSE, RENAERD, RENAT y REFOCAP), sistemas de información (SIGA, SIAF, SISTRADOC), servicios de internet, y toda la información institucional que permite a los usuarios realizar sus actividades laborales para el óptimo funcionamiento de los procesos administrativos y operacionales de la institución.*
>
> *Sin embargo, ante una situación de desastre que pueda comprometer la infraestructura física de las instalaciones de la institución, puede generar una pérdida parcial o total de la información contenida en el centro de datos.* ***En ese sentido, es necesario implementar medidas de contingencia que permitan a la institución poder recuperar y restaurar sus funciones críticas ante una situación de desastre en lo que respecta a los sistemas de información y servicios informáticos***
>
> ***5.6.2. Propuesta de Infraestructura Alterna de Tecnologías de la Información***
>
> *Es innegable que la fecha, el lugar y la magnitud de los daños derivados de eventos adversos contemplados en este plan son impredecibles. Por esta razón,* ***es imperativo designar una Sede Alterna ubicada en una geografía distinta, preferiblemente alejada de la ubicación actual****. La elección de esta sede debe basarse en una evaluación exhaustiva de la situación resultante en la infraestructura actual. (...)".* (Énfasis agregado)

Cabe precisar que, el Plan de Continuidad Operativa v2.0 vigente, se encuentra vinculado al anterior local que ocupaba la sede institucional, donde solo se contaba con un (1) Datacenter. No obstante, conforme se ha señalado precedentemente, desde el 5 de marzo de 2024[50] el CENEPRED cuenta con

[49] Aprobado con Resolución Jefatural n.° 00005-2024-CENEPRED/J de 12 de enero de 2024
[50] Según Anexo n.° 8. Acta de Conformidad de Servicios suscrita por el Especialista de la Oficina de Informática, José Luis Codarlupo Alejos; el subdirector de Gestión de la Información, Alfredo Zambrano Gonzales y el director de Gestión de Procesos, Juan Carlos Montero Chirito

dos (2) Datacenter: Principal y de Contingencias.

El **Plan de Continuidad Operativa (PCO)** establece las acciones necesarias para asegurar la continuidad de las operaciones de la Entidad. Entre otras medidas, prevé la necesidad de contar con un **servidor espejo (contingencia) externo a las instalaciones**, con el fin de garantizar que, ante la eventualidad de un evento adverso significativo, se activen de manera inmediata los sistemas informáticos esenciales para el desarrollo de las funciones críticas identificadas.

Respecto del Plan de Contingencia Informático, Directiva n.° 01-2016-CENEPRED/SG/OA[51]
En cuanto al Plan de Contingencia Informático, se dispone lo siguiente:

> *"(...)*
> ***V. RESPONSABILIDAD***
>
> ***5.1*** *El responsable de la elaboración del Plan de Contingencia Informático en la Oficina de Administración a través del Especialista de Informática.*
>
> ***5.2*** *El mantenimiento y ejecución del Plan de Contingencia Informático tiene los siguientes responsables:*
> - ***El Jefe de la Oficina de Administración es responsable de la ejecución del Plan.***
> - ***El Especialista en Informática como Coordinador del Plan.***
>
> *(...)*
> ***6.1.3 Procesos Críticos***
> *Los procesos críticos son considerados indispensables para la continuidad de las operaciones y servicios de la entidad, y cuya falta o ejecución deficiente puede tener un impacto operacional o de imagen significativo para la institución o para la ciudadanía en general.*
> *(...)*
> ***7.1 EQUIPO DE PLAN DE CONTINGENCIA***
> *(...)*
> *d) Mantenimiento del Plan de Contingencia*
> *Que consiste en la consideración de los procedimientos de mantenimiento al Plan definido, debidamente formalizado y documentado. Además del análisis del impacto que tendrá cualquier cambio en el ambiente informático sobre el Plan de Contingencia y proceder a su actualización.*
>
> *Los responsables del Mantenimiento del Plan de Contingencia son:*
> - *Jefe de Administración*
> - *Especialista en Informática*
>
> *(...)*
> ***8.1. DETERMINACIÓN DEL ESQUEMA DE TRABAJO***
> ***8.1.1 Identificación de Actividades y Servicios Críticos Informáticos***
> *Las funciones críticas de la Institución, se encuentran implementadas dentro de la infraestructura informática. Es por ello que la Institución deberá tomar medidas para tener la disponibilidad de dicha infraestructura.*
> *La determinación de las actividades y servicios críticos informáticos, se realiza en base a la determinación de los procesos críticos de la Institución. El servicio denominado Sistema de Información para la Gestión del Riesgo de Desastres – SIGRID es el proceso crítico más relevante, en mérito que gestiona la información compilada de diversas instituciones dentro del SINAGERD, es una fuente de información para las diversas instituciones involucradas en la Respuesta, Rehabilitación y Reconstrucción durante evento de desastres.*

CENEPRED Jefe OCI (e)
CENEPRED SUPERVISOR ÓRGANO DE CONTROL INSTITUCIONAL
CENEPRED JEFE DE COMISIÓN OCI
CENEPRED ABOGADO OCI

[51] Aprobado con Resolución de Secretaría General n.° 04-2016-CENEPRED/SG de 17 de junio de 2016

El SIGRID, es un servicio crítico su recuperación deberá ser prioritaria y poner en operatividad los servicios relacionados que permitan su funcionamiento.
(...)

8.3 CONSIDERACIONES AL PLAN

8.3.1 Continuidad de Operaciones
La continuidad de operaciones, para el caso de los servicios informáticos, se debe considerar los siguientes componentes:

- *Conectividad a internet*
- *Computadoras con navegador*

(...)
8.3.4 Infraestructura Alterna
La determinación de la infraestructura alterna, se hará en base a la determinación de los servicios críticos informáticos realizado en la institución.
Infraestructura alterna para la implementación de los servicios del SIGRID. (...)"

En este punto **es importante reiterar que, el Cenepred es responsable de brindar asistencia técnica e información en gestión prospectiva y correctiva del riesgo de desastres a los miembros que conforman el Sinagerd, de manera oportuna y confiable, para reducir la vulnerabilidad de la población y sus medios de vida ante el riesgo de desastres.** Para ello, cuenta con la plataforma geoespacial Sigrid, cuyo funcionamiento y operatividad son indispensables para el cumplimiento de sus funciones misionales.

Dicha plataforma tecnológica se encuentra alojada en varias máquinas virtuales dentro del Datacenter Principal y de Contingencias, constituyendo el proceso crítico más relevante conforme lo establece la normativa citada. Asimismo, el Plan de Contingencia Informático designa como responsable de su ejecución al jefe de la Oficina de Administración y como coordinador al Especialista en Informática. Del mismo modo, dispone consideraciones específicas para asegurar la continuidad de las operaciones, entre ellas la implementación de una infraestructura alterna (de contingencia). No obstante, esta disposición no fue atendida por el jefe de la Oficina de Administración, al instalar los Datacenter Principal y de Contingencias en una misma ubicación geográfica.

Los hechos descritos inobservaron la siguiente normativa:

Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD), Ley n.º 29664 de 18 de febrero de 2011.

CAPÍTULO III
CENTRO NACIONAL DE ESTIMACIÓN, PREVENCIÓN Y REDUCCIÓN DEL RIESGO DE DESASTRES (CENEPRED)

Artículo 12.- Definición y funciones del Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres (Cenepred)
(...)
g. Establecer mecanismos que faciliten el acceso público a la información geoespacial y los registros administrativos, generados por los organismos públicos técnico-científico relacionados con la Gestión del Riesgo de Desastres, coordinando, para tal fin, con los órganos y entidades públicas que corresponda.

- **Plan de Continuidad Operativa del CENEPRED v2.0", aprobado con Resolución Jefatural n.° 00005-2024-CENEPRED/J de 12 de enero del 2024.**

Glosario de Términos:

1. ***Actividades Críticas:*** *Están constituidas por las actividades que la entidad haya identificado como indispensable y que no puede dejar de realizarse, conforme a sus competencias y atribuciones señaladas en las normas sobre la materia*
(...).

III. OBJETIVOS

3.1. Objetivo General

Garantizar la continuidad de operaciones ante la ocurrencia de una emergencia o desastre, ejecutando de manera ininterrumpida los servicios críticos del CENEPRED hasta lograr su recuperación en el menor plazo posible.

3.2. Objetivos Específicos

- *Identificar las actividades críticas que requieran ser ejecutadas de manera ininterrumpida.*
- *Determinar los recursos humanos, materiales, equipos, así como los sistemas de información necesarios para ejecutar las actividades críticas.*
- *Establecer los mecanismos de activación de la continuidad operativa institucional ante eventos adversos que afecten la disponibilidad de la Sede de CENEPRED.*
- *Mantener la continuidad operativa institucional a través de la ejecución de procedimientos básicos de contingencia de las actividades críticas.*
- *Definir las acciones de recuperación de la Sede, sistemas administrativos y tecnológicos.*
- *Definir la desactivación de la modalidad de trabajo remoto para el retorno a la normalidad.*

IV. IDENTIFICACIÓN DE RIESGOS Y RECURSOS

4.1.Matriz de Riesgos

(...)

4.1.1.Identificación de los Peligros

El presente Plan ha sido diseñado considerando eventos que puede ocasionar mayor afectación, así como, para dar respuesta a incidentes.

