ÓRGANO DE CONTROL INSTITUCIONAL

INFORME DE HITO DE CONTROL N° 008-2021-OCI/5963-SCC

CONTROL CONCURRENTE
PROGRAMA NACIONAL DE ASISTENCIA SOLIDARIA PENSIÓN 65
SAN ISIDRO, LIMA, LIMA

"PROCESO DE DETERMINACIÓN DE POTENCIALES USUARIOS Y COTEJO DE INFORMACIÓN ASI COMO DETERMINACIÓN DE CASOS SENSIBLES DE VULNERABILIDAD ADICIONAL EN EL MARCO DE LA AFILIACIÓN DE USUARIOS PARA LA ENTREGA DE SUBVENCIÓN MONETARIA EN EL AMBITO NACIONAL"

HITO DE CONTROL N° 2
COTEJO DE INFORMACIÓN.

PERÍODO DE EVALUACIÓN DEL HITO DE CONTROL:
DEL11 DE MAYO AL 24 DE MAYO DE 2021

TOMO I DE I

SAN ISIDRO, 24 DE MAYO DE 2021

INFORME HITO DE CONTROL N° 008-2021-OCI/5963-SCC

"PROCESO DE DETERMINACIÓN DE POTENCIALES USUARIOS Y COTEJO DE INFORMACIÓN ASI COMO DETERMINACIÓN DE CASOS SENSIBLES DE VULNERABILIDAD ADICIONAL EN EL MARCO DE LA AFILIACIÓN DE USUARIOS PARA LA ENTREGA DE SUBVENCIÓN MONETARIA EN EL AMBITO NACIONAL"

HITO DE CONTROL N° 2 - COTEJO DE INFORMACIÓN.

ÍNDICE

DENOMINACIÓN		N° Pág.
I.	ORIGEN	4
II.	OBJETIVOS	4
III.	ALCANCE	4
IV.	INFORMACIÓN RESPECTO DEL HITO CONTROL	4
V.	SITUACIONES ADVERSAS	9
	1. PERSONAL DE LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN UTILIZA UN USUARIO COMÚN PARA ACCEDER AL SERVIDOR DE BASE DE DATOS, DONDE SE REALIZAN LOS TRABAJOS DE COTEJO DE DATOS, LO CUAL PODRÍA PERMITIR QUE INTENCIONALMENTE O POR ERROR, SEA PASIBLE DE SER MODIFICADA, BORRADA, COPIADA O EXTRAÍDA DICHA INFORMACIÓN, SIN QUE SE PUEDA CONOCER LA IDENTIDAD DE QUIEN OCASIONARÍA TALES PERJUICIOS.	
	2. SE IDENTIFICARON VULNERABILIDADES DE SEGURIDAD EN EL PORTAL WEB DE PENSIÓN 65 LO CUAL OCASIONARÍA EL RIESGO DE AFECTACIÓN A LA INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN REFERENTE A LA DIFUSIÓN DE LA RELACIÓN BIMESTRAL DE USUARIOS (RBU), INFORMACIÓN PÚBLICA QUE ES DE INTERÉS A LOS BENEFICIARIOS DEL PROGRAMA.	
VI.	DOCUMENTACIÓN VINCULADA AL HITO CONTROL	16
VII.	INFORMACIÓN DEL REPORTE DE AVANCE ANTE SITUACIONES ADVERSAS	17
VIII.	INFORMACIÓN DE LAS SITUACIONES ADVERSAS COMUNICADAS EN HITOS ANTERIORES	17
IX.	CONCLUSIONES	17

X. RECOMENDACIONES 17

APÉNDICE 19

INFORME DE HITO DE CONTROL N° 008 -2021-OCI/5963-SCC

"PROCESO DE DETERMINACIÓN DE POTENCIALES USUARIOS Y COTEJO DE INFORMACIÓN ASI COMO DETERMINACIÓN DE CASOS SENSIBLES DE VULNERABILIDAD ADICIONAL EN EL MARCO DE LA AFILIACIÓN DE USUARIOS PARA LA ENTREGA DE SUBVENCIÓN MONETARIA EN EL AMBITO NACIONAL"

HITO DE CONTROL N° 2 - COTEJO DE INFORMACIÓN.

I. ORIGEN

El presente informe se emite en mérito a lo dispuesto por el Órgano de Control Institucional (OCI) del Programa Nacional de Asistencia Solidaria Pensión 65, en adelante Programa "Pensión 65", mediante Oficio n.° D000017-2021-PENSION65-OCI de 22 de abril de 2021, registrado en el Sistema de Control Gubernamental – SCG con la Orden de Servicio n.° 5963-2021-008, en el marco de lo previsto en la Directiva n.° 002-2019-CG/NORM "Servicio de Control Simultáneo" aprobada mediante Resolución de Contraloría n.° 115-2019-CG de 28 de marzo de 2019, modificada por Resolución de Contraloría n.° 100-200-CG de 28 de marzo de 2020, Resolución de Contraloría n.° 144-2020-CG de 26 de mayo de 2020 y Resolución de Contraloría n.° 200-2020-CG de 14 de julio de 2020.

II. OBJETIVOS

2.1. Objetivo general

Determinar si el Programa "Pensión 65" viene ejecutando el proceso de determinación de potenciales usuarios y cotejo de información, así como el de casos sensibles de vulnerabilidad adicional, en el marco del proceso de afiliación de usuarios para la entrega de subvención monetaria en el ámbito Nacional, se realiza en concordancia con las disposiciones establecidas en la normatividad vigente.

2.2. Objetivo específico del Hito de Control n.° 2

Determinar si el Cotejo de Información correspondiente al proceso de Identificación de usuarios, se viene ejecutando en concordancia con las disposiciones establecidas en la normatividad vigente.

III. ALCANCE

El presente servicio de Control Concurrente se desarrolló al Hito de control n.° 2 "Cotejo de Información" y ha sido ejecutado del 11 al 24 de mayo de 2021, en los ambientes del Programa "Pensión 65", ubicado la Avenida República de Panamá 3505, San Isidro, Lima, Lima.

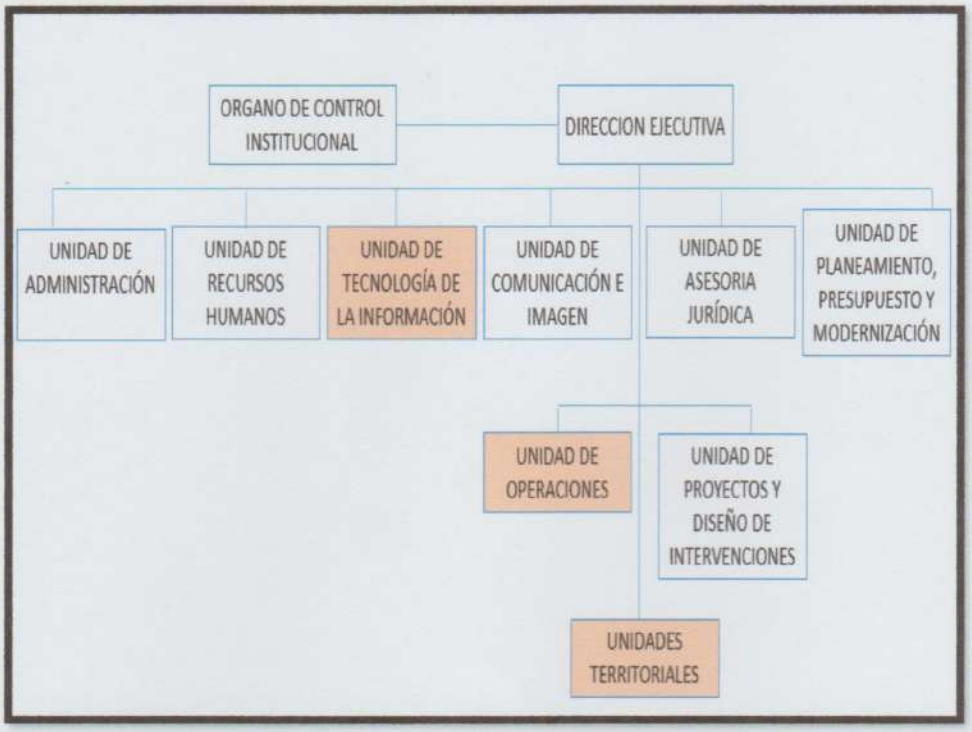
IV. INFORMACIÓN RESPECTO DEL HITO DE CONTROL

El Programa "Pensión 65" es un programa del Ministerio de Desarrollo e Inclusión Social (Midis), creado con el propósito de otorgar subvenciones económicas a los adultos en condición de extrema pobreza a partir de los sesenta y cinco (65) años de edad que cumplan con los requisitos establecidos en el Decreto Supremo n.° 081-2011-PCM de 19 de octubre de 2011, su norma de creación.

Mediante la Resolución Ministerial n.° 273-2017-MIDIS de 11 de diciembre de 2017, el Midis aprobó el Manual de Operaciones (MOP) del Programa "Pensión 65"; dicho manual establece la estructura orgánica y las funciones de las unidades orgánicas que integran el mencionado programa.

La estructura orgánica es la siguiente:

Gráfico n.° 1
Estructura Orgánica



Fuente: Manual de Operaciones (MOP) del Programa "Pensión 65", aprobado por Resolución Ministerial n.° 273-2017-MIDIS de 11 de diciembre de 2017.
Elaborado por: Comisión de control a cargo del servicio de Control Concurrente.

Para efecto del presente servicio de control, las áreas involucradas a nivel de Programa "Pensión 65" son: i) la Dirección Ejecutiva, ii) la Unidad de Administración – UA, iii) Unidad de Operaciones - UO iv) Unidad de Tecnologías de la Información – UTI, v) Unidades Territoriales – UT.

Al respecto, el artículo 9º del MOP establece las funciones de la **Dirección Ejecutiva - DE**, siendo las principales las siguientes:

a) Organizar, dirigir y supervisar la gestión del programa, así como evaluar el cumplimiento de sus objetivos y planes, en el marco de la normatividad vigente.
(...)
jj) Otras que le correspondan conforme a ley, y demás funciones que en marco de su competencia le sean asignadas por el Viceministerio de Prestaciones Sociales del Ministerio de Desarrollo e Inclusión Social.

En el artículo 16° del MOP se establece las funciones de la **Unidad de Administración - UA**, siendo las principales las siguientes:

d) Conducir y supervisar la ejecución financiera en sus fases de solicitud de certificación, compromiso, devengado y girado para una ejecución oportuna del presupuesto e informar oportunamente a la Unidad de Planeamiento, Presupuesto y Modernización del Programa Nacional.

En el artículo 25° del MOP se establece las funciones de la **Unidad de Operaciones - UO**, siendo las principales las siguientes:

a) Planificar, dirigir, coordinar y controlar el cumplimiento de las funciones y actividades para el logro de los objetivos de la Unidad de Operaciones, de conformidad con los lineamientos y directivas dispuestas por la Dirección Ejecutiva, en el marco de las políticas y lineamientos dictados por el Ministerio de Desarrollo e Inclusión Social - MIDIS y las disposiciones vigentes.
b) Dirigir, programar y ejecutar los procesos de afiliación de los usuarios de "Pensión 65", verificando el cumplimiento de los requisitos conforme a la normatividad vigente.
c) Dirigir, programar y ejecutar los procesos de transferencia monetarias a usuarios de "Pensión 65", sobre la base de la Relación Bimestral de Usuarios aprobada por la Dirección Ejecutiva.
d) Dirigir, supervisar y controlar el proceso de elaboración de la Relación Bimestral de Usuarios, luego de recibida la información procesada por la Unidad de Tecnologías de la Información - UTI, resultante de los procesos de cotejo de requisitos de acceso y permanencia al Programa "Pensión 65" que incluye aquella recibida del trabajo de campo debidamente aprobada por las jefaturas de las Unidades Territoriales – UT del Programa "Pensión 65".
(...)
h) Coordinar con la Dirección de Operaciones de Focalización (DOF) del MIDIS el acceso a la información producida por el SISFOH con la certificación de la clasificación socioeconómica de los usuarios y potenciales usuarios del Programa "Pensión 65", teniendo en cuenta las consideraciones normativas del Sistema Nacional de Focalización (SINAFO).
(...)
k) Elaborar y mantener actualizada la Relación de Usuarios del Programa correspondiente a cada periodo de entrega de subvenciones monetarias.
(...)
q) Coordinar y brindar la información que reciba de los procesos de afiliación y verificación de requisitos a la Unidad de Tecnologías de la Información, con la finalidad de que se mantengan actualizadas las bases de datos generadas para el cumplimiento de las funciones de su competencia y para el seguimiento y evaluación de la operación del programa.