La materialización de los peligros identificados puede generar la irrupción de las actividades críticas y poner en riesgo la continuidad operativa.

CENEPRED V° B° Jefe OCI (e)

CENEPRED SUPERVISOR ÓRGANO DE CONTROL INSTITUCIONAL

CENEPRED JEFE DE COMISIÓN OCI

CENEPRED ABOGADO OCI

CUADRO NRO. 02

IDENTIFICACIÓN DE LOS PELIGROS	
Eventos Externos	*a. Sismo de gran intensidad en Lima*
	b. Ataque informático
	c. Corte de servicios básicos
	d. Alteración orden público
	e. Atentado terrorista
	f. Falla de las comunicaciones
Eventos Internos	*a. Incendio de proporciones*
	b. Huelga de trabajadores

Fuente: Elaborado por Grupo de Comando del Cenepred

(...)

V. ACCIONES PARA LA CONTINUIDAD OPERATIVA

(...)

5.4. Roles y Responsabilidades para el desarrollo de las Actividades Críticas

(...)

c. Coordinador de Recuperación Tecnológica

Es el encargado de liderar la recuperación tecnológica, basado en la estrategia de continuidad contempladas en el Plan de Contingencia Informático del CENEPRED.

Responsabilidades:

(...).

- *Velar por la actualización de la Estrategia Tecnológica en los casos que se presenten situaciones como: cambios en los aplicativos, cambio en la infraestructura, roles y responsabilidades, disponibilidad de los recursos, entre otros.*

(...).

5.5. Requerimientos

5.5.3. Requerimiento de Recursos Informáticos

El desempeño y la ejecución de las funciones críticas delineadas en el Plan de Continuidad Operativa están intrínsecamente ligados al estado del software y hardware actuales. En este contexto, es imperativo que la Alta Dirección instruya a la Oficina de Planeamiento y Presupuesto para que desarrolle e implemente un Plan de Actualización y Mantenimiento destinado al equipamiento y ***servidores que albergan las bases de datos institucionales****.*

Dicho plan debe abordar la necesidad de contar con ***un servidor espejo externo a las instalaciones****, asegurando que, en caso de daños graves en las instalaciones,* ***la información crucial para el funcionamiento continuo de las actividades y procesos del Cenepred no se vea comprometida****. Esto permitirá la pronta reanudación al 100% de las operaciones cotidianas en un breve lapso de tiempo.*

Es fundamental dar prioridad a la recuperación de la página institucional, así como a los aplicativos de control y operatividad correspondientes. En este sentido, entre los servicios a recuperar, se deben destacar:

- *Conectividad a Internet (incluso mediante acceso satelital si es necesario).*
- *Firewall.*
- *Servidor de Correo.*
- *Servidor de Bases de Datos.*
- *Servidor Web.*
- *Unidad de Fuente de Poder (UPS).*
- *Grupo Electrógeno.*

CENEPRED V°B° Jefe OCI (e)

CENEPRED SUPERVISOR ÓRGANO DE CONTROL INSTITUCIONAL

CENEPRED JEFE DE COMISIÓN OCI

CENEPRED ABOGADO OCI

En todo momento, se debe tener presente que, ante la eventualidad de un evento adverso significativo, se requiere la activación inmediata de los sistemas informáticos esenciales para llevar a cabo las funciones críticas identificadas. Este enfoque proactivo garantizará la pronta restauración de la operatividad integral del Cenepred.
(...)

5.6. Determinación de la sede alterna de trabajo

5.6.1. Situación actual

Asimismo, mediante Resolución Ministerial N° 004-016-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO /IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad", en todas las entidades integrantes del Sistema Nacional de informática. Esta norma técnica, así como otros modelos y buenas prácticas están orientadas a la Gestión de la Continuidad, a través de políticas para la seguridad de las operaciones y ***el respaldo de la información****, específicamente en la generación de copias de seguridad y* ***su custodia en una localización geográficamente diferente e independiente del almacenamiento principal****.*

En este contexto, y en base a lo escrito en ***los*** *párrafos anteriores, se informa que* ***el Cenepred actualmente cuenta con un centro de datos ubicado en una única sede*** *de la institución. Dicho centro de datos alberga a los equipos que son utilizados como SERVIDORES los cuales almacenan datos, plataformas (SIGRID, Aula Virtual, SIMSE, RENAERD, RENAT y REFOCAP), sistemas de información (SIGA, SIAF, SISTRADOC), servicios de internet, y* ***toda la información institucional que permite a los usuarios realizar sus actividades laborales para el óptimo funcionamiento de los procesos administrativos y operacionales de la institución****.*

Sin embargo, ante una situación de desastre que pueda comprometer la infraestructura física de las instalaciones de la institución, ***puede generar una pérdida parcial o total de la información contenida en el centro de datos****. En ese sentido, es necesario* ***implementar medidas de contingencia*** *que permitan a la institución poder recuperar y restaurar sus funciones críticas ante una situación de desastre en lo que respecta a los sistemas de información y servicios informáticos.*

5.6.2. Propuesta de Infraestructura Alterna de Tecnologías de la Información

Es innegable que la fecha, el lugar y la magnitud de los daños derivados de eventos adversos contemplados en este plan son impredecibles. Por esta razón, es imperativo designar una Sede Alterna ubicada en una geografía distinta, preferiblemente alejada de la ubicación actual. La elección de esta sede debe basarse en una evaluación exhaustiva de la situación resultante en la infraestructura actual.

La Sede Alterna debe estar provista de sistemas de comunicación e internet*, así como cumplir con requisitos esenciales para el personal, incluyendo áreas de descanso, suministro de alimentos, medicamentos y equipos de protección personal necesarios para asegurar la continuidad operativa durante el tiempo requerido. Además, es esencial que cuente con servicios básicos para garantizar la pronta rehabilitación del servicio. Hasta la fecha, no se ha definido una Sede Alterna, y es urgente resolver esta situación sin demora.*

(...)

5.7. Activación del plan de continuidad operativa

Para la activación del PCO se deben considerar los escenarios en que pueda suceder el evento o desastre, dependerá del momento en que éste suceda para determinar la acción a realiza:

CENEPRED V°B° Jefa OCI (e)

CENEPRED SUPERVISOR ÓRGANO DE CONTROL INSTITUCIONAL

CENEPRED JEFE DE COMISIÓN OCI

CENEPRED ABOGADO OCI

5.7.1. Fase 1. Activación de la continuidad operativa institucional

Ocurrido el evento que afecta las funciones críticas del Cenepred en horario de trabajo o fuera de este. Se deben de ejecutar las siguientes acciones iniciales:

(...)

c. Restablecimiento de servicios básicos (luz, agua, telefonía, internet, etc.).

Todos los servicios básicos que sean afectados ante el evento adverso deben ser restablecidos lo más rápidamente posible para garantizar la continuidad de las actividades críticas que brinda el Cenepred. Responsable operativo, el Coordinador de Administración y su equipo, deberán verificar y coordinar que se cuente con los servicios, equipos e insumos en las unidades orgánicas afectadas para la continuidad de las operaciones. Los nombres de los integrantes del equipo técnico serán registrados en los anexos del plan.

Proceder con la pronta recuperación y operatividad de los equipos e insumos necesarios para generar energía y otras líneas vitales indispensables. Si es necesario disponer del uso del grupo electrógeno y demás materiales que permitan acceder a los servicios. Responsable: Oficina de Administración.

Restablecer la comunicación interna y externa. Disponer de los equipos de comunicación y otros que se tengan disponibles, reasignación de los equipos acorde a las acciones dispuestas por el Grupo de Comando. Acorde a las necesidades del evento adverso ocurrido. Responsable: Coordinador de Administración y su equipo.

Restablecer la conexión a internet y la operatividad de los medios de interacción institucional a nivel global por este medio. A cargo del Coordinador de Recuperación Tecnológica y Oficina de Administración.
(...)

ANEXO 1

Plan de Recuperación de los Servicios Informáticos
(...)

El éxito de cualquier proceso de recuperación dependerá de la priorización del servicio y la gravedad de la contingencia. En términos generales, se deben considerar los siguientes aspectos:
(...)

- *Determinar procedimientos que garanticen la continuidad y restauración de los servicios informáticos.*
(...)

Es responsabilidad de Informática de la Oficina de Administración, a través del Plan de Contingencia Informático, diseñar actividades de prevención y recuperación que aseguren la continuidad y recuperación de los servicios en el menor tiempo y con costos mínimos.
(...)

Principales servicios que deberán ser restablecidos y/o recuperados (para la infraestructura1 alterna de Tecnologías de la Información al implementar el Plan de Contingencia).

- *Centro de cómputo alterno al implementar el Plan de Contingencia: Router, Switch Core, Proxy, Controlador de Dominio, Controlador de Dominio 2, SIAF, SIGA, Servidor de Base de Datos, Servidor Web (SIGI), Servidor de Correos, Antivirus y Asterisk (telefonía IP).*

(...)
Además, se identifican los principales servicios que deben ser restablecidos y/o recuperados en el centro de cómputo alterno al implementar el Plan de Contingencia, incluyendo routers, switches, proxies, controladores de dominio, SIAF, SIGA, servidores de bases de datos, servidores web, correos institucionales, antivirus y telefonía IP. Se detallan servidores críticos y servicios que deben respaldarse de manera crucial para garantizar la continuidad operativa.