Asimismo, el artículo 21° del MOP establece las funciones de la **Unidad de Tecnologías de la Información - UTI**, siendo las principales las siguientes:

(...)
q) Implementar, mantener y actualizar los sistemas y/o aplicativos informáticos desarrollados para el cumplimiento de las funciones de su competencia y para el seguimiento y evaluación de la operación del Programa Nacional.
(...)
w) Velar por el registro oportuno y consistente de datos de información en los aplicativos informáticos institucionales de su competencia.
x) Definir e implementar mecanismos que permitan disponer de información confiable y oportuna del Programa.

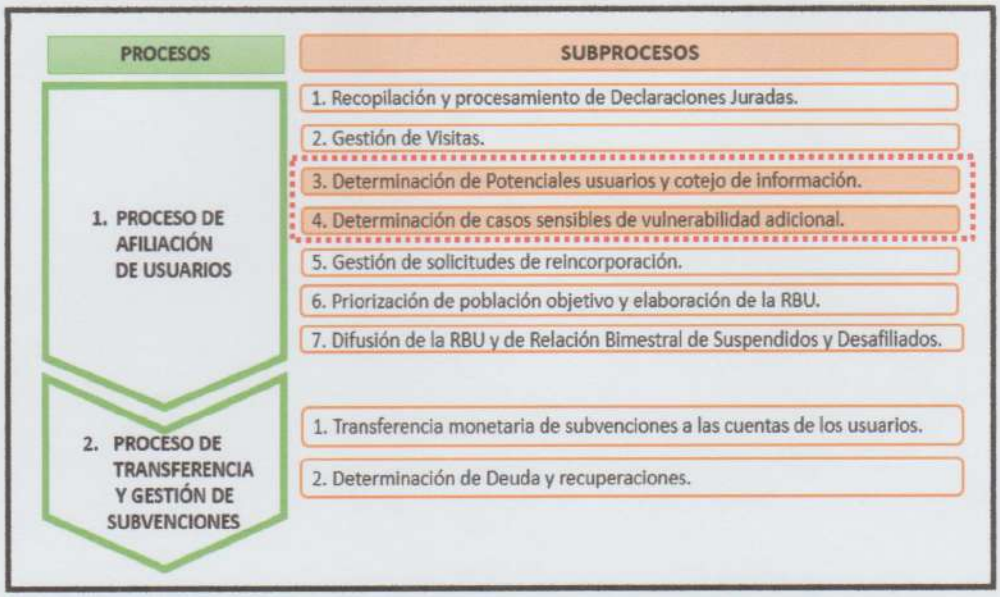
Finalmente, en el artículo 29° del MOP se establece las funciones de las **Unidades Territoriales - UT**, siendo las principales las siguientes:

a) Ejecutar, supervisar y evaluar las actividades relacionadas con los procesos de: afiliación y verificación de requisitos, programación y transferencia monetaria a usuarios, y gestión de prestaciones complementarias a los usuarios del programa, que le hayan sido encomendadas y coadyuven en el cumplimiento de los objetivos del programa, en concordancia con los lineamientos, directivas, criterios e instrumentos técnicos dictados por la Dirección Ejecutiva en el marco de las políticas y lineamientos dispuestos por el MIDIS.
b) Apoyar en los operativos de entrega de subvención monetaria realizados por el programa, efectuando la evaluación de su resultado.
(...)
l) Ejecutar y supervisar en su ámbito de trabajo las actividades relacionadas con el acopio de evidencias de las condiciones de vulnerabilidad de adultos mayores, potenciales usuarios, usuarios y ex usuarios; mediante visitas domiciliarias.

DATOS DEL PROCESO

La Directiva "Gestión de la entrega de Subvención Monetaria" del Programa "Pensión 65", aprobada mediante Resolución Directoral n.° 078-2019-MIDIS/P65-DE de 6 de agosto de 2019, regula los procesos y subprocesos siguientes:

Gráfico n.° 2
Procesos y Subprocesos de la Gestión de Entrega de Subvención Monetaria



Fuente: Directiva "Gestión de la entrega de Subvención Monetaria" del Programa "Pensión 65", aprobada mediante Resolución Directoral n.° 078-2019-MIDIS/P65-DE de 6 de agosto de 2019.
Elaborado por: Comisión de Control a cargo del servicio del Control Concurrente.

Como se puede apreciar en el Gráfico n.° 2, uno de los procesos que forman parte de la Gestión de la Entrega de Subvención Monetaria es el proceso de Afiliación de Usuarios del Programa "Pensión 65".

El proceso de Afiliación de Usuarios del Programa "Pensión 65", es un acto administrativo que tiene como propósito la declaración de cumplimiento de los requisitos de acceso previsto en el Decreto Supremo n.° 081-2011-PCM de 19 de octubre de 2011 y sus modificatorias que permite a una persona adulta mayor ser usuario/a del Programa "Pensión 65".

Al incorporarse un adulto mayor como usuario, el Programa "Pensión 65" le abre una cuenta de ahorros en el Banco de la Nación a la cual se le transfiere cada dos meses el monto de la subvención monetaria. Tanto la creación de la cuenta, como la transferencia de la subvención al Banco de la Nación, las coordinan y realizan las Unidades de Operaciones y de Administración.

Asimismo, el Gráfico n.° 2 muestra, entre otros, el subproceso de Determinación de Potenciales Usuarios y Cotejo de Información, el cual es materia del presente Hito de Control n.° 2, cuya gestión operativa se detalla a continuación:

Determinación de Potenciales usuarios y cotejo de información:

El subproceso Determinación de Potenciales usuarios y cotejo de información, inicia con las actividades de la Coordinación de Afiliaciones del Programa "Pensión 65", la cual a través de la Unidad de Operaciones, solicita a la Dirección de Focalización – DOF del Midis, la relación de los potenciales usuarios[1] y la Certificación de la Clasificación Socio Económica – CSE de los usuarios del Programa "Pensión 65" registrados en el registro Nacional de Usuarios – RNU del Midis en el período anterior.

Dicha información, a su vez es entregada a la Unidad de Tecnologías de la Información – UTI del Programa "Pensión 65" a fin que esta sea ingresado en la base de datos del programa.

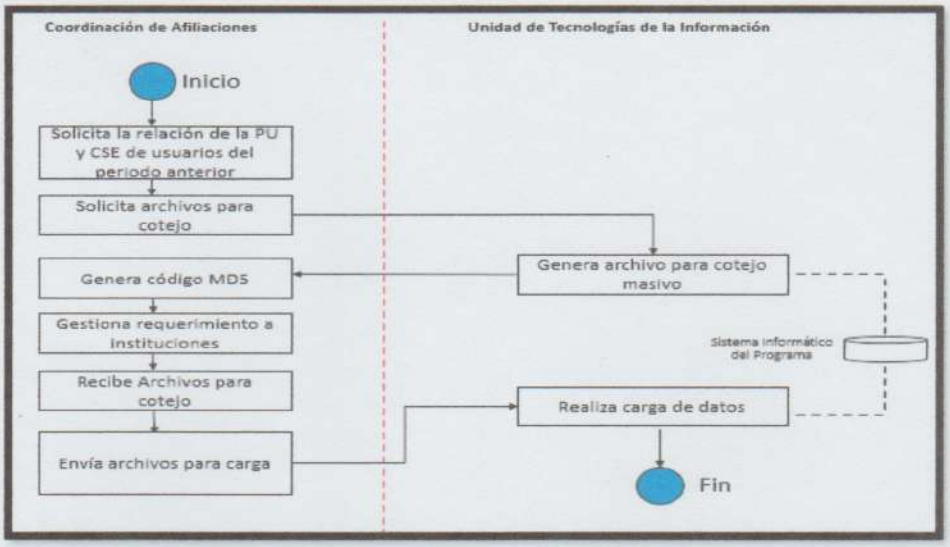
Posteriormente, solicita la generación de los archivos para el cotejo masivo de información con otras entidades a fin de evitar duplicidad de subvenciones, para que luego la Coordinación de Afiliaciones genere un código de seguridad para dichos archivos y las envié a las entidades externas.

Finalmente, la respuesta por parte de éstas de la información sobre los cotejos, es entregada a la Unidad de Tecnologías de la Información e ingresada al sistema informático de Pensión 65.

Las actividades e interacciones del subproceso Determinación de Potenciales usuarios y cotejo de información se muestran a continuación:

[1] Conforme a la Directiva "Gestión de la entrega de Subvención Monetaria" del Programa "Pensión 65", aprobada mediante Resolución Directoral n.° 078-2019-MIDIS/P65-DE, se define Potencial Usuario: Persona adulta mayor de 65 que cuenta con una clasificación socioeconómica de pobre extremo de acuerdo con el Sistema de Focalización de Hogares – SISFOH, certificada por la Dirección de Operaciones de Focalización del Midis.

Gráfico n.° 3
Subproceso de Determinación de Potenciales Usuarios y Cotejo de Información



Fuente: Directiva "Gestión de la entrega de Subvención Monetaria" del Programa "Pensión 65", aprobada mediante Resolución Directoral n.° 078-2019-MIDIS/P65-DE de 6 de agosto de 2019.

V. SITUACIONES ADVERSAS

De la revisión efectuada al Hito de Control n.° 2: "Cotejo de Información", se ha identificado dos (2) situaciones adversas que podrían afectar el cumplimiento de los objetivos del Programa, las cuales se detallan a continuación:

1. PERSONAL DE LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN UTILIZA UN USUARIO COMÚN PARA ACCEDER AL SERVIDOR DE BASE DE DATOS, DONDE SE REALIZAN LOS TRABAJOS DE COTEJO DE DATOS, LO CUAL PODRÍA PERMITIR QUE INTENCIONALMENTE O POR ERROR, SEA PASIBLE DE SER MODIFICADA, BORRADA, COPIADA O EXTRAÍDA DICHA INFORMACIÓN, SIN QUE SE PUEDA CONOCER LA IDENTIDAD DE QUIEN OCASIONARÍA TALES PERJUICIOS.

a) Condición

Durante la revisión de los procesos de Cotejo de Información realizados vía electrónica en la Unidad de Tecnología de la Información de Pensión 65, correspondiente al proceso de Identificación de Usuarios, de la etapa "Determinación de potenciales Usuarios y cotejo de información así como determinación de casos sensibles de vulnerabilidad adicional", se obtuvo, información del servidor de base de datos sobre el cual se realizan los trabajos de cotejos de datos, determinándose que existen ciertas vulnerabilidades en la seguridad de la información, originada por el acceso de dicha información a todos los colaboradores de las Unidades de Operaciones y de Tecnologías de la Información[2].

[2] Aspecto señalado en el Cuestionario de Control N°01-2021-PENSION65-OCI de 20 de mayo de 2021.

Al respecto, mediante Memorando n.° D000060- 2021-PENSION65-OCI de 20 de mayo de 2021 se solicitó a la Unidad de Tecnologías de la Información nos brinde respuesta a un cuestionario y mediante el Memorando N° D000135-2021-PENSION65-UTI-AZ de la misma fecha remitió el Cuestionario de Control n.° 01-2021-CG/PENSION65-OCI de 20 de mayo de 2021, a través del cual la citada unidad señaló que respecto al servidor de Base de datos tienen acceso los siguientes colaboradores de la Unidad de Tecnologías de la Información (UTI):

Cuadro n.° 01
Personal de UTI que Accede al Servidor de Base de datos donde se realizan los cotejos de datos

Nombre y Apellidos	Perfil	Usuario de acceso
Wilfredo Amoretti	Programador	User_p65
Elizabet Rodríguez	Programador	User_p65
Ricardo Vilela	Programador	User_p65

Fuente: Memorando N° D000135-2021-PENSION65-UTI-AZ de 20 de mayo de 2021, Cuestionario de Control n.° 01-2021-CG/PENSION65-OCI de 20 de mayo de 2021.
Elaborado por: Comisión de Control Concurrente.

De acuerdo a lo señalado por la Unidad de Tecnologías de Información, se confirma que en el Programa hay personal de la UTI que accede con un usuario común denominado "User_p65", que, si bien no cuenta con privilegios de administrador, tiene los privilegios suficientes para crear, modificar, exportar e importar información, a fin de cumplir con el proceso de cotejo de datos que se realiza en el Programa; no obstante, esta situación no permitiría identificar a las personas que accedieron o modificaron o incluso extrajeron la información de la base de datos fuera del Programa. Asimismo, cabe señalar, la identificación es la capacidad de identificar de forma exclusiva a un usuario de un sistema o una aplicación que se está ejecutando en el sistema[3].

Asimismo, dicho Cuestionario de Control, respecto a la información que se utiliza para efectuar el Cotejo de Información y que se encuentra en la Base de datos, refiere que la misma es compartida con las Unidades de Operaciones y Tecnologías de Información, por lo que carecen de medidas que protejan la citada información en el Programa, situación que podría ocasionar el riesgo que personal ajeno a las labores de Cotejo pueda tener acceso a dicha información, y pueda ser utilizada para fines que no son propios del Programa.