➢ **Directiva n.° 01-2016-CENEPRED/SG/OA "Plan de Contingencia Informático del Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres – CENEPRED", aprobado con Resolución de Secretaría General n.° 04-2016-CENEPRED/SG de 17 de junio de 2016.**

V. RESPONSABILIDAD

5.1 *El responsable de la elaboración del Plan de Contingencia Informático en la Oficina de Administración a través del Especialista de Informática.*

5.2 *El mantenimiento y ejecución del Plan de Contingencia Informático tiene los siguientes responsables:*
- *El Jefe de la Oficina de Administración es responsable de la ejecución del Plan.*
- *El Especialista en Informática como Coordinador del Plan.*
- *El Técnico en Informática como apoyo para la Coordinación.*
- *El Técnico de Recursos Humanos como apoyo para la puesta en operaciones de los servicios.*
- *Profesionales de la Subdirección de Gestión de la Información de la Dirección de Gestión de Procesos – SGI-DGP, como apoyo para la puesta en operaciones de los servicios críticos.*
- *El personal de seguridad para apoyo con los movimientos de los equipos que se puedan requerir.*

(...)

6.1.3 Procesos Críticos
Los procesos críticos son considerados indispensables para la continuidad de las operaciones y servicios de la entidad, y cuya falta o ejecución deficiente puede tener un impacto operacional o de imagen significativo para la institución o para la ciudadanía en general.
(...)
7.1 EQUIPO DE PLAN DE CONTINGENCIA
(...)
7.1.2 Equipo de Ejecución del Plan
(...)
a) (...)
Los responsables de la Coordinación de Recuperación de Tecnologías de la Información son
- *Jefe de Administración*
- *Especialista en Informática*

(...)
7.1.2 Equipo de Administración del Plan
(...)
d) Mantenimiento del Plan de Contingencia
Los responsables de la Coordinación de Recuperación de Tecnologías de la Información son:
- *Jefe de Administración*
- *Especialista en Informática*

(...)

8.3 CONSIDERACIONES AL PLAN

8.3.1 Continuidad de Operaciones

La continuidad de operaciones, para el caso de los servicios informáticos, se debe considerar los siguientes componentes:

- *Conectividad a internet*
- *Computadoras con navegador*

(...)

8.3.4 Infraestructura Alterna

La determinación de la infraestructura alterna, se hará en base a la determinación de los servicios críticos informáticos realizado en la institución.

Infraestructura alterna para la implementación de los servicios del SIGRID.

La infraestructura alterna deberá contar con las siguientes características:

- *Estar ubicado en una zona geográfica distante a la ubicación del servicio originario.*
- *Contar con conectividad a internet permanente de al menos 10Mbps de subida.*
- *Flujo de energía respaldada (mediante UPS u otro dispositivo de continuidad de energía)*
- *Personal técnico, con conocimiento de administración de redes y servidores.*

(...)

9.2 EJECUCIÓN DEL PLAN

9.2.1 Recuperación de Contingencia Según Escenarios

9.2.1.1. Procedimiento de recuperación para el Escenario 1

a) Servicio no crítico:

(...)

- *Se inicia la operación del grupo electrógeno para el centro de datos*
- *Se verifica la calidad de la línea de energía del grupo electrógeno.*
- *Se levanta la línea de energía de los gabinetes de los servidores y switches.*

(...)

9.2.1.5 Procedimiento de recuperación para el Escenario 5:

(...)

b) Servicio crítico:

- *Se activa el procedimiento de restauración del servicio en la ubicación alterna.*

➢ **Directiva n.° 008-2016-CENEPRED/J "*Administración y Uso del Sistema de Información para la Gestión del Riesgo de Desastre - Sigrid*", aprobado con Resolución Jefatural n.° 068-2016-CENEPRED/J de 3 de mayo de 2016.**

6. RESPONDABILIDADES

Son responsables de su aplicación las siguientes unidades orgánicas del CENEPRED:

6.2. La Oficina de Administración del CENEPRED, el área de Sistemas, quien estará a cargo de administrar los recursos tecnológicos para el soporte informático y de comunicaciones que garanticen la operatividad del SIGRID;

(...)

7. FUNCIONES

7.1. DEL CENEPRED

(...)

7.1.3. Oficina de Administración a través del Área de Sistemas

a) Mantener operativos los servicios que ofrece el SIGRID.

b) Resolver los problemas técnicos que pudieran afectar la operatividad del SIGRID.
c) Mantener y optimizar la red dedicada al servicio SIGRID.
d) Mantener operativos los servicios de red y comunicaciones (voz, datos e imagen)

- **Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas de los tres niveles de gobierno, aprobado con Resolución Ministerial n.° 320-2021-PCM de 30 de diciembre de 2021.**

2. OBJETIVO

Establecer los procedimientos para la implementación de la Gestión de la Continuidad Operativa y la formulación de los Planes de Continuidad Operativa en las entidades públicas de los tres niveles de gobierno, con el fin de continuar funcionando ante un desastre o cualquier evento que interrumpa prolongadamente sus operaciones.

(...)
5. DISPOSICIONES GENERALES
5.1 Definiciones:
(...)
b. ***Gestión de la Continuidad Operativa del Estado****: Proceso continuo que forma parte de las operaciones habituales de la Entidad Pública con el objetivo de que siga cumpliendo con su misión, mediante la implementación de mecanismos adecuados, con el fin de continuar brindando servicios necesarios a la población, ante la ocurrencia de un desastre o evento que produzca una interrupción prolongada de sus operaciones.*

f. Plan de Recuperación de los servicios informáticos*: Plan que forma parte del Plan de Continuidad Operativa, el cual busca inicialmente, restaurar los servicios de tecnología de información necesarios para ejecutar las actividades críticas identificadas, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia. Para su desarrollo toma en cuenta la Norma Técnica Peruana NTP ISO/IEC 20071: 2014.*

g. ***Sede alterna de la entidad pública****: Espacio físico o infraestructura segura y accesible, determinada con anterioridad y de disponibilidad inmediata, que permite la ejecución de los servicios o actividades críticas señaladas en el Plan de Continuidad Operativa de la entidad. Para ello, cuenta con el equipamiento necesario y servicios básicos indispensables, que opera con autonomía energética y de conectividad.*

5.2 Componentes de la Gestión de la Continuidad Operativa
(...)
5.2.3 Ejercicios y actualización del Plan de Continuidad Operativa
Las Entidades Públicas de los tres niveles de gobierno, para los ejercicios y actualización del plan realizan las acciones siguientes:
a. Ejecución de ejercicios:
b. Actualización del plan: *El plan se actualiza ante cualquier cambio interno o externo que afecte a la Entidad, cambios en la infraestructura tecnológica, cambios geográficos de las oficinas, modificaciones en la organización o ante las recomendaciones procedentes de la ejecución de los ejercicios (simulacros y simulaciones), bajo responsabilidad del Grupo de Comando.*

- **ETP-ISO/IEC TS 22237-2 2019, Normativa Técnica Peruana para la Construcción de Centro de Datos ISO/IEC TS 22237, aprobado mediante Resolución Directoral n.° 030-2019-INACAL/DN**

4. Conformidad

Para que un centro de datos cumpla con este documento:
a) su ubicación debe haber sido seleccionada luego de una evaluación del sitio como se requiere en Numeral 5;
(...)

5 ubicación
5.1 Evaluación de la ubicación
5.1.1 Requisitos
La ubicación de un sitio para un centro de datos se puede evaluar ya sea para una construcción "no urbanizada" de un nuevo centro de datos o la evaluación de un sitio existente. La ubicación se evaluará según los siguientes criterios:
(...)
c) Adyacencias. (Ver 5.4)
d) Factores infraestructurales. (Véase 5.5)
(...)
5.4 Adyacencias
5.4.1 Requisitos
Se debe realizar un análisis de riesgos que, como mínimo, considera la adyacencia a los siguientes ítems:
(...).
f) *Instalaciones altas e inestables que podrían dañar el centro de datos si estos colapsan;*
(...)
5.5 Factores infraestructurales

5.5.1 Requisitos
Se debe de considerar el acceso a todos los suministros de servicios públicos (por ejemplo, electricidad, infraestructura de telecomunicaciones, agua, alcantarillado y gas) que serán necesarias durante la vida útil prevista del centro de datos en términos de:
(...)
c) disponibilidad (confiabilidad basada en tendencias históricas, si está disponible).
d) capacidad (por ejemplo, electricidad: corriente de cortocircuito; agua: presión y el flujo; aguas residuales: dimensionamiento).
(...)
6. Configuración del sitio
(...).
6.2 Selección del servicio
6.2.1 Requisitos
El tamaño y forma de un nuevo sitio deben ser adecuados para alojar las funciones previstas.
(...).
6.3 Evaluación de locales existentes
6.3.1 Requisitos
La idoneidad de las instalaciones existentes será determinada por un análisis de riesgo que refleja las necesidades específicas del centro de datos propuesto, que incluye la evaluación de los criterios del Numeral 5. Se puede considerar un estudio existente si su documentación no tiene más de seis meses de antigüedad. Un análisis de riesgos existentes sólo será referido si se realiza con un objetivo similar (ver Numeral 5).
(...).
6.4 Servicios públicos
6.4.1 Requisitos
La prestación de los servicios públicos externos a las instalaciones debe ser adecuada para la clase disponibilidad prevista del centro de datos, tal como se define en la ISO/IEC TS 22237-1.
Se debe de recopilar la documentación que permita evaluar el riesgo para la operación del centro de datos derivado de las infraestructuras de servicios públicos.