Cuadro n.° 02
Cuestionario de Control n.° 01-2021-CG/PENSION65-OCI

N°	PREGUNTAS	SI	NO	RESPUESTAS/ COMENTARIOS
5	Se tomó conocimiento que, los archivos que contiene las bases de datos, y que comparten de forma interna las Unidades de Operaciones y Tecnologías de Información, no tienen aplicados mecanismo de protección, pues esta información se trabaja dentro del Programa, y no es considerada sensible o confidencial; no obstante, cuando se elabora una base de datos que será remitida a una entidad externa, se aplica mecanismos de seguridad para conservar la integridad de la información que sale del Programa.	X		

Fuente: Memorando N° D000135-2021-PENSION65-UTI-AZ de 20 de mayo de 2021, Cuestionario de Control n.° 01-2021-CG/PENSION65-OCI de 20 de mayo de 2021.
Elaborado por: Comisión de Control Concurrente.

[3] Fuente: https://www.ibm.com/docs/es/ibm-mq/7.5?topic=ssfksj-7-5-0-com-ibm-mq-sec-doc-q009740--htm

b) Criterio:

- **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. 2a. Edición", aprobada mediante Resolución Ministerial n.° 246-2007-PCM de 22 de agosto del 2007.**

  "11.5.2 Identificación y autenticación del usuario

  Control
  Todos los usuarios deberían disponer de un identificador único para su uso personal y debería ser escogida una técnica de autentificación adecuada para verificar la identidad de estos.

  Guía de Implementación
  Este control debe ser aplicado para todos los tipos de usuario (incluidos los administradores de red y de bases de datos, los programadores de sistemas y el personal técnico de apoyo).
  Los ID de los usuarios deben ser utilizados para seguir la pista de las actividades de cada responsable individual. Las actividades regulares del usuario no deben ser realizadas desde cuentas privilegiadas (...)

c) Consecuencia:

La situación expuesta podría ocasionar que intencionalmente o por error, la información de la base de datos donde se realiza el proceso de cotejo de datos, sea modificada o copiada o extraída del Programa, sin que se conozca la identidad de las personas que realizaron dichas operaciones y que no se logren determinar las responsabilidades a que hubiere lugar; asimismo, al poder tener acceso a dicha información el personal ajeno al proceso de cotejo, podría generar que la misma sea utilizada para fines distintos a los que persigue el Programa, siendo su finalidad la de brindar la protección a los adultos mayores de sesenta y cinco años que se encuentran en situación de vulnerabilidad.

2. SE IDENTIFICARON VULNERABILIDADES DE SEGURIDAD EN EL PORTAL WEB DE PENSIÓN 65 LO CUAL OCASIONARÍA EL RIESGO DE AFECTACIÓN A LA INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN REFERENTE A LA DIFUSIÓN DE LA RELACIÓN BIMESTRAL DE USUARIOS (RBU), INFORMACIÓN PÚBLICA QUE ES DE INTERÉS A LOS BENEFICIARIOS DEL PROGRAMA.

a) Condición:

El Portal Web Institucional de Pensión 65, de Url[4]: https://www.pension65.gob.pe/, el cual cuenta con información pública sobre el Programa de Asistencia Solidaria Pensión 65, implementado en lenguaje de programación PHP[5] y base de datos MySql[6], es el medio por el cual se publican los padrones de usuarios o Relación Bimestral de Usuarios (RBU), el cual es el producto final del

---

[4] URL: Uniform Resource locator (Localizador Uniforme de Recursos), es la ruta que se encuentra en la caja de texto ubicada en la barra de navegación del navegador web, sirve para ubicar de manera precisa en un servidor, cualquier recurso: una imagen, un video o una página web.

[5] PHP: (acrónimo recursivo de PHP: Hypertext Preprocessor) es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML. Fuente: https://www.php.net/manual/es/intro-whatis.php.

[6] Fuente: Inventario de aplicaciones de procesos misionales remitido por correo electrónico de fecha 13 de enero de 2021, por el señor Miguel Santiago Ávila Jara, jefe de la Unidad de Tecnologías de la Información del programa, en atención al Oficio Circular n.° 000040-2020-CG/SOCC de 4 de diciembre de 2020.

proceso de afiliación de usuarios[7], así como la respectiva Resolución Directoral (RD) que la aprueba.

Al respecto, como parte del servicio de control concurrente el día 19 de mayo de 2021, por medio de un análisis de identificación de vulnerabilidades, haciendo uso de las herramientas open source gratuita ZAP[8], la cual es tomada del "Proyecto de Seguridad de Aplicaciones Web Abiertas" (OWASP[9], por sus siglas en ingles) y versión demo de la Herramienta de Escáner de vulnerabilidades de Acunetix[10], se constató la existencia de vulnerabilidades de seguridad[11] de riesgo medio y bajo, detalladas en los reportes[12], lo cual genera riesgos a la confidencialidad, integridad y disponibilidad de la información contenida en el Portal. A continuación, se presenta la lista de las vulnerabilidades de riesgo medio identificadas:

Vulnerabilidades de riesgo Medio

1. **Ausencia de tokens anti-CSRF en Formulario HTML**

   No se encontraron tokens Anti-CSRF[13] en un formulario de envío HTML. Una solicitud falsa entre sitios en un ataque que compromete y obliga a una víctima a enviar su solicitud HTTP a un destino objetivo sin su conocimiento o intención para poder realizar una acción como víctima. La naturaleza del ataque es que CSRF explota la confianza que un sitio web proporciona a un usuario, pues cualquier cosa que utilice un servidor para establecer la confianza con un navegador (por ejemplo, cookies), es exactamente lo que permite que CSRF tenga lugar, pero esta es solo la primera pieza para un ataque CSRF exitoso[14]. El impacto del ataque depende del nivel de permisos que tenga la víctima, ya que aprovechan el hecho de que un sitio web confía completamente en un usuario una vez que puede confirmar que el usuario es realmente quien dice ser[15].

   Si la víctima es un administrador o un usuario privilegiado, las consecuencias pueden incluir obtener un control completo sobre la página web: eliminar o robar datos, desinstalar el producto o usarlo para lanzar otros ataques contra todos los usuarios del producto.

---

7 Fuente: Directiva de Gestión de la Entrega de la Subvención Monetaria, aprobada por Resolución Directoral n.° 078-2019-MIDIS/P65-DE de 6 de agosto de 2019.

8 El Proxy Zed Attack (ZAP) de OWASP es una herramienta de seguridad gratuita puede ayudarlo a encontrar automáticamente vulnerabilidades de seguridad en sus aplicaciones web mientras desarrolla y prueba sus aplicaciones.
Fuente: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project.

9 OWASP, es una comunidad abierta sin fines de lucro, dedicada a permitir a las organizaciones concebir, desarrollar, adquirir, operar y mantener aplicaciones confiables.
Fuente: https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project#The_OWASP_Foundation

10 Acunetix, es una solución completa de prueba de seguridad de aplicaciones web que se puede usar tanto de forma independiente como como parte de entornos complejos. Fuente: https://www.acunetix.com/vulnerability-scanner/

11 Vulnerabilidades de seguridad. de información, según CVE® (diccionario de vulnerabilidades y exposiciones de seguridad de información de alcance internacional y libre de uso público), es un error en el software que puede ser directamente utilizado por un pirata informático para obtener acceso a un sistema o red. CVE®, considera una vulnerabilidad si se permite a un atacante utilizarlo para violar una política de seguridad razonable para el sistema. Fuente: https://cve.mitre.org/

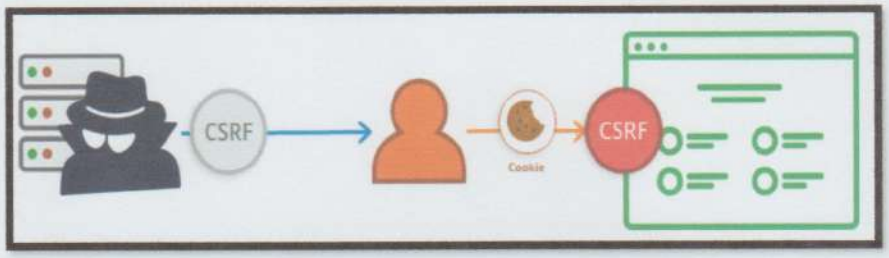
12 Reportes "Acunetix Affected Items.pdf" y "ZAP Scanning Report.html" de 19 de mayo de 2021.

13 Tokens Anti-CSRF: La técnica llamada falsificación de petición en sitios cruzados, proviene de su nombre en inglés **Cross Site Request Forgery** (**CSRF** o XSRF). Este ataque fuerza al navegador web de su víctima, validado en algún servicio (como por ejemplo correo o home banking) a enviar una petición a una aplicación web vulnerable. Fuente: https://backtrackacademy.com/articulo/anti-csrf-tokens-para-prevenir-cross-site-request-forgery-csrf.

14 https://owasp.org/www-community/Anti_CRSF_Tokens_ASP-NET

15 Fuente: https://www.acunetix.com/websitesecurity/csrf-attacks/

Imagen n.° 1
Un ejemplo de ataque CSRF usando una solicitud GET



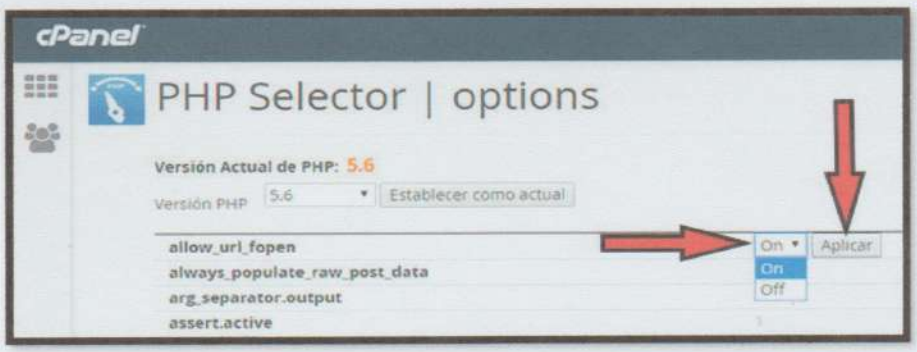
Fuente: Extraído del sitio web https://www.acunetix.com/websitesecurity/csrf-attacks/

2. Directiva PHP "allow_url_fopen" habilitada

La directiva de configuración de PHP "allow_url_fopen" está habilitada. Cuando está habilitada, esta directiva permite recuperación de datos de ubicaciones remotas (sitio web o servidor FTP), una gran cantidad de vulnerabilidades de inyección de código reportadas en aplicaciones web basadas en PHP, son causados por la combinación de habilitar la directiva "allow_url_fopen" y un filtrado de entrada incorrecto[16].

Cuando está habilitada, la opción "allow_url_fopen" permite que las funciones PHP que aceptan un nombre de archivo operen en archivos remotos usando una URL HTTP o FTP. La opción, que se introdujo desde PHP 4.0.4 y está habilitada de forma predeterminada, es peligrosa porque puede permitir que los atacantes introduzcan contenido malicioso en una aplicación. En el mejor de los casos, operar en archivos remotos deja la aplicación susceptible a los atacantes que alteran el archivo remoto para incluir contenido malicioso. En el peor de los casos, si los atacantes pueden controlar una URL en la que opera la aplicación, pueden inyectar contenido malicioso arbitrario en la aplicación proporcionando una URL a un servidor remoto[17].

Imagen n.° 2
Activar y Desactivar la Directiva "allow_url_fopen" desde el Selector PHP de cPanel



Fuente: Extraído de https://www.hostinet.com/formacion/panel-alojamiento/activar-desactivar-allow-url-fopen-selector-php-cpanel/

16 Fuente: https://www.acunetix.com/vulnerabilities/web/php-allow_url_fopen-enabled/
17 Fuente: https://vulncat.fortify.com/en/detail?id=desc.config.php.php_misconfiguration_allow_url_fopen.

3. Directiva PHP "open_basedir" no está configurada

La directiva de configuración "open_basedir" limitará los archivos que PHP puede abrir al árbol de directorios especificado. Cuando un script intenta abrir un archivo, por ejemplo, fopen () o gzopen (), se comprueba la ubicación del archivo, cuando el archivo está fuera del árbol de directorios especificado, PHP se negará a abrirlo. Esta directiva es una buena protección contra las vulnerabilidades de inclusión de archivos remotos, toda vez que, para un atacante remoto, no es posible romper las restricciones de "open_basedir" si solo puede inyectar el nombre de un archivo para ser incluido. Por lo tanto, la cantidad de archivos que podrá incluir con una vulnerabilidad de inclusión de archivos local de este tipo es limitada[18].