CENEPRED V°B° Jefe OCI (e)
CENEPRED SUPERVISOR ORGANO DE CONTROL INSTITUCIONAL
CENEPRED JEFE DE COMISIÓN OCI
CENEPRED ABOGADO OCI

- **Norma Técnica Peruana NTP-ISO/IEC 27001: 2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos, de 20 de noviembre de 2014.**

ANEXO A
OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA

(...)
TABLA A.1 – Objetivos de control y controles

A.17 Aspectos de seguridad de la información en la gestión de continuidad del negocio		
A.17.1 Continuidad de seguridad de la información		
Objetivo: La continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio de la organización		
A.17.1.1	*Planificación de continuidad de seguridad de la información*	*Control* *La organización debe determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.*
A.17.1.2	*Implementación de continuidad de seguridad de la información*	*Control* *La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de seguridad de la información durante una situación adversa.*
A.17.1.3	*Verificación, revisión y evaluación de continuidad de seguridad de la información*	*Control* *La organización debe verificar los controles de continuidad de seguridad de la información que han establecido e implementado a intervalos regulares para asegurarse que son válidos y efectivos durante situaciones adversas.*

- **Norma Técnica Peruana NTP ISO/IEC 17799 2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información, actualizada mediante Resolución Ministerial n.° 246-2007-PCM de 25 de agosto del 2007**

9. SEGURIDAD FÍSICA Y DEL ENTORNO
(...)
9.1.4 Protección contra amenazas externas y ambientales
(...)
b) el equipo y los medios de respaldo deberían estar a una distancia de seguridad conveniente para evitar que se dañen por un desastre en el área principal.

- **Establecen la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas, aprobada con Resolución de Secretaría de Gobierno y Transformación Digital n.° 003-2023-PCM/SGTD publicada el 8 de setiembre de 2023.**

Artículo 1. Implementación del Sistema de Gestión de Seguridad de la Información

1.1 Las entidades públicas usan obligatoriamente la Norma Técnica Peruana NTP ISO/IEC 27001 vigente para el análisis, diseño, implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (en adelante, SGSI).
Asimismo, aseguran que el SGSI establezca como alcance mínimo a los procesos misionales y aquellos relevantes para la operación y funcionamiento de la entidad pública.

1.2 Las entidades públicas establecen como objetivos del SGSI:
a) Preservar la confidencialidad, integridad y disponibilidad de la información de la entidad pública.

b) Fortalecer la cultura de seguridad de la información en los servidores, funcionarios y colaboradores de la entidad pública.
c) Asegurar el cumplimiento normativo en materia de seguridad y confianza digital.
d) Gestionar de manera eficaz los riesgos, eventos e incidentes de seguridad de la información

Los hechos expuestos ocasionaron la inoperatividad de procesos críticos y misionales como el Sistema de Información para la Gestión del Riesgo de Desastres **(Sigrid)**, el Sistema de Información de Monitoreo, Seguimiento y Evaluación **(Simse)** y la **Plataforma del Aula Virtual**; y de sistemas informáticos de gestión administrativa como el **Sistradoc**[52], además de afectar el acceso a los sistemas **SIAF** y **SIGA** de la Entidad; situación que limitó el acceso público a la información geoespacial y a los registros administrativos generados por los organismos públicos técnico científicos para la gestión prospectiva y correctiva del riesgo de desastres, durante los cortes de energía eléctrica ocurridos en marzo de 2025.

La situación descrita se originó por la inadecuada gestión de la Oficina de Administración, que dispuso la instalación y acondicionamiento del Datacenter Principal y de Contingencias en la misma sede institucional sin realizar la evaluación técnica de riesgos del local arrendado, ni gestionar la implementación de una infraestructura alterna geográficamente independiente para la reubicación del Datacenter de Contingencia, contraviniendo la normativa aplicable[53] Asimismo, se evidenció la inacción de los Jefes de la Oficina de Administración, en sus respectivos períodos de gestión, quienes conforme a la normativa interna son responsables de la ejecución del Plan de Contingencia Informático, respecto a la adopción de medidas oportunas para garantizar la ubicación en una sede alterna del Datacenter de Contingencia y el aseguramiento de la capacidad eléctrica requerida para su funcionamiento, pese a las advertencias técnicas formuladas[54].

Comentarios de las personas comprendidas en los hechos

Las personas comprendidas en los hechos presentaron sus comentarios y aclaraciones, conforme se detalla en el **Apéndice n.° 36** del Informe de Control Específico.

Se debe mencionar que los señores: Zoila Elena Huamán Marky y Elvis Renzo Revilla Llerena presentaron de forma extemporánea[55] sus comentarios o aclaraciones al Pliego de Hechos comunicado.

Evaluación de los comentarios o aclaraciones de las personas comprendidas en los hechos

Efectuada la evaluación de los comentarios o aclaraciones y documentos presentados por las personas comprendidas en los hechos, se concluye que no desvirtúan los hechos comunicados en el Pliego de Hechos. La referida evaluación, las cédulas de comunicación y notificación, forman parte del **Apéndice n.° 36** del Informe de Control Específico.

52 Sistema de Trámite Documentario del Cenepred, que facilita la gestión de documentos y trámites internos dentro del CENEPRED, permitiendo a los usuarios acceder, consultar y procesar información relevante para la gestión del riesgo de desastres.
53 Plan de Continuidad Operativa v2.0 del CENEPRED, el Plan de Contingencia Informático (Directiva N.° 01-2016-CENEPRED/SG/OA) y la normativa técnica aplicable (NTP ISO/IEC TS 22237 y NTP ISO/IEC 27001).
54 Previamente por la propia Unidad Funcional de Informática
55 Sin embargo, en atención a los principios de legalidad, razonabilidad y debido procedimiento que rigen el control gubernamental, y considerando la autonomía funcional de la comisión de control, se dispuso la evaluación de los comentarios y/o aclaraciones de las personas comprendidas en los hechos, a fin de no restringir el ejercicio del derecho de defensa, ni afectar la validez del procedimiento de control. Con ello, se garantiza que el desarrollo del presente servicio de control específico se lleve a cabo bajo un estándar de objetividad y respeto a las normas que lo regulan, sin que ello signifique convalidar la extemporaneidad en la presentación de los comentarios y/o aclaraciones.

La participación de las personas comprendidas en los hechos se describe a continuación:

- **Zoila Elena Huamán Marky,** identificada con DNI n.° [redacted], quien se desempeñó como jefa de la Oficina de Administración, periodo de gestión del 1 de mayo de 2024 al 3 de febrero de 2025, contratada mediante contrato administrativo de servicios n.° 026-2024-CENEPRED de 1 de mayo de 2024, designada mediante Resolución Jefatural n.° 00051-2024-CENEPRED/J de 30 de abril de 2024 y cesada mediante Resolución Jefatural n.° 00009-2025-CENEPRED/J de 3 de febrero de 2025 **(apéndice n.° 37),** a quien se le comunicó el Pliego de Hechos a través de la Cédula de Notificación n.° 001-2025-CG/OCI-SCE-001-CENEPRED de 5 de agosto de 2025, cuya notificación se realizó a través del sistema de e-Casilla Electrónica de la Contraloría General de la República - Cédula de Notificación Electrónica n.° 00000005-2025-CG/5775-02-001; habiendo presentado sus comentarios o aclaraciones, de forma extemporánea mediante carta n.° 003-2025-ZEHM de 19 de agosto de 2025, en doce (12) folios sin anexos. **(apéndice n.° 36),** de forma presencial y mediante correo electrónico institucional.

  Como resultado de la evaluación de los comentarios o aclaraciones de la señora **Zoila Elena Huamán Marky,** cuyo desarrollo consta em el **(apéndice n.° 36)** del Informe de Control Especifico; se ha determinado que el hecho con evidencias de presunta irregularidad no ha sido desvirtuado; puesto que:

  En su calidad de jefa de la Oficina de Administración omitió sus deberes funcionales de administrar los recursos para el soporte informático y de comunicaciones, lo cual incluye asegurar la continuidad de la infraestructura tecnológica crítica; considerando que, suscribió el contrato de arrendamiento[56] del nuevo local institucional, sin que se haya efectuado previamente un análisis del predio, evaluando los riesgos asociados a la infraestructura eléctrica y la idoneidad del sitio para alojar los Datacenter de la Entidad;

  Asimismo, autorizó y aprobó el traslado e instalación del Datacenter Principal y el Datacenter de Contingencia al mismo predio institucional, ubicado en la Av. Del Parque Norte 829-833, San Isidro, sin gestionar una ubicación geográfica distinta para el Datacenter de Contingencia, lo que constituyó una omisión incompatible con dichas obligaciones, configurando un incumplimiento funcional que expuso al Cenepred a riesgos operativos previsibles y que posteriormente se materializaron con la interrupción de procesos críticos y misionales.

  Respecto a la alegación de que los cortes eléctricos ocurrieron en marzo de 2025, con posterioridad a su cese, corresponde aclarar que el inicio de la irregularidad se configuró durante su gestión, al disponer que tanto el Datacenter principal como el de Contingencia funcionaran en un mismo predio, sin gestionar la habilitación de una sede alterna. Esta omisión expuso al Cenepred a un riesgo cierto y previsible, que se materializó con los cortes de energía, la condición que los generó se encontraba directamente vinculada con las decisiones adoptadas durante la gestión de la funcionaria.

  En tal sentido, inobservó lo establecido en los numerales 8.1 y 8.3.4 de la Directiva n.° 01-2016-CENEPRED/SG/OA – "*Plan de Contingencia Informático del CENEPRED*" aprobado con Resolución de Secretaría General n.° 04-2016-CENEPRED/SG de 17 de junio de 2016; así como el numeral 5.6.2 del Plan de Continuidad Operativa del CENEPRED v2.0 aprobado con

[56] El contrato n.° 003-2024-CENEPRED/OA de 5 de agosto de 2024

Resolución Jefatural n.° 00005-2024-CENEPRED/J de 12 de enero del 2024; incumpliéndose también los numerales 5 y 6.4.1 de la Norma Técnica Peruana ETP ISO/IEC TS 22237-2:2019 Normativa Técnica Peruana para la Construcción de Centro de Datos ISO/IEC TS 22237, aprobado mediante Resolución Directoral n.° 030-2019-INACAL/DN; inobservando también los acápites A.17.1.1 y A.17.1.2, de la Norma Técnica Peruana ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos, de 20 de noviembre de 2014.

Hechos que configuran incumplimiento de sus deberes y funciones como jefe de la Oficina de Administración establecidas en los numerales 5.2 y 7.1.2 de la Directiva n.° 01-2016-CENEPRED/SG/OA – "*Plan de Contingencia Informático del CENEPRED*", que señalan: *"5.2 El mantenimiento y ejecución del Plan de Contingencia Informático tiene los siguientes responsables: - El Jefe de la Oficina de Administración es responsable de la ejecución del Plan. (...)"* y *"7.1.2 EQUIPO DE ADMINISTRACIÓN DEL PLAN. (...). d) Mantenimiento del Plan de Contingencia. Los responsables de la Coordinación de Recuperación de Tecnologías de la Información son: Jefe de Administración. (...)"*; concordante con lo establecido en los numerales 6.2 y 7.1.3 de la Directiva n.° 008-2016-CENEPRED/J "*Administración y Uso del Sistema de Información para la Gestión del Riesgo de Desastre - Sigrid*", que señalan: *"**6.2. La Oficina de Administración del CENEPRED,** el área de Sistemas, quien estará a cargo de administrar los recursos tecnológicos para el soporte informático y de comunicaciones que garanticen la operatividad del SIGRID"*, y, " ***7.1.3. Oficina de Administración a través del Área de Sistemas a)** Mantener operativos los servicios que ofrece el SIGRID. **b)** Resolver los problemas técnicos que pudieran afectar la operatividad del SIGRID. **c)** Mantener y optimizar la red dedicada al servicio SIGRID. **d)** Mantener operativos los servicios de red y comunicaciones (voz, datos e imagen)".*

De igual modo, incumplió lo establecido en el artículo 20 del Reglamento de Organización y Funciones ROF del Cenepred, aprobado por Decreto Supremo n.° 104-2012-PCM de 18 de octubre de 2012 que establece lo siguiente: *"(...). Tiene también a su cargo la provisión de servicios de soporte de tecnologías de información y comunicaciones (...)"*; y de las funciones señaladas en el artículo 21, que le exigió: *"g) Administrar los recursos para el soporte informático, de comunicaciones y desarrollo de soluciones informáticas para el cumplimiento de las funciones de la entidad; h) Evaluar y proponer actividades de mejora de la infraestructura física del CENEPRED"*. Aunado a ello, su deber establecido en el literal a) del artículo 16 de la Ley Marco del Empleo Público -Ley n.° 28175, que establece: *"a) Cumplir personal y diligentemente los deberes que impone el servicio público."*

Finalmente, incumplió el artículo 6 de la Ley del Código de Ética de la Función Pública, aprobado con Ley n.° 27815, vigente desde el 14 de agosto de 2002, de conformidad a la disposición complementaria de la Ley n.° 28496, publicada el 16 de abril de 2005 que señala: *"6 del artículo 7° que establece: "Artículo 7.- Deberes de la Función Pública. El servidor público tiene los siguientes deberes: (...) 6. Responsabilidad. Todo servidor público debe desarrollar sus funciones a cabalidad y en forma integral, asumiendo con pleno respeto su función pública. Ante situaciones extraordinarias, el servidor público puede realizar aquellas tareas que por su naturaleza o modalidad no sean las estrictamente inherentes a su cargo, siempre que ellas resulten necesarias para mitigar, neutralizar o superar las dificultades que se enfrenten"*.

Los hechos anteriormente expuestos configuran presunta responsabilidad administrativa funcional no sujeta a la potestad sancionadora de la Contraloría General de la República, dando mérito al inicio del procedimiento administrativo correspondiente.

- **Elvis Renzo Revilla Llerena**, identificado con DNI n.° [redacted] quien se desempeña como jefe de la Oficina de Administración, periodo de gestión del 4 de febrero a la actualidad, contratado mediante contrato administrativo de servicios n.° 001-2025-CENEPRED de 4 de febrero de 2025. Designado con Resolución Jefatural n.° 00009-2025-CENEPRED/J2025-CENEPRED/J de 3 de febrero de 2025 **(apéndice n.° 37),** a quien se le comunicó el Pliego de Hechos a través de la Cédula de Notificación n.° 002-2025-CG/OCI-SCE-001-CENEPRED de 5 de agosto de 2025, cuya notificación se realizó a través del sistema de e-Casilla Electrónica de la Contraloría General de la República – Cédula de Notificación Electrónica n.° 00000004-2025-CG/5775-02-001; habiendo presentado sus comentarios o aclaraciones; a través del Sistradoc de forma extemporánea mediante oficio n.° 00066-2025-CENEPRED/OA de 21 de agosto de 2025, en veinte (20) folios y anexos[57] **(apéndice n.° 36).**

  Como resultado de la evaluación de los comentarios o aclaraciones del señor **Elvis Renzo Revilla Llerena,** cuyo desarrollo consta em el **(apéndice n.° 36)** del Informe de Control Especifico; se ha determinado que el hecho con evidencias de presunta irregularidad no ha sido desvirtuado; puesto que:

  En su condición de jefe de la Oficina de Administración del Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres, omitió adoptar medidas correctivas para mitigar el riesgo inminente de inoperatividad al tomar conocimiento de los reportes de fallas de voltaje eléctrico que no estaba alcanzando los niveles requeridos para su adecuado funcionamiento y que ello, podría ocasionar un gran perjuicio a la institución; así como de la inadecuada instalación del Datacenter de Contingencia; y por no activar medidas de recuperación ante escenarios de interrupción del servicio eléctrico; pues en su calidad de ejecutor del Plan de Contingencia, omitió las acciones de recuperación y contingencia, y por no establecer medidas que aseguren la continuidad de la seguridad de la información ante contingencias.

  Además, omitió realizar acciones inmediatas incumpliendo sus deberes funcionales respecto de la reubicación del Datacenter de Contingencias; a pesar que, con informe n.° 00019-2025-CENEPRED-OA/UFI de 17 de febrero de 2025, el Coordinador (e) de la Unidad Funcional de Informática, le informó sobre la situación del Datacenter de Contingencia, indicando que, el Datacenter de Contingencia debía ser instalado en un lugar diferente a la instalación donde funciona el Datacenter principal; y le solicitó que en su calidad de jefe de la Oficina de Administración realice las coordinaciones con la Fuerza Aérea del Perú – FAP o el Ejército del Perú – EP, para que puedan alojar dicho Datacenter de Contingencia.

  Consecuentemente, estas omisiones, en su calidad de jefe de la Oficina de Administración ocasionaron la inoperatividad del proceso crítico y misional como el Sigrid, Simse y aula virtual; así como, de los sistemas informáticos de gestión administrativa del Cenepred, como son el Sistradoc, SIAF y SIGA.

  En tal sentido, inobservó lo establecido en los numerales 8.1 y 8.3.4 de la Directiva n.° 01-2016-CENEPRED/SG/OA – "*Plan de Contingencia Informático del CENEPRED*" aprobado con Resolución de Secretaría General n.° 04-2016-CENEPRED/SG de 17 de junio de 2016; así como el numeral 5.6.2 del Plan de Continuidad Operativa del CENEPRED v2.0 aprobado con Resolución Jefatural n.° 00005-2024-CENEPRED/J de 12 de enero del 2024; incumpliéndose

[57] Ciento treinta y dos (132) folios de anexos con documentación sustentatoria.

también los numerales 5 y 6.4.1 de la Norma Técnica Peruana ETP ISO/IEC TS 22237-2:2019 Normativa Técnica Peruana para la Construcción de Centro de Datos ISO/IEC TS 22237, aprobado mediante Resolución Directoral n.° 030-2019-INACAL/DN; inobservando también los acápites A.17.1.1 y A.17.1.2, de la Norma Técnica Peruana ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos, de 20 de noviembre de 2014.