Cuando está presente, la opción de configuración "open_basedir" intenta evitar que los programas PHP operen en archivos fuera de los árboles de directorios especificados en php.ini, si no se especifican directorios con la opción "open_basedir", los programas que se ejecutan en PHP tienen acceso completo a archivos arbitrarios en el sistema de archivos local, lo que puede permitir a los atacantes leer, escribir o crear archivos a los que no deberían poder acceder[19].

Imagen n.° 3
Configuración de directiva "open_basedir" en el archivo php.ini

```
1  //php.ini
2  ...
3  ...
4  open_basedir = "/ruta/webs/miweb/www:/ruta/webs/miweb"
5  ...
6  ...
```

Fuente: Extraído de https://professor-falken.com/webmasters-y-seo/como-solucionar-el-error-open_basedir-restriction-in-effect-file-is-not-within-the-allowed-paths-en-tu-servidor-con-php/

En tal sentido, una vulnerabilidad de una página Web es lo que permite a un atacante que pueda ser explotada y, afectar la integridad y disponibilidad de su información, por lo cual es importante aplicar medidas para proteger una página web y garantizar que los datos no están expuestos a agentes internos o externos, como el uso de principios de seguridad durante el ciclo de vida del software, pudiendo ser este adquirido o desarrollado.

b) Criterio:

- **Decreto legislativo n.° 1412. Decreto legislativo que aprueba la Ley de Gobierno Digital, publicada el 13 de setiembre de 2018.**

"(...)
Artículo 31.- Marco de Seguridad Digital del Estado Peruano
El Marco de Seguridad Digital del Estado Peruano se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la Administración Pública".

[18] Fuente: https://www.acunetix.com/vulnerabilities/web/php-open_basedir-is-not-set/
[19] Fuente: https://vulncat.fortify.com/en/detail?id=desc.config.php.php_misconfiguration_open_basedir

- **Decreto Supremo n.° 050-2018-PCM. Aprueban la definición de Seguridad Digital en el Ámbito Nacional, publicada el 15 de mayo de 2018.**

  "(...)
  Artículo 2.- Definición de Seguridad Digital en el ámbito nacional
  La Seguridad Digital en el ámbito nacional es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas; debiéndose tener presente para estos efectos los aspectos siguientes:
  (..)
  b) Nota 2: Las medidas proactivas y reactivas comprenden tecnología, políticas, controles, programas de capacitación y sensibilización que tienen por finalidad preservar la confidencialidad, integridad y disponibilidad de la información contenida en el entorno digital.
  c) Nota 3: Los riesgos en el entorno digital o riesgo de seguridad digital es resultado de una combinación de amenazas y vulnerabilidades en el entorno digital. La gestión del riesgo de seguridad digital comprende los procesos que garantizan que las acciones o medidas son apropiadas con los riesgos y objetivos económicos y sociales en juego. (...)".

- **Norma Técnica Peruana "NTP ISO/IEC 12207: 2016 Ingeniería de software y sistemas. Procesos del ciclo de vida del software. 3ª Edición" aprobada por Resolución Ministerial n.° 041-2017-PCM de 27 de febrero de 2017.**

  "7.2.4 Procesos de Verificación del Software
  (...)
  7.2.4.3.2.3 Verificación del código. El código se debe verificar considerando los criterios que se indican a continuación:
  a) El código es trazable hasta el diseño y requisitos, comprobable, correcto y cumple con los requisitos y los estándares de codificación.
  (...)
  d) El código implementa requisitos de protección, seguridad y otros requisitos críticos de manera correcta, como indican los métodos adecuadamente rigurosos."

- **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. 2a. Edición", aprobada mediante Resolución Ministerial n.° 246-2007-PCM de 22 de agosto del 2007.**

  "12.6.1 Control de las vulnerabilidades técnicas.

  Control
  Se debe obtener a tiempo la información sobre las vulnerabilidades técnicas de los sistemas información utilizadas. Igualmente, se debe evaluar la exposición de la organización a tales vulnerabilidades y las medidas apropiadas para tratar a los riegos asociados.

  Guía de Implementación
  Un inventario actual y completo de activos (véase el inciso 7.1) es un prerrequisito para una efectiva gestión de vulnerabilidades técnicas. La información específica requerida para apoyar

la gestión de vulnerabilidades técnicas incluye al vendedor de software, numero de versiones, el estado actual de despliegue (por ejemplo, que software es instalado en que sistema) y las personas dentro de la organización responsables del software.

Una acción apropiada y a tiempo debe ser tomada en cuenta en respuesta a la identificación de vulnerabilidades técnicas potenciales. Las siguientes pautas deben seguirse para establecer un proceso de gestión de vulnerabilidades técnicas efectivas:

a) La organización debe definir y establecer los roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas, incluyendo el monitoreo de vulnerabilidades, la evaluación de la vulnerabilidad de riesgo, el parchado, el seguimiento de activos y cualquiera otra responsabilidad coordinada; (...)
b) Los recursos de información que se utilizaran para identificar las vulnerabilidades técnicas relevantes y para mantener precaución sobre ellos se deben identificar para el software y otras tecnologías (basadas en el inventario de activos, véase 7.1.1); estos recursos de información deben ser actualizados basados en cambios de inventario o cuando un recurso nuevo o más útil se encuentre;
c) Se debería definir una línea de tiempo para reaccionar ante notificaciones de vulnerabilidades técnicas potenciales y relevantes".

c) Consecuencia:

La situación expuesta podría ocasionar que el Portal Web Institucional de Pensión 65, presente vulnerabilidades de seguridad, generando el riesgo de afectación a la integridad y disponibilidad de la información pública del programa, como lo es la difusión de la Relación Bimestral de Usuarios – RBU, que es de importancia para los adultos mayores de sesenta y cinco (65) años que se encuentran en situación de vulnerabilidad.

VI. DOCUMENTACIÓN VINCULADA AL HITO DE CONTROL

La información y documentación que la Comisión de Control ha revisado y analizado durante el desarrollo del servicio de Control Concurrente al Hito de Control n.° 2: "Cotejo de información", se encuentra detallada en el Apéndice n.° 1.

Las situaciones adversas identificadas en el presente informe se sustenta en la revisión y análisis de la documentación e información obtenida por la Comisión de Control, las cuales han sido señaladas en la condición y se encuentra en el acervo documentario del Programa "Pensión 65".