Hechos que configuran incumplimiento de sus deberes y funciones como jefe de la Oficina de Administración establecidas en los numerales 5.2 y 7.1.2 de la Directiva n.° 01-2016-CENEPRED/SG/OA – "*Plan de Contingencia Informático del CENEPRED*", que señalan: *"5.2 El mantenimiento y ejecución del Plan de Contingencia Informático tiene los siguientes responsables: - El Jefe de la Oficina de Administración es responsable de la ejecución del Plan. (...)"* y *"7.1.2 EQUIPO DE ADMINISTRACIÓN DEL PLAN. (...). d) Mantenimiento del Plan de Contingencia. Los responsables de la Coordinación de Recuperación de Tecnologías de la Información son: Jefe de Administración. (...)"*; concordante con lo establecido en los numerales 6.2 y 7.1.3 de la Directiva n.° 008-2016-CENEPRED/J "*Administración y Uso del Sistema de Información para la Gestión del Riesgo de Desastre - Sigrid*", que señalan: ***"6.2. La Oficina de Administración del CENEPRED,*** *el área de Sistemas, quien estará a cargo de administrar los recursos tecnológicos para el soporte informático y de comunicaciones que garanticen la operatividad del SIGRID"*, y, " ***7.1.3. Oficina de Administración a través del Área de Sistemas a)*** *Mantener operativos los servicios que ofrece el SIGRID.* ***b)*** *Resolver los problemas técnicos que pudieran afectar la operatividad del SIGRID.* ***c)*** *Mantener y optimizar la red dedicada al servicio SIGRID.* ***d)*** *Mantener operativos los servicios de red y comunicaciones (voz, datos e imagen)".*

De igual modo, incumplió lo establecido en el artículo 20 del Reglamento de Organización y Funciones ROF del Cenepred, aprobado por Decreto Supremo n.° 104-2012-PCM de 18 de octubre de 2012 que establece lo siguiente: *"(...). Tiene también a su cargo la provisión de servicios de soporte de tecnologías de información y comunicaciones (...)"*; y de las funciones señaladas en el artículo 21, que le exigió: *"g) Administrar los recursos para el soporte informático, de comunicaciones y desarrollo de soluciones informáticas para el cumplimiento de las funciones de la entidad; h) Evaluar y proponer actividades de mejora de la infraestructura física del CENEPRED"*. Aunado a ello, su deber establecido en el literal a) del artículo 16 de la Ley Marco del Empleo Público -Ley n.° 28175, que establece: *"a) Cumplir personal y diligentemente los deberes que impone el servicio público."*

Finalmente, incumplió el artículo 6 de la Ley del Código de Ética de la Función Pública, aprobado con Ley n.° 27815, vigente desde el 14 de agosto de 2002, de conformidad a la disposición complementaria de la Ley n.° 28496, publicada el 16 de abril de 2005 que señala: *"6 del artículo 7° que establece: "Artículo 7.- Deberes de la Función Pública. El servidor público tiene los siguientes deberes: (...) 6. Responsabilidad. Todo servidor público debe desarrollar sus funciones a cabalidad y en forma integral, asumiendo con pleno respeto su función pública. Ante situaciones extraordinarias, el servidor público puede realizar aquellas tareas que por su naturaleza o modalidad no sean las estrictamente inherentes a su cargo, siempre que ellas resulten necesarias para mitigar, neutralizar o superar las dificultades que se enfrenten"*.

Los hechos anteriormente expuestos configuran una presunta responsabilidad administrativa funcional no sujeta a la potestad sancionadora de la Contraloría General de la República, dando inicio del procedimiento administrativo correspondiente.

III. ARGUMENTOS JURÍDICOS

Los argumentos jurídicos por presunta responsabilidad administrativa funcional no sujeta a la potestad sancionadora de la Contraloría General de la República, de la irregularidad: "Funcionarios del Cenepred no gestionaron la instalación del Datacenter de Contingencia en una ubicación geográfica distinta a la sede institucional, lo que ocasionó la inoperatividad de procesos críticos y misionales así como de los sistemas de gestión administrativa durante los cortes de energía eléctrica ocurridos en marzo de 2025", están desarrollados en el **Apéndice n.° 2** del Informe de Control Específico.

IV. IDENTIFICACIÓN DE PERSONAS INVOLUCRADAS EN EL HECHO ESPECÍFICO PRESUNTAMENTE IRREGULAR

En virtud de la documentación sustentante, la cual se encuentra detallada en los anexos del presente Informe de Control Específico, los responsables por los hechos irregulares están identificados en el **Apéndice n.° 1.**

V. CONCLUSIÓN

Como resultado del Servicio de Control Específico a Hechos con Evidencia de Irregularidad practicado al Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres, se formula la conclusión siguiente:

De la revisión de la documentación proporcionada por la Entidad, se evidenció que el Datacenter Principal y de Contingencia fue acondicionado e instalado en la nueva sede institucional[58] ubicada en la avenida Del Parque Norte n.° 829 – 833, distrito de San Isidro, sin haberse efectuado previamente la evaluación técnica del local arrendado; tampoco se gestionó su implementación y acondicionamiento en una ubicación geográfica distinta a la del Datacenter principal.

Los hechos expuestos inobservaron lo dispuesto en el literal g) del artículo 12 de la Ley n.° 29664, Ley del Sistema Nacional de Gestión del Riesgo de Desastres (Sinagerd); los numerales 5.5, 5.6, 5.7 y el numeral 6.1. del "*Plan de Continuidad Operativa del Cenepred v2.0*"; así como los numeral 5.1, 5.2, 6.1, 7.1, 8.3 y 9.2 de la Directiva n.° 01-2016-CENEPRED/SG/OA "*Plan de Contingencia Informático del Cenepred*"; concordante con los numerales 6 y 7 de la Directiva n.° 008-2016-CENEPRED/J "*Administración y Uso del Sistema de Información para la Gestión del Riesgo de Desastre - Sigrid*"; y el numeral 5 de los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de la Entidades Públicas de los tres niveles de gobierno, aprobado con Resolución Ministerial n.° 320-2021-PCM. Aunado a ello se ha inobservado, los numerales 4, 5, 6 de la Normativa Técnica Peruana para la Construcción de Centro de Datos ISO/IEC TS 22237 ETP-ISO/IEC TS 22237-2 2019; concordante con el anexo A y la tabla A de la Norma Técnica Peruana NTP-ISO/IEC 27001: 2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información; así como, el numeral 9 de la Norma Técnica Peruana NTP ISO/IEC 17799 2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de

[58] Arrendamiento del local a través de la Contratación Directa n.° 003-2024-CENEPRED/OEC "*Servicio de alquiler de local institucional para el CENEPRED*", suscribiéndose el contrato n.° 003-2024-CENEPRED/OA de 5 de agosto de 2024.

la información y el artículo 1 de la Resolución de Secretaría de Gobierno y Transformación Digital n.° 003-2023-PCM/SGTD.

En consecuencia, durante los cortes de energía eléctrica ocurridos el 3, 4 y 6 de marzo de 2025, ambos datacenter quedaron inoperativos, ocasionando la interrupción de procesos críticos y misionales vinculados al Sistema de Información para la Gestión del Riesgo de Desastres (Sigrid), el Sistema de Monitoreo, Seguimiento y Evaluación (Simse) y el Aula Virtual; así como de los sistemas administrativos institucionales Sistradoc, SIAFy SIGA, situación que limitó el acceso público a la información geoespacial y a los registros administrativos generados por los organismos públicos técnico–científicos para la gestión prospectiva y correctiva del riesgo de desastres, durante los cortes de energía eléctrica ocurridos en marzo de 2025.

La causa identificada se encuentra en la falta de diligencia funcional de la Oficina de Administración al suscribir y ejecutar el contrato de arrendamiento del local institucional; asimismo, se dispuso la instalación del Datacenter Principal y de Contingencias en la misma sede institucional sin realizar la evaluación técnica de riesgos del local arrendado, ni gestionar la implementación de una infraestructura alterna geográficamente independiente, contraviniendo la normativa aplicable[59]. Debido a la inacción del Jefe de la Oficina de Administración, quien conforme a la normativa interna es responsable de la ejecución del Plan de Contingencia Informático, respecto a la adopción de medidas oportunas para garantizar la ubicación en una sede alterna del Datacenter de Contingencia y el aseguramiento de la capacidad eléctrica requerida para su funcionamiento, pese a las advertencias técnicas formuladas[60]. **(Irregularidad única).**

VI. RECOMENDACIÓN

Al Jefe del Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres:

Realizar las acciones tendentes a fin que el órgano competente efectúe el deslinde de las responsabilidades que correspondan, de los funcionarios del Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres comprendidos en los hechos observados del presente Informe de Control Específico, de acuerdo a las normas que regulan la materia. **(Conclusión única).**

59 Plan de Continuidad Operativa v2.0 del CENEPRED, el Plan de Contingencia Informático (Directiva N.° 01-2016-CENEPRED/SG/OA) y la normativa técnica aplicable (NTP ISO/IEC TS 22237 y NTP ISO/IEC 27001).