VII. INFORMACIÓN DEL REPORTE DE AVANCE ANTE SITUACIONES ADVERSAS

Durante la ejecución del Hito de Control n.° 2 del servicio de Control Concurrente, la Comisión de Control no emitió Reporte de Avance ante situaciones adversas.

VIII. INFORMACIÓN DE LAS SITUACIONES ADVERSAS COMUNICADAS EN INFORMES DE HITO DE CONTROL ANTERIORES

No aplica.

IX. CONCLUSIONES

Durante la ejecución del servicio de Control Concurrente del Hito de control n.° 2: "Cotejo de información", se han advertido dos (2) situaciones adversas que podrían afectar el resultado o el logro de los objetivos del Programa "Pensión 65"; las cuales se revelan en el presente informe, sin perjuicio del control posterior que hubiera lugar.

Las situaciones adversas se detallan a continuación:

- Personal de la Unidad de Tecnologías de la Información utiliza un usuario común para acceder al servidor de base de datos, donde se realizan los trabajos de cotejo de datos, lo cual podría permitir que intencionalmente o por error, sea pasible de ser modificada, borrada, copiada o extraída dicha información, sin que se pueda conocer la identidad de quien ocasionaría tales perjuicios.
  (Situación adversa n.° 1).

- Se identificaron vulnerabilidades de seguridad en el Portal web de Pensión 65 lo cual ocasionaría el riesgo de afectación a la integridad y disponibilidad de la información referente a la difusión de la relación bimestral de usuarios (RBU), información pública que es de interés a los beneficiarios del programa.
  (Situación adversa n.° 2).

X. RECOMENDACIONES

1. Hacer de conocimiento a la Directora Ejecutiva del Programa el presente Informe de Hito de Control, el cual contiene dos situaciones adversas identificadas como resultado del servicio de Control Concurrente al hito de control n.° 2: "Cotejo de información", con la finalidad se adopten las acciones preventivas y correctivas que correspondan, en el marco de sus competencias y obligaciones en la gestión institucional, con el objeto de asegurar la continuidad del proceso, el resultado o el logro de los objetivos en lo que corresponde al "Cotejo de información"

2. Hacer de conocimiento a la Directora Ejecutiva del Programa que debe comunicar a la Comisión de Control las acciones preventivas o correctivas que implemente respecto a las situaciones adversas contenidas en el presente Informe.

Lima, 24 de mayo de 2021.

Ricardo Suarez Frías
Supervisor de la
Comisión de Control

Anthoanette Macazana Rojas
Jefa de Comisión
de Control

Susan Jakelin Farfan Giove
Jefa del Órgano de Control Institucional
Pensión 65

APÉNDICE N° 1

DOCUMENTACIÓN VINCULADA AL HITO DE CONTROL N° 1: "DETERMINACIÓN DE POTENCIALES USUARIOS Y COTEJO DE INFORMACIÓN".

1. **PERSONAL DE LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN UTILIZA UN USUARIO COMÚN PARA ACCEDER AL SERVIDOR DE BASE DE DATOS, DONDE SE REALIZAN LOS TRABAJOS DE COTEJO DE DATOS, LO CUAL PODRÍA PERMITIR QUE INTENCIONALMENTE O POR ERROR, SEA PASIBLE DE SER MODIFICADA, BORRADA, COPIADA O EXTRAÍDA DICHA INFORMACIÓN, SIN QUE SE PUEDA CONOCER LA IDENTIDAD DE QUIEN OCASIONARÍA TALES PERJUICIOS.**

N°	Documento
1	Memorando n.° D000060- 2021-PENSION65-OCI de 20 de mayo de 2021.
2	Memorando N° D000135-2021-PENSION65-UTI-AZ de 20 de mayo de 2021.
3	Cuestionario de Control n.° 01-2021-CG/PENSION65-OCI de 20 de mayo de 2021.

2. **SE IDENTIFICARON VULNERABILIDADES DE SEGURIDAD EN EL PORTAL WEB DE PENSIÓN 65 LO CUAL OCASIONARÍA EL RIESGO DE AFECTACIÓN A LA INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN REFERENTE A LA DIFUSIÓN DE LA RELACIÓN BIMESTRAL DE USUARIOS (RBU), INFORMACIÓN PÚBLICA QUE ES DE INTERÉS A LOS BENEFICIARIOS DEL PROGRAMA.**

N°	Documento
1	Portal Web Institucional de Pensión 65
2	Reportes "Acunetix Affected Items.pdf" y "ZAP Scanning Report.html" de 19 de mayo de 2021.

Señora
MABEL GALVEZ GALVEZ
Directora Ejecutiva
Programa Nacional de Asistencia Solidaria Pensión 65
Av. República de Panamá 3505 - Oficina 601
Lima/Lima/San Isidro

ASUNTO : Comunicación de Informe de Hito de Control N° 008-2021-OCI/5963.

REFERENCIA : a) Artículo 8° de la Ley n.° 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, y sus modificatorias.
b) Directiva n.° 002-2019-CG/NORM, "Servicio de Control Simultáneo", aprobada con Resolución de Contraloría n.° 115-2019-CG, del 28 de marzo de 2019.

Me dirijo a usted en el marco de la normativa de la referencia, que regula el servicio de Control Simultáneo y establece la comunicación al Titular de la entidad o responsable de la dependencia, y de ser el caso a las instancias competentes, respecto de la existencia de situaciones adversas que afectan o podrían afectar la continuidad del proceso, el resultado o el logro de los objetivos del proceso en curso, a fin que se adopten oportunamente las acciones preventivas y correctivas que correspondan.

Sobre el particular, de la revisión de la información y documentación vinculada al Hito de Control n.° 2 "Proceso de determinación de potenciales usuarios y cotejo de información, así como determinación de casos sensibles de vulnerabilidad adicional en el marco de la afiliación de usuarios para la entrega de subvención monetaria en el ámbito nacional", comunicamos que se han identificado las situaciones adversas contenidas en el Informe de Hito de Control n.° 008-2021-OCI/5963-SCC, que se adjunta al presente documento.

En tal sentido, solicitamos que una vez adoptadas las acciones que correspondan, éstas sean informadas a la brevedad a la Comisión de Control.

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

Atentamente,

Esta es una copia auténtica imprimible de un documento electrónico archivado en el Programa Nacional de Asistencia Solidaria Pension65, 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: **http://mesadepartes.pension65.gob.pe:8080/verificadorDocumental** e ingresando la siguiente clave: **3KYY4RO**

N° Exp : OCI00020210000098