60 Previamente por la propia Unidad Funcional de Informática

VII. APÉNDICES

Apéndice n.° 1. Relación de personas comprendidas en la Irregularidad.
Apéndice n.° 2. Argumentos jurídicos por presunta responsabilidad administrativa funcional no sujeta a la potestad sancionadora de la Contraloría.
Apéndice n.° 3. Impresión de contrato n.° 003-2024-CENEPRED/OA de 5 de agosto de 2024, en copia fedateada
Apéndice n.° 4. Impresión Bases Integradas de la contratación directa n.° 002-2024-CENEPRED-1 para el Mejoramiento de la Plataforma Tecnológica del Sistema de Información para la Gestión del Riesgo de Desastres (Sigrid) ante la ocurrencia de inundaciones y movimientos en masa como consecuencia del probable Fenómeno El Niño 2023-2024, en copia simple.
Apéndice n.° 5. Impresión de informe n.° 00011-2025-CENEPRED-OA-UFI-JCA de 14 de febrero de 2025, en copia fedateada.
Apéndice n.° 6. Impresión de informe n.° 00022-2025-CENEPRED-OA/UFI de 17 de febrero de 2025, con firma digital.
Apéndice n.° 7. Impresión de informe n.° 00019-2025-CENEPRED-OA/UFI de 17 de febrero de 2025, con firma digital.
Apéndice n.° 8. Impresión de informe n.° 00005-2025-CENEPRED-OA-UFI-JCA de 10 de febrero de 2025, en copia fedateada.
Apéndice n.° 9. Impresión de oficio n.° 00290-2025-CENEPRED/SG, del 12 de marzo de 2025, con firma digital.
Apéndice n.° 10. Impresión de informe n.° 00161-2025-CENEPRED/OA/UFL de 7 de marzo de 2025, con firma digital.
Apéndice n.° 11. Impresión de informe n.° 055-2025-CENEPRED/DGP/SGI de 11 de marzo del 2025, con firma digital.
Apéndice n.° 12. Impresión de informe n.° 00030-2025-CENEPRED/DGP de 11 de marzo del 2025, con firma digital.
Apéndice n.° 13. Impresión de informe n.° 00035-2025-CENEPRED/DIMSE de 11 de marzo de 2025, con firma digital.
Apéndice n.° 14. Impresión de informe técnico n.° 0007-2025-CENEPRED/DIMSE/MARA de 10 de marzo de 2025, en copia fedateada.
Apéndice n.° 15. Impresión de documento CHA.0760860.2025 de 26 de marzo de 2025, en copia fedateada.
Apéndice n.° 16. Impresión de oficio n.° 00799-2025-CENEPRED/SG de 11 de julio de 2025, con firma digital.
Apéndice n.° 17. Impresión de informe n.° 00166-2025-CENEPRED/DGP/SGI de 11 de julio de 2025, con firma digital.
Apéndice n.° 18. Impresión de informe técnico n.° 138-2025-CENEPRED/DGP/SGI de 4 de junio de 2025, en copia simple
Apéndice n.° 19. Impresión de memorándum n.° 0185-2024-CENEPRED/DGP de 16 de abril de 2024, con firma digital.
Apéndice n.° 20. Impresión de Resolución Jefatural n.° 061-2024-CENEPRED/J de 30 de mayo de

2024, con firma digital.

Apéndice n.° 21. Impresión de memorándum n.° 00621-2025-CENEPRED/OA de 16 de julio de 2025, con firma digital.

Apéndice n.° 22. Impresión de informe n.° 00108-2025-CENEPRED-OA/UFI de 15 de julio de 2025, con firma digital.

Apéndice n.° 23. Impresión de informe n.° 00057-2025-CENEPRED-OA/UFI de 21 de abril de 2025, con firma digital.

Apéndice n.° 24. Impresión de oficio n.° 00450-2025-CENEPRED/SG de 15 de abril de 2025, con firma digital.

Apéndice n.° 25. Impresión de informe n.° 0093-2025-CENEPRED/DGP/SGI de 14 de abril de 2025, con firma digital.

Apéndice n.° 26. Impresión de Reporte de Accesos al SIGRID de los días 3, 4, 5 y 6 de marzo de 2025, con firma digital.

Apéndice n.° 27. Impresión de oficio n.° 00484-2025-CENEPRED/SG de 25 de abril de 2025, con firma digital.

Apéndice n.° 28. Impresión de informe n.° 007-2025-CENEPRED/DIFAT-MASS de 25 de abril de 2025, en copia simple.

CENEPRED V°B° Jefe OCI (e)

Apéndice n.° 29. Impresión de oficio n.° 00800-2025-CENEPRED/SG de 14 de julio de 2025, con firma digital.

Apéndice n.° 30. Impresión de informe n.° 00162-2025-CENEPRED/OA de 14 de julio de 2025, con firma digital.

Apéndice n.° 31. Impresión de informe n.° 00105-2025-CENEPRED-OA/UFI de 11 de julio de 2025, con firma digital.

CENEPRED SUPERVISOR ÓRGANO DE CONTROL INSTITUCIONAL

Apéndice n.° 32. Impresión de informe n.° 0044-2025-CENEPRED/OA/UFI/JCA de 10 de julio de 2025, en copia simple.

Apéndice n.° 33. Impresión de Reporte de accesos al Sistradoc de los días 3, 4, y 6 de marzo de 2025, en copia simple.

Apéndice n.° 34. Impresión de oficio n.° 00478-2025-CENEPRED/SG de 22 de abril de 2025, con firma digital.

Apéndice n.° 35. Impresión de informe n.° 00058-2025-CENEPRED-OA/UFI de 21 de abril de 2025, con firma digital.

CENEPRED JEFE DE COMISIÓN OCI

Apéndice n.° 36. Cédula de notificación, Pliego de hechos, 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.

- Impresión de Pliego de Hechos, con firma digital.
- Impresión de Cédula de Notificación n.° 001-2025-CG/OCI-SCE-001-CENEPRED de 5 de agosto de 2025, con firma digital.
- Impresión de Cédula de Notificación Electrónica n.° 00000005-2025-CG/5775-02-001 de 5 de agosto de 2025, con firma digital.

CENEPRED ABOGADO OCI

- Impresión de Cargo de notificación de la Cédula de Notificación n.° 01-2025, con firma digital.
- Impresión de Carta n.° 001-2025-EHM de 11 de agosto de 2025 solicitud de prórroga de plazo, presentado por la señora **Zoila Elena Huamán**, con firma digital.
- Impresión de Documento n.° 001-2025-CG/OCI-SCE-CENEPRED de 11 de agosto de 2025, respuesta de solicitud de ampliación de plazo, con firma digital.
- Impresión de Cédula de Notificación Electrónica n.° 00000006-2025-CG/5775-02-001 del 11 de agosto de 2025, con firma digital.
- Impresión de Cargo de Notificación de Carta N° 001-2025-CG/OCI-SCE-CENEPRED de 11 de agosto de 2025. Con firma digital.
- Impresión de correo institucional de 11 de agosto de 2025, en copia simple.
- Impresión de Carta n.° 002-2025-ZEHM de 11 de agosto de 2025, con firma digital.
- Impresión de Carta n.° 003-2025-ZEHM de 19 de agosto de 2025, comentarios y aclaraciones de la señora **Zoila Elena Huamán Marky**, con firma digital.

CENEPRED V°B° Jefe OCI (e)

- Impresión de Cédula de Notificación n.° 002-2025-CG/OCI-SCE-001-CENEPRED de 5 de agosto de 2025, con firma digital.
- Impresión de Cédula de Notificación Electrónica n.° 00000004-2025-CG/5775-02-001 del 5 de agosto de 2025, con firma digital.
- Impresión de Cargo de Notificación de la Cédula de Notificación n.° 02-2025, con firma digital.
- Impresión de Oficio n.° 00063-2025-CENEPRED/OA de 13 de agosto de 2025 (solicitud de ampliación de plazo) con firma digital.
- Impresión de oficio n.° 00066-2025-CENEPRED/OA de 21 de agosto de 2025, comentarios o aclaraciones del señor **Elvis Renzo Revilla Llerena**, con firma digital.

CENEPRED SUPERVISOR ÓRGANO DE CONTROL INSTITUCIONAL

Evaluación de comentarios o aclaraciones elaborada por la Comisión de Control

CENEPRED JEFE DE COMISIÓN OCI

Apéndice n.° 37. Documentos de gestión de la entidad o dependencia que sustentan el incumplimiento funcional/disciplinario de las personas involucradas en los hechos específicos presuntamente irregulares

- Impresión de Resolución Jefatural n.° 00051-2024-CENEPRED/J de 30 de abril de 2024, con firma digital.
- Impresión de Contrato Administrativo de Servicios n.° 026-2024-CENEPRED de 1 de mayo de 2024, en copia fedateada.

CENEPRED ABOGADO OCI

- Impresión de Resolución Jefatural n.° 00009-2025-CENEPRED/J de 3 de febrero de 2025, con firma digital.
- Impresión de Contrato Administrativo de Servicios n.° 001-2025-CENEPRED de 4 de febrero de 2025, en copia fedateada.

Apéndice n.° 38. Documento de gestión

- Impresión del Decreto Supremo n.° 104-2012-PCM de 18 de octubre de 2012, publicado en el Diario Oficial El Peruano / Normas Legales - Reglamento de Organización y Funciones del Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres – Cenepred, en copia simple.

Lima, 3 de setiembre de 2025

Santiago Ysidro Rodriguez Davila
Supervisor
Comisión de Control

Margarita Albina Nagaki Muñoz
Jefa de Comisión de Control

María Teresa Meléndez Lázaro
Abogada de la Comisión de Control

El jefe (e) del Órgano de Control Institucional que suscribe el presente Informe, ha revisado su contenido y lo hace suyo, procediendo a su aprobación.

Lima, 3 de setiembre de 2025

Santiago Ysidro Rodriguez Davila
Jefe (e) del Órgano de Control Institucional
Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres - CENEPRED

CONTRALORÍA
GENERAL DE LA REPÚBLICA DEL PERÚ

CENEPRED

Apéndice n.° 1

Relación de personas comprendidas en la Irregularidad.



CONTRALORÍA
GENERAL DE LA REPÚBLICA DEL PERÚ

CENEPRED

APÉNDICE N° 1 DEL INFORME DE CONTROL ESPECÍFICO N° 007-2025-2-5775-SCE

RELACIÓN DE PERSONAS COMPRENDIDAS EN LA IRREGULARIDAD

N°	Sumilla del Hecho con evidencia de Irregularidad	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 (Marcar con X)			
					Desde	Hasta				Civil	Penal	Administrativa funcional	
												Sujeta a la potestad sancionadora de la Contraloría	Entidad (*)
1	FUNCIONARIOS DEL CENEPRED NO GESTIONARON LA INSTALACIÓN DEL DATACENTER DE CONTINGENCIA EN UNA UBICACIÓN GEOGRÁFICA DISTINTA A LA SEDE INSTITUCIONAL, LO QUE OCASIONÓ LA INOPERATIVIDAD DE PROCESOS CRÍTICOS Y MISIONALES ASI COMO DE LOS SISTEMAS DE GESTIÓN ADMINISTRATIVA DURANTE LOS CORTES DE ENERGÍA ELÉCTRICA OCURRIDOS EN MARZO DE 2025.	Zoila Elena Huamán Marky	[redacted]	Jefa de la Oficina de Administración	1/5/2024	3/2/2025	CAS	[redacted]	–				X
2		Elvis Renzo Revilla Llerena	[redacted]	Jefe de la Oficina de Administración	4/2/2025	Actualidad	CAS	[redacted]	–				X

CENEPRED Jefe OCI (e)

CENEPRED SUPERVISOR ORGANO DE CONTROL INSTITUCIONAL

CENEPRED JEFE DE COMISIÓN OCI

CENEPRED ABOGADO OCI

000053

Firmado digitalmente por: RODRIGUEZ DÁVILA Santiago Ysidro FAU 20543891755 soft
Motivo: Soy el autor del documento
Fecha: 03/09/2025 16:01:01-0500

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año de la recuperación y consolidación de la economía peruana"

CENEPRED V° B° 10067326 OCI

San Isidro, 3 de setiembre de 2025

OFICIO N° 00161-2025-CENEPRED/OCI

Señor
ROLANDO CAPUCHO CARDENAS
Jefe Institucional
Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres - CENEPRED
Av. del Parque Norte N° 829 - 833, Urb. Córpac
San Isidro, Lima Lima

Asunto: Remite Informe de Control Específico n.° 007-2025-2-5775-SCE.

Referencia:
a) Oficio n.° 00140-2025-CENEPRED/OCI de 7 julio de 2025.
b) Directiva n.° 007-2021-CG/NORM "Servicio de Control Específico a Hechos con Presunta Irregularidad" aprobada mediante Resolución de Contraloría n.° 134-2021-CG, de 12 de junio de 2021 y modificatorias

---

Me dirijo a usted en relación al documento de la referencia a), mediante el cual se comunicó el inicio del Servicio de Control Específico a Hechos con Presunta Irregularidad a la ***"Acondicionamiento del Datacenter de Contingencia del Cenepred",*** en el Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres – CENEPRED a su cargo.

Sobre el particular, como resultado del Servicio de Control Especifico a Hechos con Presunta Irregularidad, se ha emitido el Informe de Control Específico n.° n.° 007-2025-2-5775-SCE, periodo de 10 de octubre de 2024 al 6 de marzo de 2025, con sus apéndices en un (1) tomo, conteniendo quinientos noventa y dos (592) folios, el cual se remite a su despacho para su conocimiento con el propósito que en su condición de Titular de la entidad examinada disponga las acciones necesarias para la elaboración del Plan de Acción, que deberá ser remitido al Órgano de Control Institucional en el plazo de veinte (20) días hábiles contados a partir del día hábil siguiente de recibido el presente informe de control, conforme a lo establecido en la normativa de la referencia b).

Es propicia la oportunidad para expresarle las seguridades de mi consideración.

Atentamente,

Documento firmado digitalmente

Santiago Rodriguez Dávila
Jefe (e) del Órgano de Control Institucional
Centro Nacional de Estimación, Prevención y
Reducción del Riesgo de Desastres

SRD

Esta es una copia auténtica imprimible de un documento electrónico archivado en el CENEPRED, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://cenepred.gob.pe/web/sistradoc/verifica_digital.php e ingresando los siguientes datos: Código: BNQEC, clave: 5265

Ponle Punche y ganamos todos PERÚ

Firmado digitalmente por MELÉNDEZ LÁZARO María Teresa FAU 20543891755 soft
Motivo: Soy el autor del documento
Fecha: 03-09-2025 17:50:05 -05:00

CONTRALORÍA
GENERAL DE LA REPÚBLICA DEL PERÚ

CÉDULA DE NOTIFICACIÓN ELECTRÓNICA N° 00000007-2025-CG/5775-02-001

DOCUMENTO	:	OFICIO N° N° 00161-2025-CENEPRED/OCI
EMISOR	:	SANTIAGO YSIDRO RODRIGUEZ DAVILA - SUPERVISOR - DATACENTER DE CONTINGENCIA - ÓRGANO DE CONTROL INSTITUCIONAL
DESTINATARIO	:	ROLANDO GUSTAVO CAPUCHO CARDENAS
ENTIDAD SUJETA A CONTROL	:	CENTRO NACIONAL DE ESTIMACION, PREVENCION Y REDUCCION DEL RIESGO DE DESASTRES (CENEPRED)
DIRECCIÓN	:	CASILLA ELECTRÓNICA N° 20543891755
TIPO DE SERVICIO CONTROL GUBERNAMENTAL O PROCESO ADMINISTRATIVO	:	SERVICIO DE CONTROL POSTERIOR
N° FOLIOS	:	1163

Sumilla: Notificación de Informe de Servicio de Control Específico n.° 007-2025-2-5775-SCE

Se adjunta lo siguiente:

1. INFORME 7-2025-SCE y APÉNDICE 1[F]
2. OFICIO N° 00161-2025-CENEPRED-OCI[F]
3. INFORME 7-2025-SCE-APÉNDICE 20 AL 35[F]
4. INFORME 7-2025-SCE-APÉNDICE 37-38[F]
5. INFORME 7-2025-SCE-APÉNDICE 2 AL 19[F]
6. INF 7-APÉNDICE 36 PRIMERA PARTE[F]
7. INF 7-APÉNDICE 36 SEGUNDA PARTE[F]

Esta es una copia auténtica imprimible de un documento electrónico archivado por la Contraloría General de la República, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: **https://verificadoc.contraloria.gob.pe/ecasilla** e ingresando el siguiente código de verificación: **95BUPWW**

Firmado digitalmente por Agente Automatizado CGR
Motivo: Soy el autor del documento
Fecha: 03-09-2025 17:50:49 -05:00

CONTRALORÍA
GENERAL DE LA REPÚBLICA DEL PERÚ

CARGO DE NOTIFICACIÓN

Sistema de Notificaciones y Casillas Electrónicas - eCasilla CGR

DOCUMENTO	:	OFICIO N° N° 00161-2025-CENEPRED/OCI
EMISOR	:	SANTIAGO YSIDRO RODRIGUEZ DAVILA - SUPERVISOR - DATACENTER DE CONTINGENCIA - ÓRGANO DE CONTROL INSTITUCIONAL
DESTINATARIO	:	ROLANDO GUSTAVO CAPUCHO CARDENAS
ENTIDAD SUJETA A CONTROL	:	CENTRO NACIONAL DE ESTIMACION, PREVENCION Y REDUCCION DEL RIESGO DE DESASTRES (CENEPRED)

Sumilla:

Notificación de Informe de Servicio de Control Específico n.° 007-2025-2-5775-SCE

Se ha realizado la notificación con el depósito de los siguientes documentos en la **CASILLA ELECTRÓNICA N° 20543891755**:

1. CÉDULA DE NOTIFICACIÓN N° 00000007-2025-CG/5775-02-001
2. INFORME 7-2025-SCE y APÉNDICE 1[F]
3. OFICIO N° 00161-2025-CENEPRED-OCI[F]
4. INFORME 7-2025-SCE-APÉNDICE 20 AL 35[F]
5. INFORME 7-2025-SCE-APÉNDICE 37-38[F]
6. INFORME 7-2025-SCE-APÉNDICE 2 AL 19[F]
7. INF 7-APÉNDICE 36 PRIMERA PARTE[F]
8. INF 7-APÉNDICE 36 SEGUNDA PARTE[F]

NOTIFICADOR : MARÍA TERESA MELÉNDEZ LÁZARO - CENTRO NACIONAL DE ESTIMACIÓN, PREVENCIÓN Y REDUCCIÓN DEL RIESGO DE DESASTRES - CENEPRED - CONTRALORÍA GENERAL DE LA REPÚBLICA

Esta es una copia auténtica imprimible de un documento electrónico archivado por la Contraloría General de la República, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: **https://verificadoc.contraloria.gob.pe/ecasilla** e ingresando el siguiente código de verificación: **9B778DN**